



DECYZJA WYKONAWCZA KOMISJI (UE) 2025/2574

z dnia 19 grudnia 2025 r.

zmieniająca decyzję wykonawczą Komisji (UE) 2021/1772 na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzającą odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo

(notyfikowana jako dokument nr C(2025) 8771)

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie 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 (ogólne rozporządzenie o ochronie danych) ⁽¹⁾, w szczególności jego art. 45 ust. 3,

a także mając na uwadze, co następuje:

1. WPROWADZENIE

- (1) W decyzji wykonawczej Komisji (UE) 2021/1772 ⁽²⁾ stwierdzono, że do celów art. 45 rozporządzenia (UE) 2016/679 Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej do Zjednoczonego Królestwa w zakresie stosowania tego rozporządzenia ⁽³⁾.
- (2) Podczas przyjmowania decyzji wykonawczej (UE) 2021/1772 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 ⁽⁴⁾ 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 ⁽⁵⁾, Zjednoczone Królestwo przyjmie nowy system ochrony danych, różniący się od systemu, który obowiązywał, gdy Zjednoczone Królestwo było związane prawem Unii, a także będzie stosowało ten nowy system i egzekwowało jego stosowanie.
- (3) Jako że mogłoby to wiązać się z poprawkami do ram ochrony danych poddanych ocenie w decyzji wykonawczej (UE) 2021/1772 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) 2021/1772 miała zatem stracić moc w dniu 27 czerwca 2025 r., chyba że zostałaby przedłużona zgodnie z procedurą, o której mowa w art. 93 ust. 2 rozporządzenia (UE) 2016/679.

⁽¹⁾ Dz.U. L 119 z 4.5.2016, s. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>.

⁽²⁾ Decyzja wykonawcza Komisji (UE) 2021/1772 z dnia 28 czerwca 2021 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo (Dz.U. L 360 z 11.10.2021, s. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

⁽³⁾ Zob. art. 1 ust. 1 decyzji wykonawczej (UE) 2021/1772. Zgodnie z art. 1 ust. 2 tej decyzji: decyzja nie dotyczy danych osobowych przekazywanych do celów kontroli imigracji w Zjednoczonym Królestwie ani danych, które z innego względu wchodzą w zakres wyłączenia niektórych praw osób, których dane dotyczą, do celów utrzymania skutecznej kontroli imigracyjnej zgodnie z pkt 4 ppkt 1 załącznika 2 do brytyjskiej ustawy o ochronie danych z 2018 r.

⁽⁴⁾ Dz.U. C 384 I z 12.11.2019, s. 1.

⁽⁵⁾ 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).

- (4) Aby podjąć decyzję o ewentualnym przedłużeniu obowiązywania decyzji wykonawczej (UE) 2021/1772, 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) 2021/1772 w odniesieniu do elementów wymienionych w art. 45 ust. 2 rozporządzenia (UE) 2016/679.
- (5) W dniu 23 października 2024 r. rząd Zjednoczonego Królestwa przedstawił w parlamencie Zjednoczonego Królestwa projekt ustawy o wykorzystaniu danych i dostępie do danych⁽⁶⁾, zawierający propozycje zmian w ogólnym rozporządzeniu o ochronie danych Zjednoczonego Królestwa (RODO UK) i ustawie o ochronie danych z 2018 r. (DPA 2018), które oceniono w decyzji wykonawczej (UE) 2021/1772. W dniu 24 czerwca 2025 r. Komisja przyjęła decyzję wykonawczą (UE) 2025/1226⁽⁷⁾, która przedłużyła obowiązywanie decyzji wykonawczej (UE) 2021/1772 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⁽⁸⁾.
- (6) Od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 Komisja na bieżąco monitorowała istotne zmiany w Zjednoczonym Królestwie⁽⁹⁾. Zgodnie z motywem 281 decyzji wykonawczej (UE) 2021/1772 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) 2021/1772, na skuteczność korzystania z indywidualnych praw, w tym wszelkie istotne zmiany w prawie i praktyce dotyczące wyjątków lub ograniczeń takich praw (w szczególności wyjątku dotyczącego utrzymania skutecznej kontroli imigracyjnej) oraz przestrzegania ograniczeń i zabezpieczeń w odniesieniu do dostępu rządowego. 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 RODO UK i 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 rozporządzenia (UE) 2016/679 z Unii Europejskiej do Zjednoczonego Królestwa.
- (8) Komisja stwierdza również, że w świetle zmian w odpowiednich przepisach prawa Zjednoczonego Królestwa⁽¹⁰⁾ wyłączenie z zakresu decyzji wykonawczej (UE) 2021/1772 danych osobowych przekazywanych do celów kontroli imigracyjnej Zjednoczonego Królestwa lub w inny sposób objętych zakresem wyłączenia niektórych praw osób, których dane dotyczą, do celów utrzymania skutecznej kontroli imigracyjnej („wyłączenie dotyczące imigracji”) na podstawie pkt 4 ppkt 1 załącznika 2 do brytyjskiej ustawy o ochronie danych, nie jest już uzasadnione, jak wyjaśniono w motywie 37 niniejszej decyzji.

⁽⁶⁾ Dostęp pod adresem: <https://bills.parliament.uk/bills/3825/news>.

⁽⁷⁾ Decyzja wykonawcza Komisji (UE) 2025/1226 z dnia 24 czerwca 2025 r. zmieniająca decyzję wykonawczą (UE) 2021/1772 na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzającą odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo (Dz.U. L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

⁽⁸⁾ Ustawa o wykorzystaniu danych i dostępie do danych otrzymała zgodę królewską w dniu 19 czerwca 2025 r.

⁽⁹⁾ Art. 45 ust. 4 rozporządzenia (UE) 2016/679.

⁽¹⁰⁾ W maju 2021 r. sąd apelacyjny dla Anglii i Walii uznał wyłączenie dotyczące imigracji w brzmieniu sformułowanym wówczas w pkt 4 ppkt 1 załącznika 2 do brytyjskiej ustawy o ochronie danych za niezgodne z prawem Zjednoczonego Królestwa, ponieważ środek ustawodawczy nie zawierał szczegółowych przepisów określających zabezpieczenia wymienione w art. 23 ust. 2 RODO UK. Aby zastosować się do tego wyroku, rząd Zjednoczonego Królestwa zmienił wyłączenie dotyczące imigracji, przyjmując rozporządzenie z 2022 r. w sprawie zmiany załącznika 2 do ustawy o ochronie danych z 2018 r. Zmienione wyłączenie zostało jednak ponownie zakwestionowane jako niespełniające wszystkich wymogów określonych w art. 23 ust. 2 RODO UK. W wyroku z dnia 11 grudnia 2023 r. sąd apelacyjny ponownie uznał zmienione wyłączenie dotyczące imigracji za niezgodne z art. 23 ust. 2 RODO UK. Aby dostosować się do tego wyroku, rząd Zjednoczonego Królestwa przyjął następnie rozporządzenie z 2024 r. w sprawie zmiany załącznika 2 do ustawy o ochronie danych z 2018 r., które weszło w życie w dniu 8 marca 2024 r.

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

2.1. Ramy ochrony danych obowiązujące w Zjednoczonym Królestwie

- (9) W momencie przyjęcia decyzji wykonawczej (UE) 2021/1772 ramy prawne dotyczące ochrony danych osobowych w Zjednoczonym Królestwie obejmowały:
- RODO UK ⁽¹¹⁾, wprowadzone do prawa Zjednoczonego Królestwa w drodze ustawy o wystąpieniu z Unii Europejskiej z 2018 r. ⁽¹²⁾ i zmienione rozporządzeniem w sprawie ochrony danych, prywatności i łączności elektronicznej wprowadzającym zmiany w związku z wyjściem z UE 2019 r. (rozporządzenie DPPEC) ⁽¹³⁾,
 - DPA 2018 ⁽¹⁴⁾, zmienioną rozporządzeniem DPPEC.
- (10) Choć te dwa akty, które ściśle odzwierciedlały odpowiednie przepisy mające zastosowanie w Unii Europejskiej, nadal stanowią prawodawstwo Zjednoczonego Królestwa w zakresie ochrony danych, od tego czasu podlegały pewnym ograniczonym zmianom, co odzwierciedla fakt, że Zjednoczone Królestwo nie podlega już prawu Unii Europejskiej.
- (11) Po pierwsze, w ustawie o zachowanym prawie UE (i uchyleniu lub reformie niektórych przepisów) z 2023 r. (ustawa REUL) ⁽¹⁵⁾ wyjaśniono, że od końca 2023 r. ogólne zasady prawa UE nie są już częścią prawa krajowego Zjednoczonego Królestwa ⁽¹⁶⁾. Ponadto sądy Zjednoczonego Królestwa nie muszą już dokonywać wykładni 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 ⁽¹⁷⁾. Odpowiednie sądy Zjednoczonego Królestwa muszą jednak nadal dokonywać wykładni niezmienionego prawa asymilowanego zgodnie ze stosownym orzecznictwem Europejskiego Trybunału Sprawiedliwości wydanym przed zakończeniem okresu przejściowego ⁽¹⁸⁾, jak wspomniano również w motywie 13 decyzji wykonawczej (UE) 2021/1772. 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. 183A 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. 183A ust. 2

⁽¹¹⁾ Ogólne rozporządzenie o ochronie danych, dostępne pod adresem: <https://www.legislation.gov.uk/eur/2016/679/contents>.

⁽¹²⁾ Ustawa o wystąpieniu z Unii Europejskiej z 2018 r., dostępna pod adresem: <https://www.legislation.gov.uk/ukpga/2018/16/contents>, włączyła przepisy Unii, które miały bezpośrednie zastosowanie w Zjednoczonym Królestwie w dniu zakończenia okresu przejściowego, do prawa Zjednoczonego Królestwa. To tzw. „zachowane prawo UE” obejmuje rozporządzenie (UE) 2016/679 w całości, włącznie z motywami (zob. noty wyjaśniające do ustawy o wystąpieniu z Unii Europejskiej z 2018 r., pkt 83, dostępne pod adresem: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Zgodnie z tą ustawą sądy Zjednoczonego Królestwa musiały dokonywać wykładni tego niezmienionego, zachowanego prawa UE zgodnie ze stosownym orzecznictwem Europejskiego Trybunału Sprawiedliwości i ogólnymi zasadami prawa Unii obowiązującymi bezpośrednio przed zakończeniem okresu przejściowego (zwanymi odpowiednio „zachowanym orzecznictwem UE” i „zachowanymi ogólnymi zasadami prawa UE”).

⁽¹³⁾ 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.

⁽¹⁴⁾ 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 zapewniała, w przypadkach dozwolonych na mocy rozporządzenia (UE) 2016/679, przepisy krajowe doprecyzowujące i ograniczające stosowanie przepisów rozporządzenia (UE) 2016/679 oraz transponowała 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 uchyłająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89, ELI: <http://data.europa.eu/eli/dir/2016/680/oj>).

⁽¹⁵⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/ukpga/2023/28>.

⁽¹⁶⁾ Art. 5 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., zmienionej ustawą REUL.

⁽¹⁷⁾ Art. 5 ust. A2 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., zmienionej ustawą REUL.

⁽¹⁸⁾ Art. 6 ust. 3 i 7 ustawy o wystąpieniu z Unii Europejskiej z 2018 r., zmienionej ustawą REUL.

lit. b) DPA 2018 odstępianie od stosowania tego domniemania jest możliwe, jeżeli parlament Zjednoczonego Królestwa wyraźnie postanowi o tym w ustawodawstwie, zachowując suwerenność parlamentarną. Ponadto w art. 186 ust. 2A 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.

- (12) Po drugie, od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 przepisy Zjednoczonego Królestwa o ochronie danych zostały już zmienione rozporządzeniem zmieniającym w sprawie podstawowych praw i wolności w zakresie ochrony danych z 2023 r. ⁽¹⁹⁾ W rozporządzeniu tym zdefiniowano odniesienia do praw podstawowych lub podstawowych wolności w RODO UK i DPA 2018 (które wcześniej zdefiniowano tak, aby obejmowały prawa podstawowe i podstawowe wolności UE ⁽²⁰⁾) 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. ⁽²¹⁾ 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 ⁽²²⁾.
- (13) Ponadto RODO UK i DPA 2018 były 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. przepisy dotyczące przetwarzania danych do celów badań naukowych, podstawy prawne przetwarzania danych, przepisy dotyczące zasady ograniczenia celu oraz warunki zautomatyzowanego podejmowania decyzji. Ponadto ustawą o wykorzystaniu danych i dostępie do danych wprowadzono zmiany w strukturze zarządzania podmiotem, 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.
- (14) 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) 2021/1772. Ocena przeprowadzona w decyzji wykonawczej (UE) 2021/1772 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) 2021/1772.
- (15) 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 ⁽²³⁾. Jak wyjaśnił w swoim orzecznictwie Trybunał Sprawiedliwości Unii Europejskiej, nie oznacza to konieczności stwierdzenia identycznego stopnia ochrony ⁽²⁴⁾. 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 ⁽²⁵⁾. 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 ⁽²⁶⁾.

⁽¹⁹⁾ Dostęp pod adresem: <https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023>.

⁽²⁰⁾ 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.

⁽²¹⁾ Art. 2 ust. 3 rozporządzenia zmieniającego w sprawie podstawowych praw i wolności w zakresie ochrony danych z 2023 r.

⁽²²⁾ Art. 6, 8, 10 i 13 EKPC (zob. także załącznik 1 do ustawy o prawach człowieka z 1998 r.).

⁽²³⁾ Motyw 104 rozporządzenia (UE) 2016/679.

⁽²⁴⁾ Sprawa C-362/14, Schrems („Schrems I”), ECLI:EU:C:2015:650, pkt 73.

⁽²⁵⁾ Schrems I, pkt 74.

⁽²⁶⁾ 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%3A52017DC0007&qid=1765461142928>.

2.1.1. Definicje

- (16) Podstawowe pojęcia z dziedziny ochrony danych odzwierciedlające terminologię rozporządzenia (UE) 2016/679 nadal mają zastosowanie w systemie ochrony danych Zjednoczonego Królestwa. Pojęcia te oceniono w motywie 23 decyzji wykonawczej (UE) 2021/1772.
- (17) W ustawie o wykorzystaniu danych i dostępie do danych pozostawiono wprowadzić zdecydowaną większość definicji bez zmian, w art. 4 pkt 2, 3, 4 i 5 RODO UK wprowadzono jednak szczegółowe definicje dotyczące przetwarzania danych osobowych do celów naukowych, historycznych i statystycznych. W pkt 2 zdefiniowano „przetwarzanie do celów naukowych” jako przetwarzanie danych osobowych do celów wszelkich badań, które można racjonalnie określić jako naukowe. Badania te mogą być finansowane ze środków publicznych lub prywatnych i mogą być prowadzone jako działalność komercyjna lub niekomercyjna. Pkt 3, odzwierciedlający treść motywu 159 rozporządzenia (UE) 2016/679, zawiera niewyczerpujący wykaz przykładów działań badawczych, które kwalifikują się jako służące celom naukowym, obejmujący rozwój techniczny, demonstrację, badania podstawowe i badania stosowane. W pkt 4 wyjaśniono, że „badania historyczne” obejmują badania genealogiczne, które uznano również za cel historyczny w motywie 160 rozporządzenia (UE) 2016/679. Wreszcie pkt 5 definiuje przetwarzanie do celów statystycznych jako przetwarzanie danych na potrzeby badań statystycznych lub w celu uzyskania wyników statystycznych, w przypadku gdy dane są zagregowane do tego stopnia, że nie stanowią już danych osobowych. Ponadto przetwarzane dane lub wynikające z nich informacje nie mogą być wykorzystywane do podejmowania decyzji lub działań skierowanych do jakiejkolwiek osoby fizycznej. Definicja ta jest zgodna z celami statystycznymi w rozumieniu określonym w motywie 162 rozporządzenia (UE) 2016/679.
- (18) Podsumowując, chociaż w ramach zmian do art. 4 RODO UK dodano szczegółowe definicje przetwarzania danych do celów naukowych, historycznych i statystycznych, definicje te są spójne z literą i duchem rozporządzenia (UE) 2016/679, co odzwierciedlono we wspomnianych wyżej motywach 159, 160 i 162.
- (19) Przez dodanie pkt 6 do art. 4 RODO UK ustawą o wykorzystaniu danych i dostępie do danych ustanowiono również szczegółowe ramy uzyskiwania zgody osoby, której dane dotyczą, na przetwarzanie danych osobowych do celów naukowych. Podobnie jak w motywie 33 rozporządzenia (UE) 2016/679, w którym uznano, że w obszarze badań naukowych nie zawsze możliwe jest uzyskanie zgody na konkretny cel przetwarzania, nowy przepis dopuszcza szersze formy zgody, zezwalając osobom, których dane dotyczą, na udzielenie ważnej zgody, nawet jeżeli w momencie zbierania danych nie można w pełni zidentyfikować dokładnych celów badań, pod warunkiem że ubieganie się o zgodę jest spójne z ogólnie uznanymi normami etycznymi odnoszącymi się do konkretnej dziedziny badań. W każdym przypadku osoby, których dane dotyczą, muszą mieć możliwość wyrażenia zgody na przetwarzanie danych osobowych wyłącznie w odniesieniu do określonych części badań, o ile to możliwe.
- (20) Ponadto w ustawie o wykorzystaniu danych i dostępie do danych doprecyzowano zabezpieczenia określone wcześniej w art. 89 RODO UK i art. 19 DPA 2018 w odniesieniu do przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych i do celów statystycznych w nowym rozdziale 8A RODO UK ⁽²⁷⁾. Zabezpieczenia te są podobne do zabezpieczeń wymaganych na mocy art. 89 rozporządzenia (UE) 2016/679 i obejmują wymóg wdrożenia środków technicznych i organizacyjnych w celu zapewnienia poszanowania zasady minimalizacji danych.

2.2. Zabezpieczenia, prawa i obowiązki

2.2.1. Zgodność z prawem i rzetelność przetwarzania

- (21) Ramy ochrony danych Zjednoczonego Królestwa nadal wymagają, aby dane były przetwarzane w sposób zgodny z prawem, rzetelny i prawnie uzasadniony, jak oceniono w motywach 24–26 decyzji wykonawczej (UE) 2021/1772.

