II

*(Akty o charakterze nieustawodawczym)*

# DECYZJE

## ROZPORZĄDZENIE WYKONAWCZE 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**

*(notyfikowana jako dokument nr C(2021) 4800)*

**(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 rozporządzeniu (UE) 2016/679 określono zasady dotyczące przekazywania danych osobowych przez administratorów danych lub podmioty przetwarzające w Unii Europejskiej do państw trzecich i organizacji międzynarodowych w zakresie, w jakim takie przekazywanie wchodzi w zakres stosowania rozporządzenia. Zasady dotyczące międzynarodowego przekazywania danych określono w rozdziale V rozporządzenia, tj. w art. 44–50. Chociaż przepływ danych osobowych do państw spoza Unii Europejskiej oraz z takich państw jest niezbędnym warunkiem rozwoju współpracy międzynarodowej i handlu transgranicznego, przekazywanie danych osobowych do państw trzecich nie może obniżać stopnia ochrony zapewnianego tym danym w Unii Europejskiej ([2]).

(2) Na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Przy spełnieniu tego warunku przekazanie danych osobowych do państwa trzeciego może nastąpić bez konieczności uzyskania jakiegokolwiek dodatkowego zezwolenia, jak przewidziano w art. 45 ust. 1 i motywie 103 rozporządzenia.

(3) Jak określono w art. 45 ust. 2 rozporządzenia (UE) 2016/679, przy przyjmowaniu decyzji stwierdzającej odpowiedni stopień ochrony należy opierać się na wszechstronnej analizie porządku prawnego państwa trzeciego, obejmującej zarówno jego przepisy dotyczące podmiotów odbierających dane, jak i ograniczenia oraz zabezpieczenia w zakresie dostępu organów publicznych do danych osobowych. W swojej ocenie Komisja musi ustalić, czy dane państwo trzecie daje gwarancje zapewniające stopień ochrony „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii Europejskiej (motyw 104 rozporządzenia (UE) 2016/679). Oceny spełnienia tego warunku dokonuje się według standardu ustanowionego w przepisach Unii Europejskiej, w szczególności w rozporządzeniu (UE) 2016/679, a także w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej ([3]). Istotne znaczenie w tym zakresie mają również wytyczne dotyczące odpowiedniego stopnia ochrony przekazywanych danych osobowych zatwierdzone przez Europejską Radę Ochrony Danych (EROD) ([4]).

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) Zob. motyw 101 rozporządzenia (UE) 2016/679.
([3]) Zob. niedawna sprawa C-311/18, Facebook Ireland i Schrems („Schrems II"), ECLI:EU:C:2020:559.
([4]) Europejska Rada Ochrony Danych, Odpowiedni stopień ochrony przekazywanych danych osobowych, WP 254 rev.01, dokument dostępny pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

(4) Jak wyjaśnił w swoim orzecznictwie Trybunał Sprawiedliwości Unii Europejskiej, nie oznacza to konieczności stwierdzenia identycznego stopnia ochrony ([5]). 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 wysoki stopień ochrony ([6]). W związku z powyższym odpowiedni standard ochrony można osiągnąć bez konieczności dokładnego powielenia przepisów unijnych. Przy określaniu odpowiedniości 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 zapewnia jako całość wymagany stopień ochrony ([7]).

(5) Komisja uważnie przeanalizowała prawo i praktykę Zjednoczonego Królestwa. Na podstawie ustaleń przedstawionych w motywach 8–270 Komisja stwierdza, że Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych w ramach zakresu stosowania rozporządzenia (UE) 2016/679 z Unii Europejskiej do Zjednoczonego Królestwa.