⁽²⁷⁾ Art. 84A–84D RODO UK, wprowadzone art. 86 ustawy o wykorzystaniu danych i dostępie do danych.

- (22) Zasady zgodności z prawem i rzetelności oraz podstawy zgodności przetwarzania z prawem są nadal zagwarantowane w prawie Zjednoczonego Królestwa poprzez art. 5 ust. 1 lit. a) i art. 6 ust. 1 RODO UK, jak oceniono w decyzji wykonawczej (UE) 2021/1772. Chociaż przepisy te pozostają w dużej mierze identyczne⁽²⁸⁾ z odpowiednimi przepisami rozporządzenia (UE) 2016/679, w ustawie o wykorzystaniu danych i dostępie do danych po raz pierwszy zmieniono art. 6 ust. 1 RODO UK, wprowadzając dodatkową podstawę prawną przetwarzania danych osobowych na mocy art. 6 ust. 1 lit. ea)⁽²⁹⁾. Zgodnie z tym przepisem przetwarzanie danych jest zgodne z prawem, jeżeli i w zakresie, w jakim „jest niezbędne do celów związanych z uznanym prawnie uzasadnionym interesem”. W przeciwieństwie do prawnie uzasadnionego interesu jako podstawy prawnej wynikającej z art. 6 ust. 1 lit. f) RODO UK nowo wprowadzona podstawa prawna dotycząca uznanego prawnie uzasadnionego interesu nie wymaga indywidualnego wyważenia prawnie uzasadnionych interesów administratora z interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą, co ma w założeniu zapewnić większą pewność prawa administratorom będącym podmiotami niepublicznymi. W nowo wprowadzonym art. 6 ust. 5 RODO UK określono, że przetwarzanie jest niezbędne do celów związanych z uznanym prawnie uzasadnionym interesem tylko wtedy, gdy spełnia warunek określony w załączniku 1⁽³⁰⁾, w którym wymieniono sytuacje, gdy przetwarzanie uznaje się za niezbędne do celów związanych z uznanym prawnie uzasadnionym interesem, na przykład gdy przetwarzanie odbywa się w odpowiedzi na żądanie otrzymane przez organ publiczny, który potrzebuje danych do celów wykonania zadania realizowanego w interesie publicznym, mającego podstawę prawną zgodną z art. 6 ust. 3 RODO UK, w przypadku gdy przetwarzanie jest niezbędne do ochrony bezpieczeństwa narodowego, ochrony bezpieczeństwa publicznego lub do celów obrony, do reagowania na sytuację nadzwyczajną, wykrywania przestępstw i zapobiegania im, prowadzenia postępowań przygotowawczych lub ochrony osób wymagających szczególnego traktowania⁽³¹⁾.

- (23) Ustawa o wykorzystaniu danych i dostępie do danych rozszerza wprawdzie tym samym wykaz podstaw prawnych przetwarzania danych osobowych, które są dostępne dla administratora, jednak nowo wprowadzona podstawa prawna dotycząca uznanego prawnie uzasadnionego interesu podlega kilku istotnym ograniczeniom. Po pierwsze, uznane prawnie uzasadnione interesy ograniczają się do konkretnych sytuacji wymienionych w sposób wyczerpujący w ustawie. Po drugie, organy publiczne nie mogą powoływać się na tę podstawę prawną przy wykonywaniu swoich zadań⁽³²⁾. Po trzecie, dotyczy to wyłącznie obszarów, w których istnieje wyraźny interes publiczny związany z czynnością przetwarzania (zgodnie z warunkami określonymi w załączniku 1), tj. w których przetwarzanie służy celom wymienionym w art. 23 RODO UK (który odpowiada art. 23 rozporządzenia (UE) 2016/679) i w związku z tym nie można się na nie powoływać do celów komercyjnych. Po czwarte, choć ustawa o wykorzystaniu danych i dostępie do danych przyznaje Sekretarzowi Stanu prawo do zmiany wykazu

⁽²⁸⁾ W celu doprecyzowania ustawa o wykorzystaniu danych i dostępie do danych wprowadza również w art. 6 RODO UK nowy ustęp, w którym przedstawiono przykłady rodzajów przetwarzania, które można uznać za niezbędne do celów związanych z prawnie uzasadnionym interesem w rozumieniu art. 6 ust. 1 lit. f) RODO UK. Przykłady te (marketing bezpośredni, wewnątrzgrupowe przekazywanie danych do celów administracyjnych oraz bezpieczeństwo sieci i systemów informatycznych) wymieniono również w motywach 47 i 48 rozporządzenia (UE) 2016/679 jako sytuacje, w których przetwarzanie byłoby uznawane za zgodne z prawnie uzasadnionym interesem administratora.

⁽²⁹⁾ Art. 70 ust. 2 lit. b) ustawy o wykorzystaniu danych i dostępie do danych. Art. 70 ust. 5 ustawy o wykorzystaniu danych i dostępie do danych rozszerzył prawo sprzeciwu określone w art. 21 RODO UK na nowy przepis art. 6 ust. 1 lit. ea) RODO UK.

⁽³⁰⁾ Art. 70 ust. 4 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³¹⁾ Zob. załącznik 4 do ustawy o wykorzystaniu danych i dostępie do danych. Według władz Zjednoczonego Królestwa przykłady sytuacji, w których podmioty niepubliczne mogą potrzebować przetwarzać dane osobowe w celu zapobiegania przestępstwom lub ich wykrywania, obejmują sytuacje, w których przedsiębiorstwo dowiaduje się o próbach bezprawnego włamania do jego systemów komputerowych lub w których bank lub instytucja finansowa dowiadują się o nieuczciwych próbach otwarcia rachunku. Przetwarzanie danych osobowych przez podmiot niepubliczny może być na przykład konieczne do ochrony bezpieczeństwa narodowego lub obrony narodowej, jeżeli organizacja handlowa podejrzewa, że działalność internetowa klienta wskazuje na jego zaangażowanie w działalność terrorystyczną. Komisarz ds. Informacji opracowuje obecnie szczegółowe wytyczne w tej kwestii, w tym definicje odpowiednich pojęć. Zgodnie z tymi wytycznymi „bezpieczeństwo narodowe” może na przykład obejmować bezpieczeństwo i dobrobyt Zjednoczonego Królestwa jako całości lub bezpieczeństwo i dobrobyt jego ludności, instytucji i systemu rządów. Zob. projekt wytycznych Komisarza ds. Informacji dotyczących uznanego prawnie uzasadnionego interesu, opublikowany do celów konsultacji publicznych, dostępny pod adresem: <https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/>.

⁽³²⁾ Art. 6 ust. 1 akapit ostatni, zmieniony art. 70 ust. 2 lit. c) ustawy o wykorzystaniu danych i dostępie do danych.

zawartego w załączniku 1 w drodze rozporządzenia ⁽³³⁾, Sekretarz Stanu może wydać takie rozporządzenie jedynie po konsultacji z Komisarzem ds. Informacji ⁽³⁴⁾ i dodać do tego wykazu uznany prawnie uzasadniony interes jedynie wtedy, gdy przetwarzanie to jest ponownie konieczne do ochrony celu leżącego w interesie publicznym wymienionego w art. 23 ust. 1 lit. c)–j) RODO UK ⁽³⁵⁾. Ponadto, jak potwierdzono również w wytycznych Komisarza ds. Informacji ⁽³⁶⁾, administratorzy danych opierający się na uznanym prawnie uzasadnionym interesie jako podstawie prawnej są zobowiązani do przestrzegania wszystkich innych wymogów wynikających z RODO UK, w tym do zapewnienia, aby przetwarzanie było niezbędne i proporcjonalne do celów realizacji prawnie uzasadnionego interesu.

- (24) Po drugie, ustawą o wykorzystaniu danych i dostępie do danych doprecyzowano art. 6 ust. 3, art. 9 ust. 2 lit. g) i art. 10 ust. 1 RODO UK, które odpowiadają odpowiednim przepisom rozporządzenia (UE) 2016/679, wyjaśniając, że podstawa przetwarzania danych osobowych, szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych zgodnie z obowiązkiem prawnym lub w celu wykonania zadania w interesie publicznym może opierać się nie tylko na prawie krajowym, ale również na odpowiednim prawie międzynarodowym ⁽³⁷⁾. Odpowiednie prawo międzynarodowe jest następnie ograniczone nowo wprowadzonym art. 9A RODO UK, w związku z załącznikiem A1, do jednej umowy, a mianowicie Umowy między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki o dostępie do danych elektronicznych w celu zwalczania poważnej przestępczości, podpisanej w dniu 3 października 2019 r. (umowa między Zjednoczonym Królestwem a USA) ⁽³⁸⁾. Zabezpieczenia przewidziane w tej umowie oceniono w motywach 153–155 decyzji wykonawczej (UE) 2021/1772, a ich wdrożenie przeanalizowano w motywach 87–93 niniejszej decyzji.

2.2.2. Przetwarzanie szczególnych kategorii danych osobowych

- (25) Ramy ochrony danych Zjednoczonego Królestwa nadal zapewniają szczególne zabezpieczenia w przypadku szczególnych kategorii danych, jak oceniono w motywach 27–42 decyzji wykonawczej (UE) 2021/1772.
- (26) Zarówno definicja szczególnych kategorii danych osobowych, jak i szczegółowe przepisy mające zastosowanie do przetwarzania tych kategorii danych w RODO UK i w DPA 2018 pozostają w mocy. Jednocześnie ustawa o wykorzystaniu danych i dostępie do danych przyznaje Sekretarzowi Stanu nowe uprawnienia regulacyjne w zakresie dodawania szczególnych kategorii danych, dostosowywania warunków ich wykorzystywania oraz dodawania nowych definicji, w razie potrzeby ⁽³⁹⁾. Co ważne, uprawnienie to nie pozwala Sekretarzowi Stanu na usunięcie lub zmianę istniejących szczególnych kategorii danych ani na zmianę warunków przetwarzania tych kategorii ⁽⁴⁰⁾. Nowo wprowadzone uprawnienia regulacyjne umożliwiają zatem rządowi jedynie dodanie nowych kategorii danych wrażliwych i określenie warunków przetwarzania tych kategorii, co ma umożliwić rządowi reagowanie w razie potrzeby na przyszłe zmiany technologiczne i społeczne.
- (27) W związku z tym zmiany te nie mają wpływu na stopień ochrony szczególnych kategorii danych osobowych uznany w decyzji wykonawczej (UE) 2021/1772 za zasadniczo odpowiadający (tzn. merytorycznie równoważny) ochronie w UE.

⁽³³⁾ Przed ustanowieniem nowych przepisów Sekretarz Stanu musi wziąć pod uwagę skutki wszelkich zmian dla interesów oraz podstawowych praw i wolności osób, których dane dotyczą, oraz fakt, że dzieci (w stosownych przypadkach) zasługują na szczególną ochronę w odniesieniu do ich danych osobowych. Takie nowe przepisy muszą zostać ustanowione w drodze rozporządzenia z mocą ustawy (ang. *statutory instrument*) i podlegają procedurze zatwierdzającej (ang. *affirmative resolution*), co oznacza, że muszą zostać aktywnie zatwierdzone przez parlament Zjednoczonego Królestwa. Art. 70 ust. 4 pkt 8 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³⁴⁾ Art. 182 ust. 2 DPA 2018.

⁽³⁵⁾ Art. 70 ust. 4 pkt 9 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³⁶⁾ Zob. wytyczne Komisarza ds. Informacji dotyczące prawnie uzasadnionych interesów, dostępne pod adresem: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy>.

⁽³⁷⁾ Art. 72 ustawy o wykorzystaniu danych i dostępie do danych.

⁽³⁸⁾ Umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki o dostępie do danych elektronicznych w celu zwalczania poważnej przestępczości, dostępna pod następującym adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

⁽³⁹⁾ Art. 74 ustawy o wykorzystaniu danych i dostępie do danych. Takie przepisy podlegają procedurze zatwierdzającej (ang. *affirmative resolution*), co oznacza, że wymagają one aktywnego zatwierdzenia przez parlament Zjednoczonego Królestwa.

⁽⁴⁰⁾ Zob. nowy art. 11A ust. 1 lit. b) i ust. 2 RODO UK, a także noty wyjaśniające do projektu ustawy o wykorzystaniu danych i dostępie do danych, pkt 571, dostępne pod następującym adresem: <https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf>.

2.2.3. Ograniczenie celu

- (28) System ochrony danych osobowych Zjednoczonego Królestwa nadal wymaga, aby dane były przetwarzane w określonym celu, a następnie wykorzystywane tylko w takim zakresie, w jakim nie jest to niezgodne z pierwotnym celem przetwarzania, jak oceniono w motywach 43–48 decyzji wykonawczej (UE) 2021/1772.
- (29) Po pierwsze, w ustawie o wykorzystaniu danych i dostępie do danych wprowadzono niewiele ukierunkowanych poprawek do zasady ograniczenia celu określonej w art. 5 ust. 1 lit. b) RODO UK. Poprawki te doprecyzowują stosowanie tej zasady, nie zmieniając jej istoty. Art. 71 ust. 1, 2 i 3 ustawy o wykorzystaniu danych i dostępie do danych stanowi, że zasada ograniczenia celu ma zastosowanie w przypadku, gdy dane są zbierane od osoby, której dane dotyczą, lub w inny sposób, że ma ona zastosowanie wyłącznie w przypadku, gdy dane osobowe są dalej przetwarzane przez tego samego administratora lub w jego imieniu (tj. nie ma zastosowania w przypadku zmiany administratora) oraz że zgodność z tego przetwarzania z prawem nie wynika z samego faktu, że przetwarzanie to jest zgodne z celami, w których dane osobowe zostały zebrane.
- (30) Po drugie, ustawą o wykorzystaniu danych i dostępie do danych doprecyzowano przepisy dotyczące dalszego przetwarzania danych osobowych, przegrupowując je w nowo dodanym art. 8A RODO UK, w którym określono pełny system dalszego przetwarzania danych osobowych. W art. 8A ust. 2 RODO UK wymieniono elementy, które należy uwzględnić przy ustalaniu, czy nowy cel przetwarzania jest zgodny z pierwotnym celem. Elementy te były wcześniej wymienione w art. 6 ust. 4 RODO UK, który odpowiada art. 6 ust. 4 rozporządzenia (UE) 2016/679 ⁽⁴¹⁾. W art. 8A ust. 3 RODO UK zebrano w jednym przepisie sytuacje, w których przetwarzanie danych osobowych w nowym celu należy traktować jako zgodne z pierwotnym celem. Obejmuje to sytuacje, w których osoba, której dane dotyczą, wyraża zgodę na przetwarzanie danych osobowych w nowym celu lub gdy przetwarzanie jest niezbędne do zabezpieczenia celu wymienionego w art. 23 ust. 1 ⁽⁴²⁾, gdy przetwarzanie odbywa się do celów badań naukowych lub historycznych, celów archiwalnych w interesie publicznym lub do celów statystycznych ⁽⁴³⁾. Wreszcie w ustawie o wykorzystaniu danych i dostępie do danych wyjaśniono, że wszelkie przetwarzanie przeprowadzane w celu zapewnienia zgodności przetwarzania z zasadami ochrony danych określonymi w art. 5 ust. 1 RODO UK lub wykazania, że przetwarzanie jest zgodne z tymi zasadami, uznaje się za zgodne z pierwotnym celem. Wyżej wymienione sytuacje nadal odpowiadają temu, co również w rozporządzeniu (UE) 2016/679 uznaje się za zgodne z przepisami dalsze przetwarzanie.
- (31) Po trzecie, ustawa o wykorzystaniu danych i dostępie do danych wprowadza również w art. 8A ust. 3 lit. d) RODO UK nowe, dodatkowe sytuacje, w których dalsze przetwarzanie danych osobowych w nowym celu uznaje się za zgodne z pierwotnym celem. Sytuacje te, wymienione w załączniku 2 do RODO UK ⁽⁴⁴⁾, obejmują na przykład sytuacje, w których przetwarzanie odbywa się w odpowiedzi na żądanie otrzymane przez organ publiczny, który potrzebuje danych do celów wykonania zadania realizowanego w interesie publicznym, mającego podstawę prawną zgodną z art. 6 ust. 3 RODO UK, w przypadku gdy przetwarzanie jest niezbędne do ochrony bezpieczeństwa publicznego, reagowania na sytuację nadzwyczajną, wykrywania przestępstw i zapobiegania im, prowadzenia postępowań przygotowawczych, ochrony żywotnych interesów osoby, której dane dotyczą, i innych osób, ochrony osób wymagających szczególnego traktowania, do celów podatkowych lub jeżeli jest to konieczne do wypełnienia obowiązku prawnego ⁽⁴⁵⁾.
- (32) Ustawa o wykorzystaniu danych i dostępie do danych rozszerza wprawdzie tym samym wykaz sytuacji, w których dalsze przetwarzanie w innym celu uznaje się za zgodne z pierwotnym celem przetwarzania, jednak rozszerzenie to podlega istotnym ograniczeniom. Po pierwsze, jest to ograniczone do konkretnych sytuacji, które są wymienione w sposób wyczerpujący w ustawie. Po drugie, dotyczy to wyłącznie obszarów, w których istnieje wyraźny interes publiczny związany z czynnością przetwarzania, tj. w których dalsze przetwarzanie służy celom

⁽⁴¹⁾ Podobnie jak w rozporządzeniu (UE) 2016/679 elementy te obejmują wszelkie związki między pierwotnym a nowym celem, kontekst, w którym zebrano dane osobowe, w tym relację między osobą, której dane dotyczą, a administratorem, charakter przetwarzania oraz to, czy obejmuje ono szczególne kategorie danych, ewentualne konsekwencje zamierzonego przetwarzania dla osoby, której dane dotyczą, oraz istnienie odpowiednich zabezpieczeń.

⁽⁴²⁾ Zob. także art. 6 ust. 4 rozporządzenia (UE) 2016/679.

⁽⁴³⁾ Motyw 50 rozporządzenia (UE) 2016/679.

⁽⁴⁴⁾ Załącznik 2 wprowadza się do RODO UK za pośrednictwem załącznika 5 do ustawy o wykorzystaniu danych i dostępie do danych, zob. art. 71 ust. 6 tej ustawy.

⁽⁴⁵⁾ Zob. załącznik 5 do ustawy o wykorzystaniu danych i dostępie do danych.

wymienionym w art. 23 RODO UK (który odpowiada art. 23 rozporządzenia (UE) 2016/679). Nie można zatem powoływać się na nie do celów komercyjnych. Po trzecie, choć ustawa o wykorzystaniu danych i dostępie do danych przyznaje Sekretarzowi Stanu prawo do zmiany wykazu zawartego w załączniku 2 w drodze rozporządzenia⁽⁴⁶⁾, Sekretarz Stanu może dodać do tego wykazu nowe rodzaje przetwarzania jedynie wtedy, gdy przetwarzanie to jest ponownie konieczne do ochrony celu leżącego w interesie publicznym wymienionego w art. 23 ust. 1 lit. c)–j) RODO UK⁽⁴⁷⁾. Po czwarte, jeżeli zbieranie danych osobowych przez administratora opiera się na zgodzie osoby, której dane dotyczą, przetwarzanie w nowym celu w sytuacjach wymienionych w załączniku 2 uznaje się za zgodne z pierwotnym celem tylko wtedy, gdy nie można racjonalnie oczekiwać od administratora uzyskania nowej zgody od osoby, której dane dotyczą⁽⁴⁸⁾.

2.2.4. Prawa indywidualne

- (33) Zgodnie z ramami ochrony danych osobowych Zjednoczonego Królestwa osoby, których dane dotyczą, nadal korzystają z tych samych praw indywidualnych co na mocy rozporządzenia (UE) 2016/679 bez żadnych istotnych zmian⁽⁴⁹⁾, 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 51–54 decyzji wykonawczej (UE) 2021/1772.
- (34) Po pierwsze, w ustawie o wykorzystaniu danych i dostępie do danych wyjaśniono pewne warunki wykonywania tych praw. Z jednej strony w drodze zmiany art. 12 i wprowadzenia nowego art. 12A w RODO UK⁽⁵⁰⁾ określono terminy, w których administratorzy muszą odpowiedzieć na żądania osoby, której dane dotyczą. Dokładniej rzecz ujmując, art. 12 RODO UK zmieniono w taki sposób, że administrator nie jest już zobowiązany do przekazywania informacji na temat podjętych działań (lub powodów niepodjęcia żadnych działań) w odpowiedzi na żądanie osoby, której dane dotyczą, zgodnie z art. 15–22 RODO UK, „w terminie miesiąca od otrzymania żądania”, lecz „przed upływem mającego zastosowanie terminu”. Mający zastosowanie termin doprecyzowano w nowo wprowadzonym art. 12A RODO UK jako okres jednego miesiąca, począwszy od odpowiedniego momentu, tj. od dnia otrzymania żądania przez administratora, otrzymania przez administratora wszelkich informacji wymaganych w związku z żądaniem na podstawie art. 12 ust. 6 RODO UK lub uiszczenia opłaty, która została naliczona w związku z żądaniem na podstawie art. 12 ust. 5 RODO UK, w zależności od tego, która z tych dat jest późniejsza⁽⁵¹⁾. W art. 12A ust. 3 zezwala się ponadto administratorowi na przedłużenie mającego zastosowanie terminu o kolejne dwa miesiące, jeżeli jest to konieczne ze względu na złożoność żądań osoby, której dane dotyczą, lub liczbę takich żądań. Z drugiej strony, 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⁽⁵²⁾. 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”⁽⁵³⁾.

⁽⁴⁶⁾ Art. 8A ust. 5 RODO UK, wprowadzony art. 71 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁴⁷⁾ Art. 8A ust. 6 RODO UK, wprowadzony art. 71 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁴⁸⁾ Art. 8A ust. 4 lit. b) RODO UK, wprowadzony art. 71 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁴⁹⁾ W art. 31 ustawy o ofiarach i więźniach z 2024 r. (ustawa VAP) wprowadzono dodatkową podstawę w prawie do usunięcia danych przewidzianym w art. 17 RODO UK, zapewniając osobom, których dane dotyczą, prawo do żądania usunięcia ich danych osobowych przez administratorów danych, gdy były one przetwarzane w wyniku bezpodstawnego zarzutu przedstawionego przez osobę działającą w złej wierze. Osobę uznaje się za „działającą w złej wierze”, jeżeli została ona skazana za przestępstwo określone w art. 31 ust. 3 ustawy VAP (takie jak molestowanie) lub podlega nakazowi ochrony przed uporczywym nękanieniem. Ustawa VAP jest dostępna pod następującym adresem: <https://www.legislation.gov.uk/ukpga/2024/21/contents>. Ponadto art. 77 ustawy o wykorzystaniu danych i dostępie do danych zmienia prawo do informacji przewidziane w art. 13 RODO UK w taki sposób, że administrator nie jest już zobowiązany do informowania osoby, której dane dotyczą, o dalszym przetwarzaniu jej danych osobowych w nowym celu, jeżeli celem tym są badania naukowe lub historyczne, cele archiwalne w interesie publicznym lub cele statystyczne, przetwarzanie odbywa się zgodnie ze szczególnymi zabezpieczeniami określonymi w nowym art. 84B RODO UK, a przekazanie informacji byłoby niemożliwe lub nieproporcjonalne.

⁽⁵⁰⁾ Art. 76 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁵¹⁾ Art. 12A ust. 1 i 2 RODO UK, wprowadzone art. 76 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁵²⁾ Art. 15 ust. 1A RODO UK, wprowadzony art. 78 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁵³⁾ Dawson-Damer v Taylor Wessing LLP [2017] EWCA Civ 74.

- (35) W związku z tym, chociaż terminy udzielania odpowiedzi na żądania osób, których dane dotyczą, oraz szczególne obowiązki administratorów danych w odniesieniu do prawa dostępu podlegają bardziej szczegółowym przepisom, system Zjednoczonego Królestwa nadal zapewnia rozpatrywanie żądań osób, których dane dotyczą, 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 ⁽⁵⁴⁾.
- (36) Ograniczenia tych praw indywidualnych określone w DPA 2018 i wpisujące się w ramy art. 23 RODO UK, a także ograniczenia i zabezpieczenia, które regulują stosowanie tych ograniczeń, nadal obowiązują w ramach prawnych Zjednoczonego Królestwa ⁽⁵⁵⁾, jak opisano szczegółowo w motywach 55–67 decyzji wykonawczej (UE) 2021/1772.
- (37) W szczególności w odniesieniu do ograniczenia dotyczącego danych osobowych przetwarzanych do celów utrzymania skutecznej kontroli imigracyjnej lub prowadzenia postępowań przygotowawczych lub wykrywania działań, które mogłyby zagrozić utrzymaniu skutecznej kontroli imigracyjnej, w zakresie, w jakim stosowanie tych przepisów mogłoby zaszkodzić którejkolwiek z tych kwestii (wyłączenie dotyczące imigracji) ⁽⁵⁶⁾, rząd Zjednoczonego Królestwa zmienił pkt 4 załącznika 2 do DPA 2018 w drodze rozporządzenia z 2022 r. w sprawie zmiany załącznika 2 do DPA 2018 ⁽⁵⁷⁾ oraz rozporządzenia z 2024 r. w sprawie zmiany załącznika 2 do DPA 2018 ⁽⁵⁸⁾, które uzupełniają rozporządzenie z 2022 r. ⁽⁵⁹⁾ Zmiany te włączają do pkt 4A i 4B załącznika 2 do DPA 2018 zabezpieczenia dotyczące korzystania z wyłączenia dotyczącego imigracji wymagane na mocy art. 23 ust. 2 RODO UK. W szczególności zawierają one wymogi, aby (i) na wyłączenie dotyczące imigracji można było powoływać się wyłącznie w indywidualnych przypadkach, oddzielnie w odniesieniu do każdego z odpowiednich przepisów RODO UK i ponownie za każdym razem, gdy Sekretarz Stanu rozważy niestosowanie lub ograniczenie stosowania któregośkolwiek z odpowiednich przepisów RODO UK ⁽⁶⁰⁾, (ii) przy korzystaniu z wyłączenia dotyczącego imigracji uwzględniano prawa i wolności osoby, której dane dotyczą, oraz potencjalną podatność na zagrożenia ⁽⁶¹⁾, (iii) Sekretarz Stanu prowadził rejestr korzystania z wyłączenia dotyczącego imigracji i informował osobę, której dane dotyczą, o jego wykorzystaniu (z wyjątkiem szczególnych okoliczności, w których informacje te naruszałyby cel wyłączenia) ⁽⁶²⁾ oraz (iv) aby jasno określono, że korzystanie z wyłączenia dotyczącego imigracji jest ograniczone do przetwarzania danych osobowych przez Sekretarza Stanu ⁽⁶³⁾, tj. w praktyce – przez Ministerstwo Spraw Wewnętrznych, na potrzeby wykonywania funkcji istotnych dla pkt 4 ppkt 1 załącznika 2 do DPA 2018. Ponadto wyjaśniają one również proces wagi interesów, który należy przeprowadzić przy ustalaniu, czy wykonywanie praw osób, których dane dotyczą, może zaszkodzić skutecznej kontroli imigracyjnej, oraz czy ograniczenie takich praw jest w rezultacie konieczne i proporcjonalne.

⁽⁵⁴⁾ 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/>.

⁽⁵⁵⁾ Art. 88 ust. 2 ustawy o wykorzystaniu danych i dostępie do danych wprowadza niewielką zmianę w art. 26 ust. 2 lit. f) DPA 2018 (wyłączenie dotyczące bezpieczeństwa narodowego i obronności), wyjaśniającą, że prawo do wniesienia skargi do Komisarza na podstawie art. 77 RODO UK nie jest częścią przepisów, których stosowanie może zostać ograniczone ze względów bezpieczeństwa narodowego lub obronności.

⁽⁵⁶⁾ W dniu przyjęcia decyzji wykonawczej (UE) 2021/1772 ważność i wykładnia wyłączenia dotyczącego imigracji na mocy prawa Zjednoczonego Królestwa nie były jeszcze rozstrzygnięte w następstwie orzeczenia sądu apelacyjnego dla Anglii i Walii z dnia 26 maja 2021 r., w którym stwierdzono, że wyłączenie dotyczące imigracji, w postaci, w jakiej było wówczas ujęte w DPA 2018, było niezgodne z prawem Zjednoczonego Królestwa, ponieważ brakowało w nim przepisów szczegółowych określających zabezpieczenia wymienione w art. 23 ust. 2 RODO UK, który odzwierciedla art. 23 ust. 2 rozporządzenia (UE) 2016/679. Z tego powodu dane osobowe przekazane do celów kontroli imigracyjnej Zjednoczonego Królestwa lub w inny sposób objęte wyłączeniem dotyczącym imigracji zostały wyłączone z zakresu stosowania decyzji wykonawczej (UE) 2021/1772.

⁽⁵⁷⁾ Rozporządzenie to weszło w życie w dniu 31 stycznia 2022 r. i jest dostępne pod następującym adresem: <https://www.legislation.gov.uk/uksi/2022/76/contents/made>.

⁽⁵⁸⁾ Rozporządzenie to weszło w życie w dniu 8 marca 2024 r. i jest dostępne pod następującym adresem: <https://www.legislation.gov.uk/uksi/2024/342/contents/made>.

⁽⁵⁹⁾ Wyłączenie dotyczące imigracji zmienione rozporządzeniem z 2022 r. ponownie zakwestionowano w drodze kontroli sądowej, ponieważ nie spełniało jeszcze wszystkich wymogów art. 23 ust. 2 RODO UK. W grudniu 2023 r. sąd apelacyjny uznał je za niezgodne z wymogami art. 23 ust. 2 RODO UK. W wyniku tego wyroku przyjęto rozporządzenie z 2024 r., uzupełniające rozporządzenie z 2022 r. i wprowadzające dalsze zmiany do wyłączenia dotyczącego imigracji.

⁽⁶⁰⁾ Pkt 4A ppkt 2 załącznika 2 do DPA 2018.

⁽⁶¹⁾ Pkt 4AB ppkt 3 i 4 załącznika 2 do DPA 2018. W sprawie projektu rozporządzenia z 2024 r. skonsultowano się z Biurem Komisarza ds. Informacji, które publicznie stwierdziło, że jest z niego zadowolone. Pismo opublikowane w odpowiedzi na konsultacje i potwierdzające wydaną opinię jest dostępne pod następującym adresem: <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/>.

⁽⁶²⁾ Pkt 4B ppkt 1 i 2 załącznika 2 do DPA 2018.

⁽⁶³⁾ Pkt 4 ppkt 1 załącznika 2 do DPA 2018.

- (38) Ponadto Komisarz ds. Informacji Zjednoczonego Królestwa wydał szczegółowe wytyczne dotyczące stosowania tego konkretnego ograniczenia⁽⁶⁴⁾. W wytycznych stwierdza się w szczególności, że „nie należy stosować wyłączenia dotyczącego imigracji jako ogólnego wyłączenia w celu ograniczenia [...] praw w odniesieniu do wszystkich posiadanych danych. Zakres stosowania wyłączenia jest ograniczony do tych praw, których wykonanie w odniesieniu do posiadanych danych stanowiłoby uszczerbek dla określonych celów w zakresie imigracji. [...] W związku z tym domyślne stanowisko administratora powinno polegać na zachowaniu zgodności z wymogami rozporządzenia (UE) 2016/679 i ustawy o ochronie danych w największym możliwym stopniu. [...] Test uszczerbku ma wysoki próg i nie należy stosować zwolnienia w sposób ogólny. [...] Należy rozważyć, czy zastosowanie wyłączenia jest proporcjonalną odpowiedzią na żądanie osoby fizycznej o ochronę danych. Można uznać, że istnieje nadrzędna potrzeba społeczna zastosowania wyłączenia dotyczącego imigracji, ale należy również wziąć pod uwagę, czy przeważa ona nad obowiązkiem wobec osób fizycznych wynikającym z rozporządzenia (UE) 2016/679. Osobom tym przysługują prawa w odniesieniu do ich danych osobowych, które należy uwzględnić w każdych okolicznościach, szczególnie prawo dostępu. W każdym przypadku ważne jest zatem, aby rozważyć, czy prawa osoby fizycznej do ochrony danych są nadrzędne wobec określonego ryzyka uszczerbku. Zastosowanie wyłączenia musi być proporcjonalne do okoliczności i konieczne jest staranne rozważenie i udokumentowanie każdego przypadku”.
- (39) Ogólnie rzecz biorąc, ograniczenie imigracyjne przewidziane w pkt 4 załącznika 2 do DPA 2018 zmienionego przez rząd Zjednoczonego Królestwa w latach 2022 i 2024 oraz zgodne z wykładnią wynikającą z orzecznictwa⁽⁶⁵⁾ i wytycznych Komisarza ds. Informacji podlega szeregowi rygorystycznych warunków, które regulują jego stosowanie i są bardzo podobne do warunków określonych w prawie Unii, w szczególności w art. 23 rozporządzenia (UE) 2016/679, w odniesieniu do ograniczenia praw i obowiązków w zakresie ochrony danych związanych z ważnymi celami interesu publicznego, takimi jak kontrola imigracyjna.

2.2.5. Ograniczenia dotyczące dalszego przekazywania danych

- (40) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii Europejskiej administratorom lub podmiotom przetwarzającym 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 rozporządzenia (UE) 2016/679, jak oceniono w motywach 74–82 decyzji wykonawczej (UE) 2021/1772.
- (41) Ustawą o wykorzystaniu danych i dostępie do danych zmieniono wprowadzić rozdział 5 RODO UK dotyczący przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, jednak zachowano podstawowy wymóg, zgodnie z którym dane osobowe mogą być przekazywane do państwa trzeciego lub organizacji międzynarodowej wyłącznie w przypadku, gdy przekazanie odbywa się na podstawie (i) rozporządzeń zatwierdzających przekazanie (nowa terminologia dla „rozporządzeń stwierdzających odpowiedni stopień ochrony”), (ii) odpowiednich zabezpieczeń lub (iii) odstępstwa w szczególnych sytuacjach. Te ogólne zasady przekazywania danych znajdują odzwierciedlenie w nowym art. 44A zastępującym art. 44 RODO UK⁽⁶⁶⁾, 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 RODO UK.
- (42) W odniesieniu do konkretnie do rozporządzeń zatwierdzających przekazanie danych art. 45A ust. 2 RODO UK 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. 45A ust. 3 RODO UK możliwość, aby przy wydawaniu takich rozporządzeń Sekretarz Stanu uwzględnił potrzebę ułatwienia przepływu danych, jest zawsze uzależniona od spełnienia warunków testu ochrony danych. Standard prawny dla spełnienia warunków testu ochrony danych sformułowany w nowym art. 45B ust. 1 RODO UK, 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. W art. 45B ust. 2 RODO UK 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

⁽⁶⁴⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/>.

⁽⁶⁵⁾ Korona na wniosek Open Rights Group i in. (powodowie), Korona przeciwko Secretary of State for the Home Department i in. [2019] EWHC 2562 (Admin), pkt 40 i 41.

⁽⁶⁶⁾ Art. 85 i załącznik 7 do ustawy o wykorzystaniu danych i dostępie do danych.

otrzymującą dane do innych państw lub organizacji międzynarodowych, odpowiednie zobowiązania międzynarodowe tego państwa lub tej organizacji oraz konstytucja, tradycje i kultura tego państwa lub tej organizacji. Chociaż nowy art. 45B ust. 2 stanowi przeformułowanie wykazu istotnych elementów przewidzianych w dawnym art. 45 RODO UK, zachowuje on podstawowe elementy tego wykazu i w związku z tym pozostaje zbliżony do tego, co przewidziano w rozdziale V rozporządzenia (UE) 2016/679. Ponadto władze Zjednoczonego Królestwa potwierdziły, że Sekretarz Stanu będzie uwzględniać elementy niewymienione w art. 45B 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. 45B ust. 2 RODO UK.