(6) Wniosek ten 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 („wyłączenie dotyczące imigracji") zgodnie z pkt 4 ppkt 1 załącznika 2 do brytyjskiej ustawy o ochronie danych. Ważność i wykładnia zwolnienia imigracyjnego na mocy prawa Zjednoczonego Królestwa nie została rozstrzygnięta w następstwie orzeczenia sądu apelacyjnego Anglii i Walii z dnia 26 maja 2021 r. Uznając, że prawa osób, których dane dotyczą, mogą co do zasady zostać ograniczone do celów kontroli imigracyjnej, co stanowi „istotny aspekt interesu publicznego", sąd apelacyjny stwierdził, że zwolnienie imigracyjne w obecnej postaci jest niezgodne z prawem Zjednoczonego Królestwa, ponieważ ten środek ustawodawczy nie zawiera szczegółowych przepisów określających zabezpieczenia wymienione w art. 23 ust. 2 ogólnego rozporządzenia o ochronie danych Zjednoczonego Królestwa (RODO UK) ([8]). W tej sytuacji przekazywanie z Unii do Zjednoczonego Królestwa danych osobowych, do których może mieć zastosowanie wyłączenie imigracyjne, należy wyłączyć z zakresu niniejszej decyzji ([9]). Gdy niezgodność z prawem Zjednoczonego Królestwa zostanie usunięta, należy ponownie ocenić wyłączenie dotyczące imigracji, a także potrzebę utrzymania ograniczenia zakresu stosowania niniejszej decyzji.

(7) Niniejsza decyzja nie powinna mieć wpływu na bezpośrednie stosowanie rozporządzenia (UE) 2016/679 w odniesieniu do organizacji mających siedzibę w Zjednoczonym Królestwie, jeżeli spełnione są warunki dotyczące terytorialnego zakresu stosowania tego rozporządzenia, określone w jego art. 3.

## 2. PRZEPISY MAJĄCE ZASTOSOWANIE DO PRZETWARZANIA DANYCH OSOBOWYCH

### 2.1. Ramy konstytucyjne

(8) Zjednoczone Królestwo jest demokracją parlamentarną, w której głową państwa jest suweren konstytucyjny. W państwie tym istnieje suwerenny parlament, który jest nadrzędny wobec wszystkich innych instytucji rządowych, władza wykonawcza wywodząca się z parlamentu i przed nim odpowiedzialna oraz niezależna władza sądownicza. Legitymacja władzy wykonawczej wywodzi się z jej zdolności do zdobycia zaufania wybieranej Izby Gmin; władza wykonawcza jest odpowiedzialna przed obiema izbami parlamentu odpowiadającymi za nadzorowanie rządu oraz za debatowanie nad ustawami i ich uchwalanie.

([5]) Sprawa C-362/14, Schrems („Schrems I"), ECLI:EU:C:2015:650, pkt 73.

([6]) Schrems I, pkt 74.

([7]) 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. 8, dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

([8]) Sąd Apelacyjny (Wydział Cywilny), Open Rights Group przeciwko Secretary of State for the Home Department i Secretary of State for the Digital, Culture, Media and Sport, [2021] EWCA Civ 800, pkt 53–56. Sąd Apelacyjny uchylił orzeczenie Wysokiego Trybunału, który wcześniej ocenił wyłączenie w świetle rozporządzenia (UE) 2016/679 (w szczególności jego art. 23) i Karty praw podstawowych Unii Europejskiej i uznał je za zgodne z prawem (Open Rights Group i in., Korona (powodowie) przeciwko Secretary of State for the Home Department i in. [2019] EWHC 2562).

([9]) Pod warunkiem spełnienia określonych warunków przekazanie danych do celów kontroli imigracyjnej Zjednoczonego Królestwa może odbywać się na podstawie mechanizmów przekazywania przewidzianych w art. 46–49 rozporządzenia (UE) 2016/679.