- (43) Rozporządzenia zatwierdzające przekazanie nadal podlegają „ogólnym” wymogom proceduralnym przewidzianym w art. 182 DPA 2018, jak określono w motywie 77 decyzji wykonawczej (UE) 2021/1772. W ramach tej procedury Sekretarz Stanu musi przeprowadzić konsultacje z Komisarzem ds. Informacji, gdy proponuje przyjęcie rozporządzenia Zjednoczonego Królestwa stwierdzającego odpowiedni stopień ochrony⁽⁶⁷⁾. 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⁽⁶⁸⁾.
- (44) Jeżeli chodzi o odpowiednie zabezpieczenia, w nowym art. 46 ust. 1A RODO UK określono, że takie przekazywanie danych może nastąpić wyłącznie wtedy, gdy w instrumentach dostępnych na podstawie art. 46 ust. 2 i 3⁽⁶⁹⁾ RODO UK przewidziano odpowiednie zabezpieczenia, a administrator, podmiot przetwarzający lub odpowiednie organy publiczne, działając w sposób racjonalny i proporcjonalny, uznają, że test ochrony danych został zaliczony. Nowo dodane ust. 6 i 7 wyjaśniają, 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, tj. jak ma to miejsce w przypadku rozporządzenia (UE) 2016/679, te same standardy prawne mają zastosowanie zarówno do rozporządzeń zatwierdzających przekazanie, jak i do odpowiednich zabezpieczeń. Zgodnie z tym samym ustępem kwestię tego, 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.
- (45) Jeżeli chodzi o odstępstwa w szczególnych sytuacjach, w art. 49 RODO UK dotyczącym warunków, na jakich można stosować wyjątki w szczególnych sytuacjach, wprowadzono szereg zmian technicznych, które dostosowują ten przepis do zmian w innych przepisach, ale nie wpływają na stopień ochrony danych osobowych w Zjednoczonym Królestwie. Ponadto dodano nowy ust. 4A w celu odtworzenia skutków art. 18 ust. 1 DPA 2018, przyznającego Sekretarzowi Stanu uprawnienia do określania, w drodze rozporządzeń, okoliczności, w jakich przekazywanie danych można uznać za niezbędne ze względu na interes publiczny. Wreszcie nowy art. 49A odtwarza skutki art. 18 ust. 2 DPA 2018, umożliwiając Sekretarzowi Stanu nakładanie, w drodze rozporządzeń, ograniczeń na przekazywanie danych, które nie zostało zatwierdzone na podstawie art. 45A (przekazywanie danych zatwierdzone rozporządzeniem), jeżeli uznano to za konieczne ze względu na ważny interes publiczny.
- (46) Jeżeli chodzi o wdrażanie przepisów Zjednoczonego Królestwa dotyczących międzynarodowego przekazywania danych, od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 nastąpił szereg zmian.

⁽⁶⁷⁾ 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>.

⁽⁶⁸⁾ W przypadku przyjęcia takiego wniosku w drodze głosowania rozporządzenie ostatecznie przestanie wywoływać jakiekolwiek dalsze skutki prawne.

⁽⁶⁹⁾ Instrument przekazywania danych dostępny na podstawie art. 46 ust. 2 i 3 RODO UK to prawnie wiążące i możliwe do wyegzekwowania instrumenty zawarte między organami lub podmiotami publicznymi, wiążące reguły korporacyjne zgodnie z art. 47 RODO UK, standardowe klauzule ochrony danych określone w rozporządzeniach wydanych przez Sekretarza Stanu lub określone w dokumencie wydanym przez Komisję ds. Informacji, zatwierdzony kodeks postępowania oraz zatwierdzony mechanizm certyfikacji.

- (47) Jeżeli chodzi o rozporządzenia zatwierdzające przekazanie, przyjęto dotychczas dwa takie nowe rozporządzenia, odpowiadające decyzjom stwierdzającym odpowiedni stopień ochrony, które obowiązują również w Unii, tj. w odniesieniu do przekazywania danych do Republiki Korei oraz w odniesieniu do przekazywania danych podmiotom handlowym, które zadeklarowały przestrzeganie rozszerzenia ram ochrony danych UE–USA na Zjednoczone Królestwo. Rozporządzenie stwierdzające odpowiedni stopień ochrony w odniesieniu do Republiki Korei ⁽⁷⁰⁾ weszło w życie w dniu 19 grudnia 2022 r. i umożliwia przekazywanie danych osobowych ze Zjednoczonego Królestwa do Republiki Korei. Rozszerzenie ram ochrony danych UE–USA na Zjednoczone Królestwo, w odniesieniu do którego odpowiednie rozporządzenie ⁽⁷¹⁾ weszło w życie w dniu 12 października 2023 r., umożliwia swobodny przepływ danych osobowych do certyfikowanych amerykańskich organizacji.
- (48) W odniesieniu do odpowiednich zabezpieczeń Zjednoczone Królestwo opublikowało własne standardowe klauzule umowne dotyczące ochrony danych, międzynarodową umowę o przekazywaniu danych (IDTA) ⁽⁷²⁾ oraz addendum do standardowych klauzul umownych UE, które weszły w życie w marcu 2022 r. Międzynarodowa umowa o przekazywaniu danych przewiduje mechanizm zapewniania odpowiednich zabezpieczeń przy przekazywaniu danych osobowych, szczególnie dla Zjednoczonego Królestwa, ale pod wieloma względami podobny do standardowych klauzul umownych UE. Addendum, wydane przez Komisarza ds. Informacji, umożliwia administratorom danych i podmiotom przetwarzającym w Zjednoczonym Królestwie opieranie się na standardowych klauzulach umownych UE na podstawie RODO UK w odniesieniu do międzynarodowego przekazywania danych. Komisarz ds. Informacji wydał również narzędzie oceny ryzyka związanego z przekazaniem, aby wesprzeć brytyjskie organizacje w ocenie ryzyka związanego z międzynarodowym przekazywaniem danych.
- (49) Zjednoczone Królestwo usprawniło również proces zatwierdzania wiążących reguł korporacyjnych za pomocą nowych wytycznych i nowych wariantów zatwierdzania tych reguł. W lipcu 2022 r. Komisarz ds. Informacji opublikował wytyczne i tabele referencyjne w celu wyjaśnienia podejścia Zjednoczonego Królestwa do wiążących reguł korporacyjnych po brexicie, a w grudniu 2023 r. opublikowano addendum do wiążących reguł korporacyjnych UE w celu zapewnienia, aby w Zjednoczonym Królestwie można było egzekwować reguły zatwierdzone na podstawie unijnych ram ⁽⁷³⁾.
- (50) Wreszcie w lipcu 2023 r. Zjednoczone Królestwo stało się członkiem stowarzyszonym Światowego Forum ds. Transgranicznych Zasad Ochrony Prywatności (CBPR) ⁽⁷⁴⁾. Co ważne, członkostwo to nie pociąga za sobą żadnych ułatwień w przekazywaniu danych ze Zjednoczonego Królestwa do innych członków Forum CBPR. Zjednoczone Królestwo wyjaśniło, że wszelkie przekazywanie danych osobowych ze Zjednoczonego Królestwa do państw trzecich lub organizacji międzynarodowych musi spełniać warunki określone w przepisach Zjednoczonego Królestwa, jak opisano powyżej, w szczególności dotyczące testu ochrony danych, który wymaga, aby zapewniane standardy ochrony nie były „znacznie niższe” niż standardy określone w RODO UK.
- (51) Jak już wyjaśniła Komisja, CBPR nie zapewniają wystarczającego stopnia ochrony danych osobowych pochodzących z UE. W szczególności nie przewidują możliwych do wyegzekwowania praw indywidualnych ⁽⁷⁵⁾. W związku z tym szczególnie ważne jest, nawet jeśli Zjednoczone Królestwo jest członkiem stowarzyszonym Światowego Forum CBPR, że CBPR nie mogą stanowić ważnego mechanizmu przekazywania danych na mocy prawa Zjednoczonego Królestwa o ochronie danych. Gdyby miało to ulec zmianie, podważyłoby to obecnie gwarantowany stopień ochrony danych osobowych przekazywanych z UE do Zjednoczonego Królestwa. W związku z tym Komisja będzie nadal uważnie monitorować dalszy rozwój sytuacji w tym zakresie.

⁽⁷⁰⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/ukxi/2022/1213/made>.

⁽⁷¹⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/ukxi/2023/1028/made>.

⁽⁷²⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/>.

⁽⁷³⁾ Po brexicie Komisarz ds. Informacji otrzymał znaczną liczbę wniosków dotyczących brytyjskich wiążących reguł korporacyjnych. Wielu zatwierdzonych wiążących reguł korporacyjnych nie dało się już stosować, ponieważ tylko te wiążące reguły korporacyjne, w przypadku których Komisarz ds. Informacji był zaangażowany w proces zatwierdzania, można było nadal stosować po brexicie, ale ich posiadacze byli zobowiązani do przedłożenia Komisarzowi ds. Informacji zaktualizowanej dokumentacji dotyczącej wiążących reguł korporacyjnych zgodnej z RODO UK.

⁽⁷⁴⁾ Forum CBPR składa się ze Stanów Zjednoczonych Ameryki, Kanady, Japonii, Republiki Korei, Filipin, Singapuru, Tajwanu i Australii, natomiast Mauritius, Międzynarodowe Centrum Finansowe w Dubaju i Bermudy są członkami stowarzyszonymi, podobnie jak Zjednoczone Królestwo.

⁽⁷⁵⁾ Zob. na przykład analiza porównawcza przeprowadzona przez organy ochrony danych grupy G-7 w odniesieniu do podstawowych elementów systemu certyfikacji RODO i systemu CBPR, która to analiza wykazała „znaczące różnice” między tymi systemami, w tym w zakresie „egzekwowalności i dochodzenia roszczeń na drodze prawnej, przepisów dotyczących niezależnego nadzoru i dostępu rządowego”). Dostęp pod adresem: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165>.

Zob. motyw 79 decyzji wykonawczej Komisji (UE) 2019/419 z dnia 23 stycznia 2019 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzającej odpowiedni stopień ochrony danych osobowych przez Japonię na mocy ustawy o ochronie informacji osobowych, dostępnej pod następującym adresem: (Dz.U. L 76 z 19.3.2019, s. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).

Zob. także Grupa Robocza Art. 29, opinia 02/2014 w sprawie listy kontrolnej wymogów dla wiążących reguł korporacyjnych składanych do krajowych organów ochrony danych w UE oraz transgranicznych zasad ochrony prywatności składanych do pełnomocników APEC odpowiedzialnych za rozliczalność w zakresie transgranicznych zasad ochrony prywatności, 6 marca 2014 r.

2.2.6. Zautomatyzowane podejmowanie decyzji

- (52) Mimo że w ustawie o wykorzystaniu danych i dostępie do danych zachowano liczne elementy przepisów dotyczących zautomatyzowanego podejmowania decyzji ocenionych w motywie 54 decyzji wykonawczej (UE) 2021/1772, zmieniono nią niektóre aspekty tych przepisów.
- (53) Po pierwsze, w nowo wprowadzonym art. 22B RODO UK ustanowiono ogólny zakaz przetwarzania szczególnych kategorii danych osobowych (zdefiniowanych w art. 9 ust. 1 RODO UK) na potrzeby decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu, mających skutki prawne lub w podobnym stopniu istotne skutki dla osoby, której dane dotyczą. W przepisie tym określono jednak trzy wyjątki od tego zakazu, mające zastosowanie, gdy: osoba, której dane dotyczą, wyraziła wyraźną zgodę na takie przetwarzanie lub decyzja jest niezbędna do zawarcia lub wykonania umowy między administratorem a osobą, której dane dotyczą lub przetwarzanie jest wymagane lub dozwolone przez prawo. W dwóch ostatnich przypadkach zautomatyzowane przetwarzanie musi być konieczne ze względu na istotny interes publiczny⁽⁷⁶⁾. Ogólny zakaz nie ma zastosowania do istotnych decyzji opartych na zautomatyzowanym przetwarzaniu kategorii danych innych niż kategorie szczególne.
- (54) Ponadto w nowym art. 22A RODO UK 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. 22A RODO UK wyjaśniono również, że „istotna decyzja” to decyzja, która wywołuje skutki prawne lub podobnie znaczące skutki dla osoby, której dane dotyczą⁽⁷⁷⁾.
- (55) Po drugie, w nowo wprowadzonym art. 22C RODO UK zobowiązano administratorów do wdrożenia środków służących zapewnieniu odpowiednich zabezpieczeń w odniesieniu do wszelkich istotnych decyzji opartych w całości lub w części na danych osobowych i opartych wyłącznie na zautomatyzowanym przetwarzaniu (w tym kategorii danych osobowych innych niż kategorie szczególne). Zabezpieczenia te muszą obejmować przekazywanie osobie, której dane dotyczą, informacji na temat procesu decyzyjnego, umożliwienie tej osobie zakwestionowania decyzji i składania oświadczeń oraz zapewnienie, że może ona uzyskać udział człowieka w procesie decyzyjnym⁽⁷⁸⁾.
- (56) Ponadto w nowo wprowadzonym art. 22D RODO UK przyznano Sekretarzowi Stanu uprawnienia do wydawania aktów wykonawczych w celu opisania, co stanowi znaczące zaangażowanie człowieka, a co nie, oraz jakie decyzje uznaje się za mające podobnie znaczące 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⁽⁷⁹⁾. Co ważne, przed przyjęciem nowego rozporządzenia zgodnie z art. 22D RODO UK Sekretarz Stanu musi skonsultować się z Komisarzem ds. Informacji⁽⁸⁰⁾, a rozporządzenie takie nie może zmieniać art. 22C RODO UK⁽⁸¹⁾ i podlega procedurze zatwierdzenia (ang. *affirmative resolution*)⁽⁸²⁾, co oznacza, że do jego przyjęcia wymagane jest zatwierdzenie przez obie izby parlamentu Zjednoczonego Królestwa.
- (57) 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 kluczowym zabezpieczeniom wymagającym prawa do uzyskania interwencji ludzkiej we wszystkich przypadkach podejmowania istotnych decyzji wyłącznie w oparciu o zautomatyzowane przetwarzanie, tj. na podstawie przetwarzania wrażliwych i niewrażliwych danych

⁽⁷⁶⁾ Art. 22B RODO UK, wprowadzony art. 80 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁷⁷⁾ Art. 22A RODO UK, wprowadzony art. 80 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁷⁸⁾ Art. 22C RODO UK, wprowadzony art. 80 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁷⁹⁾ Art. 22D RODO UK, wprowadzony art. 80 ust. 1 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. 22C.

⁽⁸⁰⁾ Art. 182 ust. 2 DPA 2018.

⁽⁸¹⁾ Art. 22D ust. 4 RODO UK.

⁽⁸²⁾ Art. 22D ust. 5 RODO UK.

osobowych⁽⁸³⁾. Ponadto, jak zauważyła Komisja we wcześniejszych decyzjach stwierdzających odpowiedni stopień ochrony⁽⁸⁴⁾, przepisy szczegółowe dotyczące zautomatyzowanego podejmowania decyzji zawarte w RODO UK prawdopodobnie nie będą miały wpływu na stopień ochrony danych osobowych przekazywanych z Unii do Zjednoczonego Królestwa. Jeżeli chodzi o dane osobowe zebrane w Unii, wszelkie decyzje opierające się na zautomatyzowanym przetwarzaniu podejmowane są zazwyczaj przez administratora w Unii (który ma bezpośrednie powiązanie z zainteresowaną osobą, której dane dotyczą), w związku z czym podlegają przepisom rozporządzenia (UE) 2016/679.

2.3. Nadzór i egzekwowanie przepisów

2.3.1. *Niezależny nadzór*

- (58) W Zjednoczonym Królestwie nadzór i egzekwowanie zgodności z ramami ochrony danych nadal sprawuje niezależny organ nadzorczy odpowiedzialny za ochronę danych, jak przeanalizowano w motywach 85–91 decyzji wykonawczej (UE) 2021/1772. 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.
- (59) 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⁽⁸⁵⁾. Ustawa przewiduje również możliwość, aby w okresie przejściowym Komisarz ds. Informacji objął funkcje przewodniczącego Komisji ds. Informacji, będącego jednym z jej członków niewykonawczych⁽⁸⁶⁾. 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⁽⁸⁷⁾ 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⁽⁸⁸⁾.
- (60) 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 87–90 decyzji wykonawczej (UE) 2021/1772⁽⁸⁹⁾. 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⁽⁹⁰⁾. 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⁽⁹¹⁾. Członkowie wykonawczy są pracownikami Komisji ds. Informacji zatrudnionymi na zasadach i warunkach określonych przez członków niewykonawczych⁽⁹²⁾. 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⁽⁹³⁾.
- (61) 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

⁽⁸³⁾ Art. 22C ust. 2 RODO UK, wprowadzony art. 80 ust. 1 ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁸⁴⁾ Zob. na przykład motyw 94 decyzji wykonawczej (UE) 2019/419 oraz motyw 81 decyzji wykonawczej Komisji (UE) 2022/254 z dnia 17 grudnia 2021 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzającej odpowiedni stopień ochrony danych osobowych przez Republikę Korei na mocy ustawy o ochronie danych osobowych (Dz.U. L 44 z 24.2.2022, s. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).

⁽⁸⁵⁾ Pkt 3 ppkt 1 załącznika 12A do DPA 2018.

⁽⁸⁶⁾ Art. 117, 118, 119 i 120 wraz z załącznikiem 14 do ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁸⁷⁾ Pkt 13 i 14 załącznika 12A do DPA 2018.

⁽⁸⁸⁾ Pkt 16 załącznika 12A do DPA 2018.

⁽⁸⁹⁾ Art. 52 RODO UK, a także załącznik 12A do DPA 2018, wprowadzony art. 114A projektu ustawy o wykorzystaniu danych i dostępie do danych.

⁽⁹⁰⁾ Pkt 5 ppkt 1 i pkt 3 ppkt 2 załącznika 12A do DPA 2018.

⁽⁹¹⁾ Pkt 3 ppkt 2, pkt 5 i pkt 6 załącznika 12A do DPA 2018.

⁽⁹²⁾ Pkt 11 załącznika 12A do DPA 2018.

⁽⁹³⁾ Pkt 5 ppkt 2 załącznika 12A do DPA 2018.

spełnił szczegółowych wymogów informacyjnych w odniesieniu do potencjalnych konfliktów interesów lub nie jest w stanie, nie jest zdolny lub nie chce pełnić swoich funkcji⁽⁹⁴⁾. 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⁽⁹⁵⁾.

- (62) Główną rolą Komisji ds. Informacji nadal będzie monitorowanie i egzekwowanie ram ochrony danych w Zjednoczonym Królestwie „w celu ochrony podstawowych praw i wolności” osób fizycznych⁽⁹⁶⁾. Jeżeli chodzi o funkcję Komisji ds. Informacji polegającą na zapewnieniu odpowiedniego stopnia ochrony danych osobowych, w ustawie o wykorzystaniu danych i dostępie do danych wyraźnie nałożono na Komisję ds. Informacji obowiązek uwzględniania interesów osób, których dane dotyczą, administratorów i innych podmiotów, kwestii leżących w ogólnym interesie publicznym oraz propagowania zaufania publicznego do przetwarzania danych osobowych⁽⁹⁷⁾. Cele te wymieniono również w motywie 7 rozporządzenia (UE) 2016/679.
- (63) Ponadto w ustawie o wykorzystaniu danych i dostępie do danych określono, że Komisja ds. Informacji uwzględnia podczas wykonywania swoich funkcji na mocy przepisów o ochronie danych propagowanie 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⁽⁹⁸⁾. Prawo UE o ochronie danych również uznaje potrzebę równoważenia ochrony danych osobowych z szeregiem innych praw podstawowych oraz celów, takich jak postęp gospodarczy i społeczny, bezpieczeństwo i sprawiedliwość oraz swoboda prowadzenia działalności gospodarczej⁽⁹⁹⁾.

2.3.2. Egzekwowanie przepisów, w tym sankcje

- (64) Uprawnienia i zadania Komisji ds. Informacji nadal odpowiadają uprawnieniom i zadaniom organów nadzorczych odpowiedzialnych za ochronę danych państw członkowskich zgodnie z odpowiednimi artykułami rozporządzenia (UE) 2016/679⁽¹⁰⁰⁾, jak oceniono w motywach 91–95 decyzji wykonawczej (UE) 2021/1772.
- (65) Ustawą o wykorzystaniu danych i dostępie do danych wprowadzono pewne wyjaśnienia dotyczące wykonywania niektórych z tych uprawnień.
- (66) Z jednej strony ustawa o wykorzystaniu danych i dostępie do danych wyjaśnia, że Komisja ds. Informacji może wymagać konkretnych „dokumentów” i „informacji” przy korzystaniu z uprawnień w zakresie zawiadomienia informacyjnego⁽¹⁰¹⁾. Z drugiej strony ustawą o wykorzystaniu danych i dostępie do danych wprowadzono dwa nowe uprawnienia dochodzeniowe Komisji ds. Informacji: nowe uprawnienie do żądania sprawozdania⁽¹⁰²⁾ i nowe uprawnienie do wydania administratorowi „wezwania na przesłuchanie” w przypadku podejrzenia naruszenia RODO UK lub DPA 2018⁽¹⁰³⁾.

⁽⁹⁴⁾ Pkt 7 ppkt 6 i 7 załącznika 12A do DPA 2018.

⁽⁹⁵⁾ Pkt 9 ppkt 6, 7, 8 i 9 załącznika 12A do DPA 2018.

⁽⁹⁶⁾ Art. 51 RODO UK.

⁽⁹⁷⁾ Art. 91 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 120A DPA 2018.

⁽⁹⁸⁾ Art. 91 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 120B DPA 2018. Ustawą o wykorzystaniu danych i dostępie do danych wprowadzono do DPA 2018 nowy art. 120C, zgodnie z którym Komisja ds. Informacji jest zobowiązana do przygotowania i opublikowania strategii odzwierciedlającej między innymi sposób, w jaki uwzględni ona wyżej wymienione kwestie oraz wspieranie wzrostu gospodarczego przy wykonywaniu swoich funkcji regulacyjnych.

⁽⁹⁹⁾ Zob. w szczególności motyw 2 i 4 oraz art. 23 rozporządzenia (UE) 2016/679.

⁽¹⁰⁰⁾ Art. 57 i 58 RODO UK.

⁽¹⁰¹⁾ Art. 97 ustawy o wykorzystaniu danych i dostępie do danych, zmieniający art. 142 DPA 2018. Rozważania dotyczące wpływu technologii i roli ochrony danych w budowaniu zaufania do gospodarki cyfrowej są częścią działań organów regulacyjnych ds. ochrony danych zarówno w Zjednoczonym Królestwie, jak i w UE. Zob. na przykład sprawozdanie roczne Europejskiej Rady Ochrony Danych za 2024 r., s. 12: „EROD jest dynamicznym organem opartym na współpracy, który odgrywa kluczową rolę w zapewnianiu spójnego stosowania przepisów o ochronie danych w całej Europie. Z perspektywy wiceprzewodniczącego postrzegam ją jako strażniczkę praw osób fizycznych do prywatności, umiejętnie równoważącą potrzeby w zakresie innowacji i wzrostu gospodarczego”.

⁽¹⁰²⁾ Art. 98 ustawy o wykorzystaniu danych i dostępie do danych, zmieniający art. 146 DPA 2018.

⁽¹⁰³⁾ Art. 100 ustawy o wykorzystaniu danych i dostępie do danych, wprowadzający art. 148A DPA 2018.

- (67) Jeżeli chodzi o wykonywanie tych uprawnień przez Komisję ds. Informacji, od czasu wejścia w życie decyzji wykonawczej (UE) 2021/1772 Komisarz ds. Informacji rozpatrywał rocznie około 40 000 skarg od osób, których dane dotyczą, co stanowi liczbę podobną do liczby skarg rozpatrywanych, gdy Zjednoczone Królestwo nadal było częścią Unii i stosowało rozporządzenie (UE) 2016/679⁽¹⁰⁴⁾. Komisarz ds. Informacji przeprowadzał również z urzędu dochodzenia dotyczące szerokiego zakresu sektorów i kwestii związanych z przestrzeganiem przepisów, w tym praw osób, których dane dotyczą⁽¹⁰⁵⁾.
- (68) Jeżeli chodzi o środki egzekucyjne, od czasu wejścia w życie decyzji wykonawczej (UE) 2021/1772 Komisarz wydał 120 nagan, 32 zawiadomienia informacyjne, 3 zawiadomienia oceniające, 12 zawiadomień egzekucyjnych, 2 ostrzeżenia i 12 grzywien⁽¹⁰⁶⁾. Obejmują one szereg znaczących kar pieniężnych nałożonych na podstawie RODO UK i DPA 2018. Na przykład w kwietniu 2023 r. Komisarz ds. Informacji nałożył na platformę mediów społecznościowych grzywnę w wysokości 12,7 mln GBP za niewłaściwe wykorzystywanie danych dzieci⁽¹⁰⁷⁾. W marcu 2025 r. przedsiębiorstwo programistyczne zostało ukarane grzywną w wysokości 3,07 mln GBP za uchybienia w zakresie bezpieczeństwa, które narażały dane osobowe ponad 70 000 osób⁽¹⁰⁸⁾. Niedawno, w czerwcu 2025 r., Komisarz ds. Informacji nałożył grzywnę w wysokości 2,31 mln GBP na przedsiębiorstwo zajmujące się wykonywaniem badań genetycznych za niewdrożenie odpowiednich środków bezpieczeństwa w celu ochrony danych osobowych użytkowników ze Zjednoczonego Królestwa w następstwie cyberataku na dużą skalę w 2023 r.⁽¹⁰⁹⁾
- (69) Od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 Biuro Komisarza ds. Informacji opracowało i opublikowało również znaczną liczbę wskazówek, opinii i innych dokumentów zawierających wytyczne, w których wyjaśniono stosowanie przepisów o ochronie danych w ważnych obszarach, takich jak rozpoznawanie twarzy, sprawiedliwość w działaniach sztucznej inteligencji, dane dzieci, marketing bezpośredni, monitoring wizyjny, prawo dostępu, przejrzystość w opiece zdrowotnej i społecznej itp., dla różnych odbiorców, w tym małych i średnich przedsiębiorstw, konkretnych podmiotów, takich jak szkoły, żłobki lub małe organy publiczne, a także dla ogółu przedsiębiorstw, ogółu społeczeństwa lub osób, których dane dotyczą⁽¹¹⁰⁾.

3. ISTOTNE ZMIANY DOTYCZĄCE DOSTĘPU DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII EUROPEJSKIEJ I ICH WYKORZYSTYWANIA PRZEZ ORGANY PUBLICZNE W ZJEDNOCZONYM KRÓLESTWIE

3.1. Ogólne ramy prawne

- (70) Zjednoczone Królestwo nadal jest członkiem Rady Europy, przestrzega europejskiej konwencji praw człowieka i podlega jurysdykcji Europejskiego Trybunału Praw Człowieka. W związku z tym nadal podlega obowiązkowi zapisanym w prawie międzynarodowym, jak opisano w motywach 116–119 decyzji wykonawczej (UE) 2021/1772, które określają ramy systemu dostępu rządowego do danych osobowych na podstawie zasad, zabezpieczeń i praw indywidualnych identycznych z tymi, które mają zastosowanie do 27 państw członkowskich jako stron EKPC i które w dużym stopniu znajdują odzwierciedlenie w odpowiednim orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej.
- (71) W DPA 2018 nadal gwarantuje się szczególne zabezpieczenia i prawa w zakresie ochrony danych, gdy dane są przetwarzane przez organy publiczne Zjednoczonego Królestwa, w tym przez organy ścigania i organy bezpieczeństwa narodowego, jak przeanalizowano w motywach 121–132 decyzji wykonawczej (UE) 2021/1772. Ustawą o wykorzystaniu danych i dostępie do danych wprowadzono jedynie ograniczone i ukierunkowane zmiany w częściach DPA 2018, które zawierają przepisy dotyczące przetwarzania danych osobowych w kontekście ścigania przestępstw (część 3 DPA 2018) i bezpieczeństwa narodowego (część 4 DPA 2018).

⁽¹⁰⁴⁾ Sprawozdania roczne Komisarza ds. Informacji za lata 2021–2022, 2022–2023 i 2023–2024. Zob. także decyzja wykonawcza (UE) 2021/1772, motyw 96.

⁽¹⁰⁵⁾ Sprawozdanie roczne Komisarza ds. Informacji za lata 2023–2024, s. 41.

⁽¹⁰⁶⁾ Sprawozdania roczne Komisarza ds. Informacji za lata 2021–2022, 2022–2023 i 2023–2024.

⁽¹⁰⁷⁾ Więcej informacji na temat tych i dalszych działań w zakresie egzekwowania przepisów można znaleźć na stronie internetowej Komisarza ds. Informacji, dostępnej pod adresem: <https://ico.org.uk/action-weve-taken/enforcement/>.

⁽¹⁰⁸⁾ Dalsze informacje są dostępne pod adresem: <https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/>.

⁽¹⁰⁹⁾ Dalsze informacje są dostępne pod adresem: <https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/>.

⁽¹¹⁰⁾ Dostęp pod adresem: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>.

- (72) W odniesieniu do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, w części 3 DPA 2018 nadal przewidziane są zasady, prawa i obowiązki podobne do tych określonych w dyrektywie (UE) 2016/680 ⁽¹¹¹⁾.
- (73) W szczególności w dniu przyjęcia niniejszej decyzji Komisja przyjęła decyzję na podstawie art. 36 ust. 3 dyrektywy (UE) 2016/680, w której ustaliła, że system ochrony danych mający zastosowanie do przetwarzania danych przez organy ścigania Zjednoczonego Królestwa do celów ścigania przestępstw nadal zapewnia stopień ochrony merytorycznie równoważny temu zagwarantowanemu w dyrektywie (UE) 2016/680.
- (74) 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 do celów 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 ⁽¹¹²⁾. 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).
- (75) 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 ⁽¹¹³⁾. 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 ⁽¹¹⁴⁾. Znajduje to również potwierdzenie w wytycznych Komisarza ds. Informacji w zakresie stosowania wyłączeń dotyczących bezpieczeństwa narodowego ⁽¹¹⁵⁾.
- (76) Ponadto na podstawie zmian wprowadzonych ustawą o wykorzystaniu danych i dostępie do danych ⁽¹¹⁶⁾ konkretne czynności przetwarzania prowadzone przez organy właściwe w zakresie ścigania przestępstw mogą również podlegać przepisom części 4 DPA 2018, która zwykle ma zastosowanie wyłącznie do przetwarzania danych przez organy bezpieczeństwa narodowego.

⁽¹¹¹⁾ Art. 69 ustawy o wykorzystaniu danych i dostępie do danych wprowadza definicję zgody i warunki korzystania ze zgody przewidziane w art. 4 pkt 11 i art. 7 RODO UK (które odzwierciedlają odpowiednie przepisy rozporządzenia (UE) 2016/679) jako nowe art. 33 ust. 1A i 40A do DPA 2018, precyzując tym samym pojęcie zgody i warunki korzystania ze zgody, gdy jest ona stosowana jako podstawa prawna przetwarzania danych osobowych przez właściwe organy do celów ścigania przestępstw. Ponadto art. 71 ust. 7 i 8 ustawy o wykorzystaniu danych i dostępie do danych w pewnym stopniu doprecyzowuje brzmienie art. 36 ust. 1 DPA 2018. Wreszcie, w stosownych przypadkach, zmiany w RODO UK wprowadzone ustawą o wykorzystaniu danych i dostępie do danych opisane w art. 2 znajdują również odzwierciedlenie w części 3 DPA 2018, zob. na przykład art. 74 ust. 2–5 dotyczący przetwarzania danych wrażliwych, art. 76 ust. 4–6 w odniesieniu do terminów udzielania odpowiedzi na żądania osoby, której dane dotyczą, art. 78 ust. 2 i 3 w odniesieniu do wyszukiwań w odpowiedzi na żądania osób, których dane dotyczą, oraz art. 80 ust. 3–5 dotyczący zautomatyzowanego podejmowania decyzji.

⁽¹¹²⁾ Art. 78A ust. 1 DPA 2018, wprowadzony art. 88 ustawy o wykorzystaniu danych i dostępie do danych. Zgodnie z art. 78A 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.

⁽¹¹³⁾ Zob. *Baker v Secretary of State for the Home Department* [2001] UKIT NSA2.

⁽¹¹⁴⁾ 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.

⁽¹¹⁵⁾ Zob. wytyczne Komisarza ds. Informacji na temat wyjątku dotyczącego bezpieczeństwa narodowego i obrony, dostępne pod adresem: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide>.

⁽¹¹⁶⁾ Art. 89–90 ustawy o wykorzystaniu danych i dostępie do danych.

- (77) System ochrony danych w odniesieniu do przetwarzania w kontekście bezpieczeństwa narodowego jest zatem w niektórych sytuacjach rozszerzony również na przetwarzanie danych przez organy ścigania, ma to jednak miejsce jedynie w szczególnych okolicznościach oraz podlega rygorystycznym warunkom i zabezpieczeniom, tj. jeżeli (i) właściwy organ jest określony jako „kwalifikujący się właściwy organ” w rozporządzeniu wydanym przez Sekretarza Stanu, które wymaga zatwierdzenia przez parlament ⁽¹¹⁷⁾, oraz (ii) Sekretarz Stanu wyznacza w drodze zawiadomienia konkretną czynność przetwarzania prowadzoną przez kwalifikujący się właściwy organ. Co ważne, takie wyznaczenie może mieć miejsce tylko wtedy, gdy Sekretarz Stanu uzna, że wyznaczenie czynności przetwarzania jest konieczne do celów ochrony bezpieczeństwa narodowego, tj. gdy organ ścigania działa w celach bezpieczeństwa narodowego, a przetwarzanie jest prowadzone przez kwalifikujący się właściwy organ jako współadministratora z co najmniej jedną służbą wywiadowczą ⁽¹¹⁸⁾. W ramach dalszych zabezpieczeń Sekretarz Stanu musi skonsultować się z Komisarzem ds. Informacji przed wysłaniem zawiadomienia o wyznaczeniu ⁽¹¹⁹⁾, tekst zawiadomienia musi co do zasady zostać opublikowany ⁽¹²⁰⁾, a osoba, której bezpośrednio dotyczy zawiadomienie o wyznaczeniu, może zwrócić się o kontrolę sądową ⁽¹²¹⁾. W związku z tym zmiana ta ma zasadniczo na celu wyjaśnienie, że w przypadku gdy organy Zjednoczonego Królestwa mają kompetencje zarówno w dziedzinie ścigania przestępstw, jak i bezpieczeństwa narodowego, a przetwarzają dane w kontekście tych drugich obowiązków, zastosowanie może mieć system ochrony danych dla służb bezpieczeństwa narodowego.
- (78) Część 4 DPA 2018 reguluje przetwarzanie danych przez służby wywiadowcze Zjednoczonego Królestwa. Nadal określa ona główne zasady ochrony danych i warunki przetwarzania szczególnych kategorii danych, zapewnia prawa osób, których dane dotyczą, zawiera wymóg uwzględniania ochrony danych w fazie projektowania oraz reguluje przekazywanie danych osobowych, jak opisano w motywach 125–132 decyzji wykonawczej (UE) 2021/1772.
- (79) Zmiany w tym systemie wprowadzone ustawą o wykorzystaniu danych i dostępie do danych są ograniczone. W odniesieniu do prawa dostępu osób, których dane dotyczą, przewidzianego w art. 94 DPA 2018, ustawą o wykorzystaniu danych i dostępie do danych wprowadzono nowy ust. 2A, wyjaśniający, że osoba, której dane dotyczą, ma prawo do odpowiednich informacji wyłącznie w zakresie, w jakim administrator jest w stanie je przekazać na podstawie rozsądnego i proporcjonalnego wyszukiwania ⁽¹²²⁾. Jak wyjaśniono w motywie 35, zmiana ta reguluje prawo dostępu na podstawie ustalonych standardów prawnych, które uwzględniają również interesy osoby, której dane dotyczą. Wprawdzie w obszarze zautomatyzowanego podejmowania decyzji administratorom nadal zakazuje się podejmowania decyzji mających znaczący wpływ na osobę, której dane dotyczą, w oparciu wyłącznie o zautomatyzowane przetwarzanie danych osobowych osoby, której dane dotyczą, chyba że taka decyzja jest wymagana lub dozwolona przez prawo, osoba, której dane dotyczą, wyraziła zgodę na podjęcie decyzji na tej podstawie lub decyzja podejmowana jest w kontekście umowy ⁽¹²³⁾, jednak ustawą o wykorzystaniu danych i dostępie do danych wprowadzono w części 4 DPA 2018 ⁽¹²⁴⁾ taką samą definicję pojęcia „decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu” jak ta zawarta w art. 22A RODO UK i przeanalizowana w motywie 53 niniejszej decyzji.