(9) Parlament Zjednoczonego Królestwa przekazał Parlamentowi Szkockiemu, Zgromadzeniu Narodowemu Walii (Senedd Cymru) oraz Zgromadzeniu Irlandii Północnej odpowiedzialność za stanowienie prawa w kwestiach krajowych w Szkocji, Walii i Irlandii Północnej, których Parlament Zjednoczonego Królestwa nie zastrzegł dla siebie. Chociaż ochrona danych jest kwestią zastrzeżoną, tj. w całym państwie obowiązują te same przepisy, inne obszary polityki istotne dla niniejszej decyzji są zdecentralizowane. Na przykład zwierzchnictwo nad systemami sądownictwa karnego, w tym nad policją, w Szkocji i Irlandii Północnej zostało powierzone odpowiednio Parlamentowi Szkockiemu i Zgromadzeniu Irlandii Północnej. Zjednoczone Królestwo nie posiada skodyfikowanej konstytucji w postaci spisanej ustawy zasadniczej. Zasady konstytucyjne kształtowały się w miarę upływu czasu i wywodzą się w szczególności z orzecznictwa i zwyczaju. Wartość konstytucyjna niektórych ustaw, takich jak Wielka Karta Swobód, ustawa o prawach z 1689 r. i ustawa o prawach człowieka z 1998 r., została uznana przez sądy. Prawa podstawowe osób fizycznych ukształtowano, jako element konstytucji, poprzez prawo precedensowe (*common law*), wspomniane ustawy oraz traktaty międzynarodowe, w szczególności europejską konwencję praw człowieka, którą Zjednoczone Królestwo ratyfikowało w 1951 r. W 1987 r. Zjednoczone Królestwo ratyfikowało również Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108) ([10]).

(10) Ustawą o prawach człowieka z 1998 r. wprowadzono prawa zawarte w europejskiej konwencji praw człowieka do prawa Zjednoczonego Królestwa. 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 jako element tego prawa) oraz prawo do rzetelnego procesu sądowego ([11]). W szczególności na podstawie art. 8 tej konwencji władza publiczna może ingerować w korzystanie z prawa do prywatności wyłącznie w przypadkach przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób.

(11) Zgodnie z ustawą o prawach człowieka z 1998 r. wszelkie działania władzy publicznej muszą być zgodne z prawem określonym w konwencji ([12]). Ponadto akty ustawowe i wykonawcze muszą być interpretowane i stosowane w sposób zgodny z prawami określonymi w konwencji ([13]).

### 2.2. **Ramy ochrony danych obowiązujące w Zjednoczonym Królestwie**

(12) Zjednoczone Królestwo wystąpiło z Unii Europejskiej w dniu 31 stycznia 2020 r. Na podstawie Umowy o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej ([14]) prawo Unii nadal miało zastosowanie w Zjednoczonym Królestwie w okresie przejściowym do dnia 31 grudnia 2020 r. Przed wystąpieniem i w okresie przejściowym ramy prawne dotyczące ochrony danych osobowych w Zjednoczonym Królestwie składały się z odpowiednich przepisów UE (w szczególności rozporządzenia (UE) 2016/679 i dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([15])) oraz ustawodawstwa krajowego, zwłaszcza ustawy o ochronie danych z 2018 r. (*Data Protection Act 2018*, „DPA 2018") ([16]), która przewidywała przepisy krajowe doprecyzowujące i ograniczające stosowanie przepisów rozporządzenia (UE) 2016/679 (w przypadkach dozwolonych na mocy tego rozporządzenia) oraz transponujące dyrektywę (UE) 2016/680.

([10]) Zasady konwencji nr 108 zostały pierwotnie wdrożone do prawa Zjednoczonego Królestwa w drodze ustawy o ochronie danych z 1984 r., którą zastąpiono DPA 1998, a następnie DPA 2018 (w związku z RODO UK). W 2018 r. Zjednoczone Królestwo podpisało również Protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (znany jako konwencja nr 108+) i obecnie pracuje nad ratyfikacją tej konwencji.

([11]) Art. 6 i 8 EKPC (zob. również załącznik 1 do ustawy o prawach człowieka z 1998 r.).

([12]) Art. 6 ustawy o prawach człowieka z 1998 r.

([13]) Art. 3 ustawy o prawach człowieka z 1998 r.