3.2. Istotne zmiany dotyczące dostępu organów publicznych Zjednoczonego Królestwa do danych na potrzeby ścigania przestępstw i wykorzystywania danych przez te organy w tym celu

- (80) W prawie Zjednoczonego Królestwa nadal nakłada się istotne ograniczenia na dostęp do danych osobowych i korzystanie z nich na potrzeby ścigania przestępstw, a także przewiduje się mechanizmy nadzoru i środki zaskarżenia w tym obszarze, jak przeanalizowano w motywach 134–174 decyzji wykonawczej (UE) 2021/1772.

⁽¹¹⁷⁾ Art. 82 ust. A1, 2A i 4 DPA 2018, wprowadzone art. 89 ust. 2 ustawy o wykorzystaniu danych i dostępie do danych.

⁽¹¹⁸⁾ Art. 82A ust. 1 i 2, wprowadzone art. 89 ust. 3 ustawy o wykorzystaniu danych i dostępie do danych. W ramach dodatkowego zabezpieczenia Sekretarz Stanu musi skonsultować się z Komisarzem przed wydaniem zawiadomienia o wyznaczeniu, zob. nowy art. 82A ust. 8 DPA 2018, tekst zawiadomienia musi co do zasady zostać opublikowany, zob. nowy art. 82D ust. 1, z zastrzeżeniem wyłączeń określonych w nowym art. 82D ust. 3 DPA 2018, a osoba, której bezpośrednio dotyczy zawiadomienie o wyznaczeniu, może zażądać kontroli sądowej, zob. nowy art. 82E DPA 2018.

⁽¹¹⁹⁾ Art. 82A ust. 8 DPA 2018.

⁽¹²⁰⁾ Art. 82D ust. 1, z zastrzeżeniem wyłączeń określonych w nowym art. 82D ust. 3 DPA 2018.

⁽¹²¹⁾ Art. 82E DPA 2018.

⁽¹²²⁾ Art. 78 ust. 4 ustawy o wykorzystaniu danych i dostępie do danych.

⁽¹²³⁾ Art. 96 DPA 2018.

⁽¹²⁴⁾ Zgodnie z nowym art. 96 ust. 4 DPA 2018 decyzja opiera się wyłącznie na zautomatyzowanym przetwarzaniu, jeżeli proces decyzyjny nie obejmuje możliwości przyjęcia decyzji, odrzucenia jej lub wpływania na nią przez człowieka. Zob. art. 80 ust. 4 lit. c) ustawy o wykorzystaniu danych i dostępie do danych.

3.2.1. Podstawy prawne i właściwe ograniczenia/zabezpieczenia

- (81) Zbieranie danych osobowych od podmiotów gospodarczych w Zjednoczonym Królestwie do celów ścigania przestępstw jest nadal dopuszczalne w porządku prawnym Zjednoczonego Królestwa na podstawie nakazów przeszukania i nakazów wydania dowodów, z zastrzeżeniem warunków i zabezpieczeń opisanych w motywach 135–138 decyzji wykonawczej (UE) 2021/1772.
- (82) Ponadto w ustawie o bezpieczeństwie narodowym z 2023 r. ⁽¹²⁵⁾, której celem jest przeciwdziałanie zagrożeniom dla bezpieczeństwa narodowego stwarzanym przez szpiegostwo, sabotaż i osoby działające na rzecz obcych mocarstw, wprowadzono nowe uprawnienia policji Zjednoczonego Królestwa w zakresie dostępu, przeszukania i zajęcia, w tym możliwość uzyskania danych osobowych, w przypadku gdy istnieją uzasadnione podstawy, by podejrzewać, że pozyskany zostanie materiał, który prawdopodobnie stanowi dowód, że popełniono lub ma zostać popełnione jedno z poważniejszych przestępstw lub działań obcego państwa zagrażających bezpieczeństwu narodowemu przewidzianych w ustawie o bezpieczeństwie narodowym z 2023 r. ⁽¹²⁶⁾. Uprawnienia te podlegają podobnym warunkom i zabezpieczeniom jak te przeanalizowane w decyzji wykonawczej (UE) 2021/1772 w odniesieniu do uprawnień istniejących w tamtym czasie. Do ich stosowania wymagane jest w szczególności uzyskanie zezwolenia w postaci nakazu przeszukania i zatrzymania, nakazu wydania dowodów lub nakazu wyjaśnienia wydanego przez niezależny organ sądowy na wniosek funkcjonariusza policji prowadzącego postępowanie przygotowawcze ⁽¹²⁷⁾. Istnieją szczególne zabezpieczenia dla materiałów poufnych, takich jak materiały dziennikarskie i elementy objęte poufnością wymiany informacji między prawnikiem a klientem ⁽¹²⁸⁾. Podobnie wydawanie nakazów ujawnienia ⁽¹²⁹⁾, nakazów dotyczących informacji o klientach ⁽¹³⁰⁾ i nakazów monitorowania rachunków ⁽¹³¹⁾, również ustanowionych w ustawie o bezpieczeństwie narodowym z 2023 r., podlega obowiązkowemu zatwierdzeniu przez sędziego na wniosek właściwego funkcjonariusza oraz szczególnym warunkom i zabezpieczeniom, w tym wymaganiom, aby wniosek o wydanie nakazu dotyczył konkretnej osoby, do celów śledztwa w sprawie działalności stanowiącej zagrożenie ze strony obcego państwa, aby nakaz ten zwiększał skuteczność śledztwa oraz aby nakaz ten nie był wykorzystywany do uzyskania informacji, które są objęte prawniczą tajemnicą zawodową lub w inny sposób wykluczonych, takich jak materiały dziennikarskie i niektóre dokumenty medyczne ⁽¹³²⁾.
- (83) Jak opisano w motywach 139–141 decyzji wykonawczej (UE) 2021/1772, w ramach prawnych Zjednoczonego Królestwa określone organy ścigania, na przykład Krajowa Agencja ds. Zwalczania Przestępczości lub Metropolitalna Służba Policyjna, mogą również korzystać z ukierunkowanych uprawnień dochodzeniowo-śledczych na mocy ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. (IPA 2016) ⁽¹³³⁾ do celów zapobiegania poważnym przestępstwom lub ich wykrywania. Szczególne uprawnienia dochodzeniowo-śledcze przysługujące wspomnianym organom ścigania to: ukierunkowane przechwytywanie (część 2 IPA 2016), ukierunkowane pozyskiwanie danych pochodzących z łączności (część 3 IPA 2016) oraz ukierunkowana ingerencja w urządzenia elektroniczne (część 5 IPA 2016). W przypadku gdy Sekretarz Stanu wydaje nakaz zatrzymywania danych na podstawie części 4 IPA 2016, organy ścigania mogą również korzystać z dostępu do zatrzymanych danych pochodzących z łączności dzięki uprawnieniom do pozyskiwania takich danych na podstawie części 3 IPA 2016.

⁽¹²⁵⁾ Dostęp pod adresem: <https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted>.

⁽¹²⁶⁾ Załącznik 2 do ustawy o bezpieczeństwie narodowym z 2023 r. Przestępstwami, o które chodzi w kontekście ustawy o bezpieczeństwie narodowym z 2023 r., są na przykład pozyskiwanie lub ujawnianie informacji chronionych (art. 1), pozyskiwanie lub ujawnianie tajemnicy przedsiębiorstwa (art. 3), pomoc zagranicznym służbom wywiadowczym (art. 4), prowadzenie sabotażu (art. 12) lub konkretne zabronione postępowanie obcego państwa z zamiarem wywołania skutku zakłócającego (art. 13).

⁽¹²⁷⁾ Zob. pkt 2 ppkt 1, pkt 3 ppkt 1, pkt 4 ppkt 1 i pkt 10 ppkt 1 załącznika 2 do ustawy o bezpieczeństwie narodowym z 2023 r.

⁽¹²⁸⁾ Zob. pkt 2 ppkt 4 lit. b), pkt 3 ppkt 4 lit. b) i c), pkt 4 ppkt 4 lit. b) i c) oraz pkt 10 ppkt 1 załącznika 2 do ustawy o bezpieczeństwie narodowym z 2023 r.

⁽¹²⁹⁾ W drodze nakazów ujawnienia na podstawie załącznika 3 do ustawy o bezpieczeństwie narodowym z 2023 r. funkcjonariusz może wezwać osobę do dostarczenia informacji, przedstawienia dokumentów lub udzielenia odpowiedzi na pytania istotne dla śledztwa w celu zidentyfikowania mienia związanego z działalnością stanowiącą zagrożenie ze strony obcego państwa, w tym z przemieszczaniem lub użytkowaniem mienia.

⁽¹³⁰⁾ W drodze nakazów dotyczących informacji o klientach na podstawie załącznika 4 do ustawy o bezpieczeństwie narodowym z 2023 r. funkcjonariusz może zażądać od instytucji finansowej dostarczenia wszelkich informacji o konkretnym kliencie.

⁽¹³¹⁾ W drodze nakazów monitorowania rachunków, o których mowa w załączniku 5, instytucja finansowa może zostać zobowiązana do przekazania funkcjonariuszowi informacji określonych w nakazie w sposób określony w nakazie i za okres określony w nakazie, nieprzekraczający 90 dni.

⁽¹³²⁾ Załącznik 3 pkt 2 ppkt 1, załącznik 4 pkt 1, załącznik 5 pkt 1 do ustawy o bezpieczeństwie narodowym z 2023 r.

⁽¹³³⁾ Ustawa o uprawnieniach dochodzeniowo-śledczych z 2016 r. (zob.: <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>) zastąpiła szereg ustaw dotyczących przechwytywania komunikacji, ingerencji w urządzenia elektroniczne oraz pozyskiwania danych pochodzących z łączności, w szczególności część I RIPA 2000, w której określono poprzednie ogólne ramy legislacyjne dotyczące korzystania z uprawnień dochodzeniowo-śledczych przez organy ścigania i bezpieczeństwa narodowego.

- (84) Od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 IPA 2016, wraz z ustawą regulującą uprawnienia dochodzeniowo-śledcze z 2000 r. (RIPA) w odniesieniu do Anglii, Walii i Irlandii Północnej oraz ustawą regulującą uprawnienia dochodzeniowo-śledcze w Szkocji z 2000 r. (RIPSA), nadal zapewnia podstawę prawną i określa obowiązujące ograniczenia i zabezpieczenia dotyczące korzystania z takich uprawnień, jak opisano w decyzji wykonawczej (UE) 2021/1772. Co ważne, zgodnie z obecnymi ramami prawnymi do skorzystania z tych uprawnień nadal wymagane jest uzyskanie nakazu (¹³⁴) wydanego przez właściwy organ (¹³⁵) i zatwierdzonego przez niezależnego komisarza sądowego (¹³⁶) (procedura „double-lock”). Uzyskanie takiego nakazu nadal wymaga przeprowadzenia analizy niezbędności i proporcjonalności (¹³⁷).
- (85) Jednocześnie od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych, która otrzymała zgodę królewską w kwietniu 2024 r., zmieniono niektóre szczególne elementy IPA 2016 (¹³⁸). W zakresie, w jakim te poprawki i inne istotne zmiany odnoszą się do warunków, ograniczeń i zabezpieczeń związanych z wykorzystaniem wyżej wymienionych szczególnych uprawnień dochodzeniowo-śledczych przez organy publiczne w Zjednoczonym Królestwie do celów ścigania przestępstw, jak oceniono w motywach 177–215 decyzji wykonawczej (UE) 2021/1772, przeanalizowano je w kolejnych punktach. W odniesieniu do elementów ram Zjednoczonego Królestwa, których nie zmieniono wyżej wymienioną ustawą ani na które nie miały wpływu inne istotne zmiany, analiza przeprowadzona w decyzji wykonawczej (UE) 2021/1772 jest nadal aktualna.
- (86) Jeżeli chodzi o ukierunkowane pozyskiwanie i zatrzymywanie danych pochodzących z łączności (¹³⁹), warunki i zabezpieczenia regulujące te uprawnienia, ocenione w decyzji wykonawczej (UE) 2021/1772, pozostają w mocy. Ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych doprecyzowano istniejące zabezpieczenia przez wprowadzenie do art. 11 IPA 2016 (w którym ustanawia się przestępstwo polegające na bezprawnym pozyskaniu danych pochodzących z łączności od operatora telekomunikacyjnego) wykazu przykładów tego, co należy rozumieć jako „zgodne z prawem upoważnienie” w tym przepisie (¹⁴⁰). Ponadto ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych doprecyzowano definicję danych pochodzących z łączności w art. 261 IPA 2016 przez wyraźne określenie, że dane abonenta kwalifikują się jako dane pochodzące z łączności (¹⁴¹).

(¹³⁴) W części 2 rozdział 2 IPA 2016 przewidziano ograniczoną liczbę przypadków, w których przechwytywanie można dokonać bez nakazu. Obejmuje to: przechwytywanie za zgodą nadawcy lub odbiorcy, przechwytywanie do celów administracyjnych lub egzekucyjnych, przechwytywanie prowadzone w określonych instytucjach (zakończonych karnych, szpitalach psychiatrycznych i imigracyjnych ośrodkach detencyjnych), jak również przechwytywanie dokonywane zgodnie z odpowiednią umową międzynarodową.

(¹³⁵) W większości przypadków organem wydającym nakazy na podstawie IPA 2016 jest Sekretarz Stanu, natomiast szkoccy ministrowie są uprawnieni do wydawania nakazów ukierunkowanego przechwytywania, nakazu w ramach wzajemnej pomocy oraz nakazów ukierunkowanej ingerencji w urządzenie elektroniczne, gdy osoby lub pomieszczenia, których ma dotyczyć przechwytywanie, oraz urządzenia elektroniczne, które mają być przedmiotem ingerencji, znajdują się w Szkocji (zob. art. 22 i 103 IPA 2016). W przypadku ukierunkowanej ingerencji w urządzenie elektroniczne szef organu ścigania (o którym mowa w części 1 i 2 załącznika 6 do IPA 2016) może wydać nakaz na warunkach określonych w art. 106 IPA 2016.

(¹³⁶) Komisarze sądowi wspierają Komisarza ds. Uprawnień Dochodzeniowo-Śledczych – niezależny organ, który sprawuje funkcje nadzorcze w kwestii wykorzystania uprawnień dochodzeniowo-śledczych przez agencje wywiadowcze.

(¹³⁷) Zob. w szczególności art. 19 i 23 IPA 2016.

(¹³⁸) Dostęp pod adresem: <https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25>.

(¹³⁹) Termin „dane pochodzące z łączności” (ang. *communications data*) obejmuje odpowiedzi na pytania: kto, kiedy, gdzie i jak przekazał wiadomość, korzystając ze środków łączności, ale nie obejmuje treści tej wiadomości, tj. tego, co powiedziano lub napisano. Dane pochodzące z łączności mogą obejmować czas i okres trwania komunikacji, numer lub adres e-mail nadawcy i odbiorcy, a czasami lokalizację urządzeń, z których dokonano połączenia, zob. art. 261 ust. 5 IPA 2016. W IPA 2016 zezwolono Sekretarzowi Stanu na wymaganie od operatorów telekomunikacyjnych zatrzymywania danych pochodzących z łączności do celów ukierunkowanego dostępu przez szereg organów publicznych, w tym organy ścigania i agencje wywiadowcze. W części 4 IPA 2016 przewidziano zatrzymywanie danych pochodzących z łączności, natomiast w części 3 przewidziano ukierunkowane pozyskiwanie danych pochodzących z łączności. W części 3 i części 4 IPA 2016 określono również szczegółowe ograniczenia w korzystaniu z tych uprawnień oraz przewidziano określone zabezpieczenia.