([14]) Umowa o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej, 2019/C 384 I/01, XT/21054/2019/INIT (Dz.U. C 384I z 12.11.2019, s. 1), dostępna pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN.

([15]) Dyrektywa 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 uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89), dostępna pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L0680&from=EN.

([16]) Ustawa o ochronie danych z 2018 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) Aby przygotować się do wystąpienia z UE, rząd Zjednoczonego Królestwa przyjął Ustawę o wystąpieniu z Unii Europejskiej z 2018 r. ([17]), która wprowadza do prawa Zjednoczonego Królestwa przepisy Unii mające bezpośrednie zastosowanie ([18]). To tzw. „pozostające w mocy prawo Unii" obejmuje rozporządzenie (UE) 2016/679 w całości (włącznie z motywami) ([19]). Zgodnie z tym aktem sądy Zjednoczonego Królestwa muszą dokonywać wykładni tego niezmienionego, pozostającego w mocy prawa Unii zgodnie ze stosownym orzecznictwem Trybunału Sprawiedliwości i ogólnymi zasadami prawa Unii obowiązującymi bezpośrednio przed zakończeniem okresu przejściowego (zwanymi odpowiednio „pozostającym w mocy orzecznictwem UE" i „pozostającymi w mocy ogólnymi zasadami prawa Unii") ([20]).

(14) Zgodnie z Ustawą o wystąpieniu z Unii Europejskiej z 2018 r. ministrowie Zjednoczonego Królestwa są uprawnieni do uchwalania przepisów wykonawczych w drodze aktów zwanych *statutory instruments*, aby wprowadzać niezbędne zmiany w pozostającym w mocy prawie Unii Europejskiej w następstwie wystąpienia Zjednoczonego Królestwa z Unii Europejskiej. Uprawnienie to wykonali za pomocą rozporządzenia w sprawie ochrony danych, prywatności i łączności elektronicznej wprowadzającego zmiany w związku z wyjściem z UE z 2019 r. (rozporządzenie w sprawie ochrony danych, prywatności i łączności elektronicznej) ([21]). Rozporządzeniem tym zmieniono rozporządzenie (UE) 2016/679 wprowadzone do prawa Zjednoczonego Królestwa Ustawą o wystąpieniu z Unii Europejskiej z 2018 r., DPA 2018 oraz inne ustawodawstwo w dziedzinie ochrony danych w celu dostosowania ich do kontekstu krajowego ([22]).

(15) W związku z tym po zakończeniu okresu przejściowego ramy prawne dotyczące ochrony danych osobowych w Zjednoczonym Królestwie obejmują:

— RODO UK, wprowadzone do prawa Zjednoczonego Królestwa na mocy Ustawy o wystąpieniu z Unii Europejskiej z 2018 r. i zmienione rozporządzeniem w sprawie ochrony danych, prywatności i łączności elektronicznej ([23]), oraz

— DPA 2018 ([24]), zmieniona rozporządzeniem w sprawie ochrony danych, prywatności i łączności elektronicznej.

(16) Ponieważ RODO UK opiera się na przepisach UE, przepisy o ochronie danych w Zjednoczonym Królestwie w wielu aspektach ściśle odzwierciedlają odpowiednie przepisy mające zastosowanie w Unii Europejskiej.

(17) Oprócz uprawnień przyznanych Sekretarzowi Stanu na mocy Ustawy o wystąpieniu z Unii Europejskiej z 2018 r. w kilku przepisach DPA 2018 przyznano Sekretarzowi Stanu uprawnienia do przyjęcia przepisów wykonawczych w celu zmiany niektórych przepisów ustawy lub przyjęcia przepisów uzupełniających i dodatkowych ([25]). Dotychczas Sekretarz Stanu wykonywał wyłącznie uprawnienie wynikające z art. 137 DPA 2018 do przyjęcia rozporządze-

([17]) Ustawa o wystąpieniu z Unii Europejskiej z 2018 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) Celem i skutkiem Ustawy o wystąpieniu z Unii Europejskiej z 2018 r. jest to, aby wszystkie bezpośrednio stosowane przepisy Unii, które zostały wprowadzone do prawa Zjednoczonego Królestwa na koniec okresu przejściowego, były częścią prawa Zjednoczonego Królestwa z takim samym skutkiem, jaki wywoływały w prawie Unii bezpośrednio przed końcem okresu przejściowego – zob. art. 3 Ustawy o wystąpieniu z Unii Europejskiej z 2018 r.