(¹⁴⁰) Na przykład w przypadku, gdy dana osoba uzyskuje dane pochodzące z łączności w ramach wykonywania ustawowych uprawnień właściwego organu publicznego lub gdy dane pochodzące z łączności uzyskuje się zgodnie z nakazem sądowym lub innym zezwoleniem sądowym. Art. 11 ust. 3A IPA 2016 wprowadzony art. 12 ust. 3 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

(¹⁴¹) Art. 261 ust. 5A i 5B wprowadzone art. 13 ust. 3 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

- (87) Wydawanie nakazów zatrzymywania danych pochodzących z łączności⁽¹⁴²⁾ nadal podlega ograniczeniom i zabezpieczeniom, jak opisano w motywach 208 i 209 decyzji wykonawczej (UE) 2021/1772, w szczególności wymogom niezbędności i proporcjonalności oraz zatwierdzenia przez niezależnego komisarza sądowego. Chociaż ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych wprowadzono możliwość przedłużenia ważności takich zawiadomień, każde przedłużenie podlega tym samym warunkom niezbędności i proporcjonalności oraz zatwierdzeniu przez komisarza sądowego⁽¹⁴³⁾.
- (88) W odniesieniu do danych pochodzących z łączności w ustawie z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych zmieniono również definicję operatora telekomunikacyjnego, obejmującą potencjalnych adresatów nakazu zatrzymywania danych. Definicja ta obejmuje obecnie każdą osobę, która „kontroluje lub dostarcza system telekomunikacyjny, który (i) nie znajduje się (w całości lub w części) w Zjednoczonym Królestwie ani nie jest (w całości lub w części) kontrolowany ze Zjednoczonego Królestwa oraz (ii) jest wykorzystywany przez inną osobę do oferowania lub świadczenia usług telekomunikacyjnych osobom w Zjednoczonym Królestwie”⁽¹⁴⁴⁾. Co ważne, zmieniona definicja nadal wymaga ścisłego związku z rynkiem Zjednoczonego Królestwa. Zmiana ta oznacza zatem, że duże przedsiębiorstwa o złożonych strukturach korporacyjnych są w całości objęte IPA 2016, bez rozszerzania zakresu definicji na dostawców usług telekomunikacyjnych, które nie są kierowane do osób w Zjednoczonym Królestwie. Potwierdzają to również noty wyjaśniające ustawę z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych, które stanowią, że zmiana ta nie ma na celu włączenia dodatkowych przedsiębiorstw w zakres odpowiednich uprawnień przewidzianych w IPA 2016⁽¹⁴⁵⁾, ale ma zasadniczo funkcję wyjaśniającą.
- (89) Ponadto ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych wprowadzono pewne ukierunkowane zmiany w procedurze wydawania nakazów, w tym w odniesieniu do ukierunkowanego przechwytywania i ukierunkowanej ingerencji w urządzenia elektroniczne, tj. uprawnień, które mogą również wykorzystywać konkretne organy ścigania w Zjednoczonym Królestwie do celów zapobiegania poważnym przestępstwom lub ich wykrywania. Zmiany dotyczą jedynie szczególnej sytuacji, w której uprawnienia te są wykorzystywane do uzyskiwania treści komunikacji lub prywatnych informacji o osobie, która jest członkiem właściwego organu ustawodawczego⁽¹⁴⁶⁾. Podczas gdy nakazy dotyczące ukierunkowanego przechwytywania i ingerencji w urządzenia elektroniczne mogą być zazwyczaj wydawane przez Sekretarza Stanu i zatwierdzane przez komisarza sądowego (zob. motywy 186–196 i 210–215 decyzji wykonawczej (UE) 2021/1772), art. 26 i 111 IPA wymagają dodatkowo zatwierdzenia przez premiera, jeżeli nakaz dotyczy posła do parlamentu lub członka innego właściwego organu ustawodawczego (procedura „triple-lock”). Ustawa z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych umożliwia obecnie premierowi nominację pięciu Sekretarzy Stanu, którzy będą uprawnieni do wykonywania uprawnień premiera do wydawania takich nakazów, pod warunkiem że konieczność uzyskania autoryzacji jest pilna, a premier nie jest w stanie jej udzielić ze względu na zły stan zdrowia lub brak dostępu do bezpiecznej komunikacji. Co ważne, ograniczenia i zabezpieczenia dotyczące wydawania tych nakazów, opisane w wyżej wymienionych motywach decyzji wykonawczej (UE) 2021/1772, pozostają w mocy.

3.2.2. Dalsze wykorzystywanie zebranych informacji

- (90) Udostępnianie danych przez organ ścigania innemu organowi do celów innych niż te, dla których pierwotnie je zebrano (tzw. „dalsze przekazywanie”), nadal podlega określonym warunkom przeanalizowanym w motywach 142–156 decyzji wykonawczej (UE) 2021/1772.

⁽¹⁴²⁾ Takie nakazy zatrzymywania danych zgodnie z art. 87–89 IPA 2016 wydaje się w celu zagwarantowania, aby operatorzy telekomunikacyjni zatrzymywali – nie dłużej niż przez 12 miesięcy – odpowiednie dane pochodzące z łączności, które w przeciwnym razie zostałyby usunięte w chwili, gdy nie są już potrzebne do celów prowadzonej działalności gospodarczej. Zatrzymywane dane należy udostępniać przez żądany okres na wypadek, gdyby na późniejszym etapie okazało się, że organ publiczny będzie musiał pozyskać takie dane na podstawie zezwolenia na ukierunkowane pozyskanie danych pochodzących z łączności, przewidzianego w części 3 IPA 2016.

⁽¹⁴³⁾ Art. 94A IPA 2016 wprowadzony art. 20 ust. 4 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁴⁴⁾ Art. 261 ust. 10 lit. c) IPA 2016, wprowadzony art. 19 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁴⁵⁾ Noty wyjaśniające do ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych, pkt 359, dostępne pod następującym adresem: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

⁽¹⁴⁶⁾ Zob. art. 26 i 111 IPA 2016.

- (91) Jeżeli chodzi o szczególną sytuację dalszego przekazywania danych ze Zjednoczonego Królestwa do Stanów Zjednoczonych, Umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki o dostępie do danych elektronicznych w celu zwalczania poważnej przestępczości (umowa między Zjednoczonym Królestwem a USA) ⁽¹⁴⁷⁾, którą zawarto w październiku 2019 r., weszła w życie i jest wdrażana od października 2022 r. Na podstawie umowy między Zjednoczonym Królestwem a USA dane przekazywane z UE do dostawców usług w Zjednoczonym Królestwie mogą podlegać nakazom wydania dowodów wydanym przez właściwe organy ścigania USA i stosowanym w Zjednoczonym Królestwie.
- (92) Co ważne, warunki i zabezpieczenia, na podstawie których takie nakazy mogą być wydawane i wykonywane, które oceniono w motywie 154 decyzji wykonawczej (UE) 2021/1772, nadal mają zastosowanie. W szczególności dane uzyskane na podstawie umowy są objęte ochroną równoważną względem szczególnych zabezpieczeń przewidzianych w tzw. „umowie ramowej między UE a USA” ⁽¹⁴⁸⁾, które w całości włączono do umowy między Zjednoczonym Królestwem a USA przez odesłanie na zasadzie odpowiedniego stosowania ⁽¹⁴⁹⁾.
- (93) Po przyjęciu decyzji wykonawczej (UE) 2021/1772 Zjednoczone Królestwo wyjaśniło już, że doprecyzowało, między innymi poprzez kontakty z odpowiednimi podmiotami w kontekście wdrażania umowy między Zjednoczonym Królestwem a USA, w jaki sposób szczególne zabezpieczenia przewidziane w umowie ramowej, które opracowano z myślą o kontekście współpracy organów ścigania, są dostosowywane i stosowane do konkretnego przekazywania danych objętego umową między Zjednoczonym Królestwem a USA. W szczególności Zjednoczone Królestwo wyjaśniło, że postanowienia umowy ramowej, które przewidują rolę odpowiedniego właściwego organu (który nie istnieje w sytuacji bezpośredniej współpracy między usługodawcą ze Zjednoczonego Królestwa a organem ścigania w Stanach Zjednoczonych), interpretuje się odpowiednio jako odnoszące się do wyznaczonego organu (określonego w umowie między Zjednoczonym Królestwem a USA) ⁽¹⁵⁰⁾ odpowiedniej strony.
- (94) Na przykład w odniesieniu do powiadomienia o incydencie związanym z bezpieczeństwem informacji zgodnie z art. 10 umowy ramowej między UE a USA, który wymaga powiadomienia właściwego organu przekazującego dane, Zjednoczone Królestwo wyjaśniło, że przepis ten stosuje się odpowiednio, co oznacza, że powiadomić należy wyznaczony organ strony, z której przekazano dane.
- (95) W odniesieniu do zgody właściwego organu przekazującego dane przed jakimkolwiek dalszym przekazaniem danych osobowych na podstawie art. 7 umowy ramowej Zjednoczone Królestwo wyjaśniło, że będzie stosować ten przepis odpowiednio, co oznacza, że na wszelkie dalsze przekazywanie danych musi zezwolić wyznaczony organ strony, z której przekazano dane.
- (96) Jeśli chodzi o wynikające z art. 8 umowy ramowej obowiązki utrzymania jakości i integralności informacji postanowienie to interpretowane odpowiednio oznaczałoby, że wyznaczony organ strony, która otrzymuje dane, byłby odpowiedzialny za kontakty z dostawcą, który przekazał dane, w przypadku jakichkolwiek problemów związanych z jakością i integralnością danych.

⁽¹⁴⁷⁾ Umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki o dostępie do danych elektronicznych w celu zwalczania poważnej przestępczości, dostępna pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Counteracting_Serious_Crime.pdf.

⁽¹⁴⁸⁾ 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, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

⁽¹⁴⁹⁾ Art. 9 ust. 1 umowy.

⁽¹⁵⁰⁾ Zgodnie z art. 1 ust. 8 umowy między Zjednoczonym Królestwem a USA „wyznaczony organ” oznacza podmiot rządowy wyznaczony, w przypadku Zjednoczonego Królestwa, przez Sekretarza Stanu Ministerstwa Spraw Wewnętrznych, a w przypadku Stanów Zjednoczonych przez Prokuratora Generalnego.

- (97) Jeżeli chodzi o środki zaskarżenia, Zjednoczone Królestwo podkreśliło, że w przekazywanie danych na podstawie umowy między Zjednoczonym Królestwem a USA będzie zawsze zaangażowany wyznaczony organ każdej ze stron. W przypadku gdy to Stany Zjednoczone są stroną otrzymującą dane od usługodawców w Zjednoczonym Królestwie, jako wyznaczony organ będzie działał Departament Sprawiedliwości USA. W związku z tym, zgodnie z interpretacją Zjednoczonego Królestwa, w każde żądanie złożone na podstawie umowy między Zjednoczonym Królestwem a USA zaangażowany będzie Departament Sprawiedliwości jako organ federalny wyznaczony na mocy amerykańskiej ustawy o środkach zaskarżenia, w związku z czym zgodnie z art. 19 umowy ramowej można skorzystać ze środków zaskarżenia przeciwko Departamentowi Sprawiedliwości. Ponadto Zjednoczone Królestwo potwierdziło służbom Komisji, że ustawa o środkach zaskarżenia nie jest jedynym mechanizmem dochodzenia roszczeń. W zależności od okoliczności i kontekstu danej sprawy inne mające zastosowanie przepisy Stanów Zjednoczonych zapewniają alternatywne możliwości zaskarżenia.

3.2.3. Nadzór i środki zaskarżenia

- (98) W zależności od uprawnień wykorzystywanych przez właściwe organy przy przetwarzaniu danych osobowych do celów ścigania przestępstw (na podstawie DPA 2018 lub IPA 2016) różne organy nadal zapewniają nadzór nad korzystaniem z tych uprawnień, jak oceniono w motywach 158–174 decyzji wykonawczej (UE) 2021/1772, a mechanizmy regulujące środki zaskarżenia są nadal dostępne na podstawie części 3 DPA 2018, na podstawie IPA 2016 i na podstawie ustawy o prawach człowieka z 1998 r., jak przeanalizowano w motywach 250–269 decyzji wykonawczej (UE) 2021/1772.
- (99) W odniesieniu do nadzoru nad częścią 3 DPA 2018 funkcje i uprawnienia Komisji ds. Informacji przeanalizowano w motywach 158–160 i 162 decyzji wykonawczej (UE) 2021/1772, z zastrzeżeniem zmian wprowadzonych ustawą o wykorzystaniu danych i dostępie do danych opisanych w sekcjach 2.3.1 i 2.3.2 niniejszej decyzji.
- (100) Jeżeli chodzi o wykonywanie tych uprawnień, od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772 Komisarz ds. Informacji rozpatrzył liczne skargi ⁽¹⁵¹⁾ 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 ⁽¹⁵²⁾. Komisarz ds. Informacji wydał również 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 ⁽¹⁵³⁾.
- (101) W odniesieniu do korzystania z uprawnień dochodzeniowo-śledczych na mocy IPA 2016 niezależny nadzór sądowy nadal zapewnia Komisarz ds. Uprawnień Dochodzeniowo-Śledczych, wspomagany przez innych komisarzy sądowych, których wspólnie określa się mianem komisarzy sądowych ⁽¹⁵⁴⁾. W tym obszarze w ustawie z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych wprowadzono jedynie ograniczone i ukierunkowane zmiany, które nie mają wpływu na niezależność, zadania i uprawnienia komisarzy sądowych, ale mają na celu wzmocnienie w praktyce funkcjonowania istniejącego systemu nadzoru, w szczególności przez wprowadzenie zastępców Komisarza ds. Uprawnień Dochodzeniowo-Śledczych, którym może on przekazać określone uprawnienia, jeżeli nie jest w stanie sprawować swoich funkcji lub nie jest dostępny. Tacy zastępcy Komisarza ds. Uprawnień Dochodzeniowo-Śledczych muszą być komisarzami sądowymi i są powoływani przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych ⁽¹⁵⁵⁾.

⁽¹⁵¹⁾ 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>.

⁽¹⁵²⁾ Dodatkowe informacje są dostępne pod następującym adresem: <https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice>.

⁽¹⁵³⁾ 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/>.

⁽¹⁵⁴⁾ Zob. motyw 250 decyzji wykonawczej (UE) 2021/1772.

⁽¹⁵⁵⁾ Art. 227 IPA 2016, wprowadzony art. 7 ustawy o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

3.3. Istotne zmiany dotyczące dostępu organów publicznych Zjednoczonego Królestwa do danych w celach związanych z bezpieczeństwem narodowym i wykorzystywania przez nie danych w tych celach

- (102) W odniesieniu do uprawnień dochodzeniowo-śledczych wykonywanych w kontekście bezpieczeństwa narodowego IPA 2016 nadal zapewnia ramy prawne korzystania z tych uprawnień. Oprócz zmian dotyczących ukierunkowanych uprawnień dochodzeniowo-śledczych, na które, pod pewnymi warunkami, mogą powoływać się również niektóre organy ścigania, jak opisano w motywach 77–85 niniejszej decyzji, ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych wprowadzono również zmiany w jednym z uprawnień przewidzianych w IPA 2016, które można wykonywać masowo.
- (103) Dokładniej rzecz ujmując, ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych wprowadzono w nowej części 7A IPA 2016 szczególny system zatrzymywania i badania określonego podzbioru masowych zbiorów danych osobowych⁽¹⁵⁶⁾, tj. zbiorów danych, w przypadku których osoby fizyczne, których dotyczą dane osobowe, nie mogą mieć uzasadnionych oczekiwań co do prywatności w odniesieniu do tych danych lub mogą mieć jedynie niewielkie uzasadnione oczekiwania co do takiej prywatności⁽¹⁵⁷⁾. To, czy dany masowy zbiór danych osobowych należy do tego określonego podzbioru masowych zbiorów danych, ustala szef służby wywiadowczej na podstawie wszystkich okoliczności, w szczególności (i) charakteru danych, (ii) zakresu, w jakim dane zostały podane do wiadomości publicznej przez osoby fizyczne lub w jakim osoby fizyczne wyraziły zgodę na ich podanie do wiadomości publicznej, (iii) tego, czy dane zostały opublikowane, zakresu, w jakim zostały one opublikowane pod kontrolą redakcyjną lub przez osobę działającą zgodnie z normami zawodowymi, (iv) tego, czy dane te zostały opublikowane lub są w inny sposób publicznie znane, zakresu, w jakim dane te są powszechnie znane, oraz (v) zakresu, w jakim dane te wykorzystano już w domenie publicznej⁽¹⁵⁸⁾.
- (104) Co ważne, w odniesieniu do zatrzymywania i badania masowych zbiorów danych osobowych, które nie wchodzą w zakres tej kategorii, tzn. takich, które są bardziej wrażliwe, a przez to wiążą się z uzasadnionym oczekiwaniem zachowania ich prywatności, nadal obowiązuje system poddany ocenie w motywach 239 i 240 decyzji wykonawczej (UE) 2021/1772, w szczególności konieczność zatwierdzenia nakazu najpierw przez Sekretarza Stanu, a następnie przez komisarza sądowego, z zastrzeżeniem wymogów niezbędności i proporcjonalności środka, przewidzianych w części 7 IPA 2016⁽¹⁵⁹⁾.
- (105) W części 7A IPA 2016 przewidziano dwa rodzaje zezwoleń: zezwolenie indywidualne i zezwolenie dotyczące kategorii. Zatrzymywanie albo zatrzymywanie i badanie każdego masowego zbioru danych osobowych przechowywanego na podstawie części 7A musi się odbywać na podstawie jednego z tych zezwoleń. Oba zezwolenia co do zasady wymagają⁽¹⁶⁰⁾ zezwolenia szefa służby wywiadowczej (lub osoby działającej w jego imieniu) i zatwierdzenia przez niezależnego komisarza sądowego⁽¹⁶¹⁾. Szef służby wywiadowczej udziela indywidualnego zezwolenia na warunkach określonych w art. 226B ust. 4 IPA 2016 i pod warunkiem uzyskania uprzedniej zgody komisarza sądowego. Komisarz sądowy musi przeanalizować wnioski osoby, która udzieliła zezwolenia, w odniesieniu do tego, czy art. 226A, tj. wymóg niewielkich uzasadnionych oczekiwań co do ochrony prywatności lub braku takich oczekiwań, ma zastosowanie do masowego zbioru danych osobowych, którego dotyczy dane zezwolenie⁽¹⁶²⁾.

⁽¹⁵⁶⁾Nakazy dotyczące masowych zbiorów danych osobowych wydane na podstawie art. 200 IPA 2016 upoważniają agencje wywiadowcze do zatrzymywania i badania zbiorów danych, które zawierają dane osobowe dotyczące większej liczby osób fizycznych, jeżeli charakter zbioru danych jest taki, że większość osób fizycznych nim objętych nie jest przedmiotem zainteresowania służb wywiadowczych w wykonywaniu ich funkcji i jest mało prawdopodobne, że stanie się jego przedmiotem, oraz które są przechowywane w formie elektronicznej przez służby wywiadowcze i zatrzymywane do analizy w ramach wykonywania ich funkcji ustawowych, zob. również art. 199 IPA 2016.

⁽¹⁵⁷⁾Art. 226A ust. 1 IPA 2016, wprowadzony art. 2 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁵⁸⁾Art. 226A ust. 3 IPA 2016, wprowadzony art. 2 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁵⁹⁾Ustawą z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych zmieniono art. 213 IPA 2016 w taki sposób, że nakazy dotyczące masowych zbiorów danych osobowych przestają obowiązywać 12 miesięcy po wydaniu. Wcześniej takie nakazy trzeba było odnawiać co 6 miesięcy. Zob. art. 3 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁶⁰⁾Indywidualne zezwolenie może zostać udzielone bez uprzedniej zgody organu sądowego wyłącznie (i) jeżeli osoba udzielająca indywidualnego zezwolenia uzna, że dany masowy zbiór danych osobowych wchodzi w zakres istniejącego zezwolenia dotyczącego kategorii, lub (ii) w pilnych przypadkach, zob. art. 226B ust. 6 IPA 2016. W tej drugiej sytuacji decyzja o udzieleniu pilnego indywidualnego zezwolenia podlega kontroli komisarza sądowego w terminie trzech dni roboczych od dnia jej wydania, zob. art. 226BC IPA 2016.

⁽¹⁶¹⁾Art. 226B ust. 1 IPA 2016, wprowadzony art. 2 ustawy o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁶²⁾Art. 226BB ust. 1 lit. a) IPA 2016, wprowadzony art. 2 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

- (106) Zezwolenie dotyczące kategorii upoważnia do zatrzymywania lub zatrzymywania i badania kategorii masowych zbiorów danych osobowych opisanej w takim zezwoleniu.
- (107) Decyzję o udzieleniu zezwolenia dotyczącego kategorii podejmuje szef służby wywiadowczej, jeżeli uzna, że art. 226A ma zastosowanie do każdego zbioru danych w ramach danej kategorii, oraz jeżeli decyzję o udzieleniu zezwolenia zatwierdził niezależny komisarz sądowy⁽¹⁶³⁾. Komisarz ten musi sprawdzić, czy art. 226A, tj. wymóg niewielkich uzasadnionych oczekiwań co do ochrony prywatności lub brak takich oczekiwań, ma zastosowanie do każdego zbioru danych należącego do kategorii zbiorów danych opisanej w zezwoleniu⁽¹⁶⁴⁾.
- (108) Co ważne, zatwierdzając decyzję o udzieleniu zezwolenia indywidualnego lub zezwolenia dotyczącego kategorii, komisarz sądowy musi „stosować te same zasady, które zastosowałby sąd w przypadku wniosku o kontrolę sądową”⁽¹⁶⁵⁾, i rozpatrywać te kwestie z wystarczającą starannością, aby zapewnić przestrzeganie przez komisarza sądowego obowiązków nałożonych na mocy art. 2 IPA 2016 (ogólne obowiązki w związku z ochroną prywatności)⁽¹⁶⁶⁾. Ponadto wydawanie zezwoleń podlega ścisłemu nadzorowi *ex post*, w szczególności w drodze corocznego składania sprawozdań Sekretarzowi Stanu oraz Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa Parlamentu⁽¹⁶⁷⁾, a także regularnych inspekcji Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych⁽¹⁶⁸⁾.
- (109) Jeżeli chodzi o istotne zmiany w obszarze nadzoru, Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych opublikowało sprawozdania roczne za lata 2021, 2022 i 2023, w których przedstawiono szczegółowe statystyki i informacje na temat korzystania z uprawnień dochodzeniowo-śledczych przez agencje wywiadowcze i organy ścigania w Zjednoczonym Królestwie⁽¹⁶⁹⁾. W sprawozdaniach tych opisano również audyty i dochodzenia Biura, a także ich ustalenia, potwierdzając, że Komisarz ds. Uprawnień Dochodzeniowo-Śledczych nadal zapewnia bardzo ważną funkcję nadzorczą w ramach systemu uprawnień dochodzeniowo-śledczych Zjednoczonego Królestwa. Na przykład w 2023 r. Komisja dokonała przeglądu uzasadnień niezbędności i proporcjonalności w odniesieniu do korzystania z uprawnień do masowego przechwytywania – jak oceniono w motywach 218–225 decyzji wykonawczej (UE) 2021/1772 – przez Centralę Łączności Rządowej, stwierdzając, że znaczną większość oświadczeń przedstawiono z należyтым uzasadnieniem, natomiast w niektórych przypadkach proporcjonalność nie była dobrze wyrażona. Ustalenia te omówiono z zespołem ds. zgodności Centrali Łączności Rządowej, który zobowiązał się do zlecenia dodatkowych wewnętrznych szkoleń uświadamiających w celu rozwiązania tej kwestii⁽¹⁷⁰⁾.
- (110) Ponadto Trybunał ds. Uprawnień Dochodzeniowo-Śledczych opublikował jawne sprawozdanie ze swojej działalności i orzecznictwa w latach 2021–2023⁽¹⁷¹⁾. Z tego sprawozdania wynika, że liczba spraw, które wpłynęły do Trybunału, od 2017 r. wzrosła ponad dwukrotnie – w 2023 r. wpłynęło ponad 400 spraw⁽¹⁷²⁾. Większość skarg

⁽¹⁶³⁾ Art. 226BA IPA 2016, wprowadzony art. 2 ustawy o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁶⁴⁾ Art. 226BB ust. 1 lit. b) IPA 2016, wprowadzony art. 2 ustawy o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁶⁵⁾ Art. 226BB ust. 2 lit. a) IPA 2016, wprowadzony art. 2 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁶⁶⁾ Art. 226BB ust. 2 lit. b) IPA 2016, wprowadzony art. 2 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych. Zgodnie z ogólnymi obowiązkami w odniesieniu do prywatności określonymi w art. 2 IPA 2016 organ publiczny musi uwzględnić, a) czy skutek, który ma zostać osiągnięty za pomocą nakazu, upoważnienia lub zawiadomienia, można by w zasadny sposób osiągnąć za pomocą innych środków związanych z mniejszą ingerencją w prywatność, b) czy stopień ochrony, który ma być stosowany w odniesieniu do wszelkiego pozyskiwania informacji na podstawie nakazu, upoważnienia lub zawiadomienia jest wyższy ze względu na szczególną wrażliwość tych informacji, c) interes publiczny w zakresie integralności i bezpieczeństwa systemów telekomunikacyjnych i usług pocztowych oraz d) wszelkie inne aspekty interesu publicznego w zakresie ochrony prywatności.

⁽¹⁶⁷⁾ Art. 226DA i 226DB IPA 2016, wprowadzone art. 2 ustawy z 2024 r. o zmianie ustawy o uprawnieniach dochodzeniowo-śledczych.

⁽¹⁶⁸⁾ Zob. sprawozdanie roczne Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2023 r., dostępne pod adresem: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, s. 3.

⁽¹⁶⁹⁾ Sprawozdania roczne są dostępne pod adresem: <https://www.ipco.org.uk/publications/annual-reports/>.

⁽¹⁷⁰⁾ Zob. pkt 6.39–6.43 sprawozdania rocznego za 2023 r., dostępnego pod adresem: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

⁽¹⁷¹⁾ Sprawozdanie Trybunału ds. Uprawnień Dochodzeniowo-Śledczych za lata 2021–2023, dostępne pod adresem: <https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf>.

⁽¹⁷²⁾ Sprawozdanie Trybunału ds. Uprawnień Dochodzeniowo-Śledczych za lata 2021–2023, s. 5.

dotyczyła organów ścigania, a tuż za nimi uplasowały się skargi dotyczące organów bezpieczeństwa i wywiadu ⁽¹⁷³⁾. Co ważne, w latach 2022 i 2023 Trybunał wydał wyroki w sprawach, które wpłynęły do niego przed 2021 r., w których stwierdził, że organy publiczne Zjednoczonego Królestwa – odpowiednio Policja Szkocji ⁽¹⁷⁴⁾, Policja Hrabstwa Greater Manchester ⁽¹⁷⁵⁾, Policja Hrabstwa Surrey ⁽¹⁷⁶⁾, MI5 oraz Minister Spraw Wewnętrznych ⁽¹⁷⁷⁾ – działały niezgodnie z prawem. Jeżeli chodzi o środki zaradcze, Trybunał ds. Uprawnień Dochodzeniowo-Śledczych nakazał między innymi zniszczenie wszystkich materiałów uzyskanych niezgodnie z prawem, a w jednym przypadku również zapłatę kwoty 12 000 GBP tytułem zadośćuczynienia za stwierdzone naruszenia. Sprawozdanie roczne potwierdza zatem, że Trybunał ds. Uprawnień Dochodzeniowo-Śledczych skutecznie wypełnia swoją ważną rolę, jaką jest gwarantowanie nadzoru i dochodzenia roszczeń w obszarze dostępu do danych osobowych na potrzeby ścigania przestępstw i ze względów bezpieczeństwa narodowego.

- (111) Ponadto w sprawozdaniu podkreślono również nowe istotne kwestie, takie jak wyrok Europejskiego Trybunału Praw Człowieka orzekający, że osoby fizyczne na całym świecie mogą wnosić do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych skargi dotyczące funkcjonowania brytyjskiego systemu masowego przechwytywania, jeżeli dane czynności zostały dokonane przez organ publiczny Zjednoczonego Królestwa i miały miejsce w Zjednoczonym Królestwie ⁽¹⁷⁸⁾.

4. WNIOSKI

- (112) Komisja uważa, że RODO UK i DPA 2018, zmienione ustawą o wykorzystaniu danych i dostępie do danych, zapewniają stopień ochrony danych osobowych przekazywanych z Unii Europejskiej merytorycznie równoważny temu zagwarantowanemu w rozporządzeniu (UE) 2016/679.
- (113) Ponadto Komisja stwierdza, że mechanizmy nadzoru i możliwości dochodzenia roszczeń przewidziane w prawie Zjednoczonego Królestwa – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia przepisów i w praktyce nakładania za te naruszenia kar 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.
- (114) Wreszcie na podstawie dostępnych informacji na temat porządku prawnego Zjednoczonego Królestwa Komisja uważa, że wszelkie ingerencje w prawa podstawowe osób fizycznych, których dane osobowe są przekazywane z Unii Europejskiej do Zjednoczonego Królestwa, jakich dopuszczają się organy publiczne Zjednoczonego Królestwa do celów związanych z interesem publicznym, w szczególności do celów ścigania przestępstw i bezpieczeństwa narodowego, nadal ograniczają się do tego, co jest ściśle niezbędne do osiągnięcia danego uzasadnionego celu, oraz że istnieje skuteczna ochrona prawna przed takimi ingerencjami.
- (115) W świetle ustaleń niniejszej decyzji należy zatem uznać, że Zjednoczone Królestwo nadal zapewnia odpowiedni stopień ochrony w rozumieniu art. 45 rozporządzenia (UE) 2016/679, interpretowanego w świetle Karty praw podstawowych Unii Europejskiej.
- (116) Wniosek ten opiera się zarówno na odpowiednim systemie krajowym Zjednoczonego Królestwa, który zmienił się od czasu przyjęcia decyzji wykonawczej (UE) 2021/1772, jak i na zobowiązaniach międzynarodowych Zjednoczonego Królestwa, w szczególności na dalszym stosowaniu się przez nie do Konwencji o ochronie praw człowieka i podstawowych wolności oraz dalszym poddawaniu się jurysdykcji Europejskiego Trybunału Praw Człowieka. Nieprzerwane przestrzeganie takich zobowiązań międzynarodowych stanowi zatem szczególnie istotny element oceny, na której opiera się niniejsza decyzja.

⁽¹⁷³⁾ Sprawozdanie Trybunału ds. Uprawnień Dochodzeniowo-Śledczych za lata 2021–2023, s. 12.

⁽¹⁷⁴⁾ *Wilson v Police Scotland* [2022] UKIPTrib 5.

⁽¹⁷⁵⁾ *Pendlebury v Greater Manchester Police* [2023] UKIPTrib 2.

⁽¹⁷⁶⁾ *Hill v Metropolitan Police Service & Independent Office For Police Conduct* [2022] UKIPTrib 6.

⁽¹⁷⁷⁾ *Liberty & Privacy International v Security Service and Secretary of State for the Home Department* [2023] UKIPTrib 1.

⁽¹⁷⁸⁾ *Wieder i Guarnieri przeciwko Zjednoczonemu Królestwu*, [2023] ETPC 668, zob. również sprawozdanie Trybunału ds. Uprawnień Dochodzeniowo-Śledczych za lata 2021–2023, s. 6.

5. SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH

- (117) 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, uchylenia, stwierdzenia ich nieważności w postępowaniu o stwierdzenie nieważności lub orzeczenia o ich nieważności w następstwie odesłania prejudycjalnego lub zarzutu niezgodności z prawem.
- (118) Decyzja stwierdzająca odpowiedni stopień ochrony danych osobowych przyjęta przez Komisję na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 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) 2021/1772 zmienionej niniejszą decyzją, przekazywanie danych przez administratora lub podmiot przetwarzający w Unii Europejskiej administratorom lub podmiotom przetwarzającym w Zjednoczonym Królestwie może odbywać się bez konieczności uzyskania jakiegokolwiek dodatkowego zezwolenia.
- (119) Należy przypomnieć, że zgodnie z art. 58 ust. 5 rozporządzenia (UE) 2016/679 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems I⁽¹⁷⁹⁾, 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 tej osobie podniesienie tych zarzutów przed sądem krajowym, który może być zobowiązany do wystąpienia z wnioskiem do Trybunału Sprawiedliwości o wydanie orzeczenia w trybie prejudycjalnym⁽¹⁸⁰⁾.

6. MONITOROWANIE

- (120) Zgodnie z art. 45 ust. 4 rozporządzenia (UE) 2016/679 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 Komisarza ds. Informacji, w tym w zakresie rozpatrywania skarg i stosowania uprawnień naprawczych, a także na przestrzeganie ograniczeń i zabezpieczeń w odniesieniu do dostępu rządowego, w szczególności w odniesieniu do nowo wprowadzonej do IPA 2016 części 7A. W monitorowaniu Komisja powinna uwzględniać między innymi zmiany w orzecznictwie oraz nadzór ze strony Komisarza ds. Informacji i innych niezależnych organów.
- (121) Aby ułatwić to monitorowanie, władze Zjednoczonego Królestwa powinny niezwłocznie informować Komisję o wszelkich istotnych zmianach w porządku prawnym Zjednoczonego Królestwa, które mają wpływ na ramy prawne będące przedmiotem decyzji wykonawczej (UE) 2021/1772 zmienionej niniejszą decyzją, a także o wszelkich zmianach praktyk związanych z przetwarzaniem danych osobowych poddanych ocenie w decyzji wykonawczej (UE) 2021/1772 zmienionej niniejszą decyzją, zarówno w odniesieniu do przetwarzania danych osobowych przez administratorów i podmioty przetwarzające na mocy RODO UK, jak i ograniczeń i zabezpieczeń dotyczących uzyskiwania dostępu do danych przez organy publiczne. Powinno to obejmować zmiany dotyczące elementów, o których mowa w motywie (120).
- (122) 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 administratorom lub podmiotom przetwarzającym 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 lub wykrywanie lub ściganie czynów zabronionych, lub za bezpieczeństwo narodowe, w tym wszelkich organów nadzoru, nie gwarantują wymaganego stopnia ochrony.

⁽¹⁷⁹⁾ Schrems I, pkt 65.

⁽¹⁸⁰⁾ Schrems I, pkt 65: „W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji”.

- (123) W przypadku gdy z dostępnych informacji, w szczególności informacji uzyskanych w wyniku monitorowania decyzji wykonawczej (UE) 2021/1772 zmienionej niniejszą decyzją 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. Procedura taka byłaby uruchamiana na przykład w przypadkach, w których dalsze przekazywanie danych, w tym na podstawie nowych rozporządzeń stwierdzających odpowiedni stopień ochrony przyjętych przez Sekretarza Stanu lub umów międzynarodowych zawartych przez Zjednoczone Królestwo, nie odbywałoby się już w ramach gwarancji zapewniających ciągłość ochrony w rozumieniu art. 44 rozporządzenia (UE) 2016/679.
- (124) Jeżeli po upływie tego określonego terminu właściwe organy Zjednoczonego Królestwa nie zastosują 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. 93 ust. 2 rozporządzenia (UE) 2016/679, w celu częściowego lub całkowitego zawieszenia lub uchylecia niniejszej decyzji.
- (125) Ewentualnie Komisja rozpocznie tę procedurę w celu zmiany decyzji, 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.
- (126) W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja skorzysta z możliwości przyjęcia zgodnie z procedurą, o której mowa w art. 93 ust. 3 rozporządzenia (UE) 2016/679, mających natychmiastowe zastosowanie aktów wykonawczych zawieszających, uchylających lub zmieniających decyzję.

7. PRZEGLĄD, OKRES OBOWIĄZYWANIA I PRZEDŁUŻENIE OBOWIĄZYWANIA NINIEJSZEJ DECYZJI

- (127) W zastosowaniu art. 45 ust. 3 rozporządzenia (UE) 2016/679 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, uwzględniając elementy wymienione w art. 45 ust. 2 rozporządzenia (UE) 2016/679. 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.
- (128) 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.
- (129) Na podstawie tej oceny Komisja powinna przygotować ogólnodostępne sprawozdanie, które przedłoży Parlamentowi Europejskiemu i Radzie.
- (130) Komisja musi również wziąć pod uwagę, że ramy ochrony danych ocenione w niniejszej decyzji i w decyzji wykonawczej (UE) 2021/1772 mogą ulec dalszym zmianom.
- (131) W związku z tym należy przewidzieć, że niniejsza decyzja będzie miała zastosowanie przez okres sześciu lat od chwili jej wejścia w życie.

- (132) 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, wsząć 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. 93 ust. 2 rozporządzenia (UE) 2016/679.

8. UWAGI KOŃCOWE

- (133) Europejska Rada Ochrony Danych opublikowała swoją opinię⁽¹⁸¹⁾, która została uwzględniona podczas przygotowywania niniejszej decyzji.
- (134) Środek przewidziany w niniejszej decyzji jest zgodny z opinią komitetu ustanowionego na mocy art. 93 rozporządzenia (UE) 2016/679.
- (135) Należy zatem odpowiednio zmienić decyzję wykonawczą (UE) 2021/1772,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Uchyła się art. 1 ust. 2 decyzji wykonawczej (UE) 2021/1772.

Artykuł 2

Art. 4 decyzji wykonawczej (UE) 2021/1772 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. 93 ust. 2 rozporządzenia (UE) 2016/679.”.

Artykuł 3

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 19 grudnia 2025 r.

W imieniu Komisji
Michael MCGRATH
Członek Komisji

⁽¹⁸¹⁾Opinia 26/2025 w sprawie projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679, stwierdzającej odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo, dostępna pod adresem https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.