([19]) W Notach wyjaśniających do Ustawy o wystąpieniu z Unii Europejskiej z 2018 r. określono, że: „W przypadku przekształcenia przepisów na mocy tego artykułu samo brzmienie przepisów stanie się częścią ustawodawstwa krajowego. Będzie ono obejmować pełen tekst każdego aktu UE (w tym motywy)". (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 informacjami przekazanymi przez władze Zjednoczonego Królestwa, ponieważ motywy nie mają statusu wiążących przepisów prawnych, nie było konieczności ich zmiany w taki sam sposób, w jaki artykuły rozporządzenia (UE) 2016/679 zmieniono rozporządzeniem w sprawie ochrony danych, prywatności i łączności elektronicznej.

([20]) Art. 6 Ustawy o wystąpieniu z Unii Europejskiej z 2018 r.

([21]) 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 w sprawie ochrony danych, prywatności i łączności elektronicznej z 2020 r., dostępnym pod adresem: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Wspomniane zmiany RODO UK i DPA 2018 mają głównie charakter techniczny, jak np. usunięcie odniesień do „państw członkowskich" lub dostosowanie terminologii, np. zastąpienie odniesień do rozporządzenia (UE) 2016/679 odniesieniami do RODO UK. W niektórych przypadkach zmiany były wymagane w celu odzwierciedlenia czysto krajowego kontekstu przepisów, na przykład w odniesieniu do tego, kto przyjmuje „rozporządzenie stwierdzające odpowiedni stopień ochrony" na potrzeby ram prawnych dotyczących ochrony danych w Zjednoczonym Królestwie (zob. art. 17A DPA 2018), tj. Sekretarz Stanu zamiast Komisji Europejskiej.

([23]) Ogólne rozporządzenie o ochronie danych (*General Data Protection Regulation*), wersja z uwzględnieniem zmian (tzw. Keeling Schedule), dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) Ustawa o ochronie danych z 2018 r. (*Data Protection Act 2018*), wersja z uwzględnieniem zmian (tzw. Keeling Schedule), dostępna pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Uprawnienia takie są zawarte m.in. w art. 16 (uprawnienie do przewidywania – w szczególnych, ściśle określonych sytuacjach – dalszych wyłączeń od przepisów szczegółowych RODO UK), art. 17A (uprawnienie do przyjmowania rozporządzeń stwierdzających odpowiedni stopień ochrony), art. 212 i 213 (uprawnienie do rozpoczynania procesu legislacyjnego i wprowadzania przepisów przejściowych) oraz art. 211 (uprawnienie do wprowadzania zmian nieznacznych i następczych) DPA 2018.

nia zmieniającego w sprawie opłat i informacji dotyczących ochrony danych z 2019 r., określającego okoliczności, w których administratorzy danych są zobowiązani do uiszczenia rocznej opłaty na rzecz niezależnego organu ochrony danych Zjednoczonego Królestwa – Komisarza ds. Informacji.

(18) Ponadto dalsze wytyczne dotyczące ustawodawstwa Zjednoczonego Królestwa w dziedzinie ochrony danych przedstawiono w kodeksach postępowania i innych wytycznych przyjętych przez Komisarza ds. Informacji. Chociaż formalnie wytyczne te nie są prawnie wiążące, mają znaczenie dla wykładni i przedstawiają, w jaki sposób ustawodawstwo w dziedzinie ochrony danych ma zastosowanie i jest egzekwowane przez Komisarza w praktyce. W szczególności w art. 121–125 DPA 2018 nałożono na Komisarza obowiązek opracowania kodeksów postępowania dotyczących udostępniania danych, marketingu bezpośredniego, projektowania dostosowanego do wieku oraz ochrony danych i dziennikarstwa.

(19) Pod względem struktury i głównych elementów ramy prawne Zjednoczonego Królestwa mające zastosowanie do danych przekazywanych na podstawie niniejszej decyzji są zatem bardzo podobne do ram obowiązujących w Unii Europejskiej. Jest to związane z faktem, że ramy takie opierają się nie tylko na zobowiązaniach ustanowionych w prawie krajowym, które zostało ukształtowane przez prawo Unii, ale również na zobowiązaniach zapisanych w prawie międzynarodowym, w szczególności w rezultacie przystąpienia przez Zjednoczone Królestwo do europejskiej konwencji praw człowieka i konwencji nr 108, a także poddania się jurysdykcji Europejskiego Trybunału Praw Człowieka. W związku z tym wspomniane zobowiązania wynikające z prawnie wiążących instrumentów międzynarodowych, dotyczące zwłaszcza ochrony danych osobowych, stanowią szczególnie ważny element ram prawnych będących przedmiotem oceny w niniejszej decyzji.

### 2.3. **Zakres przedmiotowy i terytorialny**

(20) Podobnie do rozporządzenia (UE) 2016/679 RODO UK ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany lub do przetwarzania w sposób inny niż zautomatyzowany, jeżeli dane osobowe stanowią część zbioru danych ([26]). Definicje pojęć „dane osobowe", „osoba, której dane dotyczą" i „przetwarzanie" w RODO UK są takie same jak definicje tych pojęć w rozporządzeniu (UE) 2016/679 ([27]). Ponadto RODO UK ma zastosowanie do ręcznego przetwarzania nieusystematyzowanych danych osobowych ([28]) przechowywanych przez niektóre organy publiczne Zjednoczonego Królestwa ([29]), chociaż zasady i prawa określone w RODO UK, które nie są związane z takimi danymi osobowymi, nie mają już zastosowania na mocy art. 24 i 25 DPA 2018. Podobnie do zakresu rozporządzenia (UE) 2016/679 RODO UK nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze ([30]).

(21) RODO UK obejmuje swoim zakresem także przetwarzanie w ramach działalności, która bezpośrednio przed końcem okresu przejściowego nie wchodziła w zakres prawa Unii Europejskiej (np. bezpieczeństwo narodowe) ([31]) lub wchodziła w zakres tytułu V rozdział 2 Traktatu o Unii Europejskiej (działania w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa) ([32]). Podobnie jak w systemie Unii Europejskiej RODO UK nie ma zastosowania do przetwarzania danych osobowych przez właściwy organ do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed

([26]) Art. 2 ust. 1 i 5 RODO UK.

([27]) Art. 4 ust. 1 i 2 RODO UK.

([28]) Ręczne nieusystematyzowane przetwarzanie danych osobowych zdefiniowano w art. 2 ust. 5 lit. b) jako przetwarzanie danych osobowych, które nie jest zautomatyzowanym ani usystematyzowanym przetwarzaniem danych osobowych.

([29]) Art. 2 ust. 1A RODO UK stanowi, że rozporządzenie to ma zastosowanie również do ręcznego, nieusystematyzowanego przetwarzania danych osobowych przechowywanych przez organ publiczny, o którym mowa w ustawie o swobodnym dostępie do informacji. Odniesienie do organów publicznych, o których mowa w ustawie o swobodnym dostępie do informacji, oznacza wszelkie organy publiczne zdefiniowane w ustawie o swobodnym dostępie do informacji z 2000 r. lub wszelkie szkockie organy publiczne zdefiniowane w ustawie o swobodnym dostępie do informacji w Szkocji z 2002 r. (asp 13). Art. 21 ust. 5 DPA 2018.

([30]) Art. 2 ust. 2 lit. a) RODO UK.

([31]) Działania w obszarze bezpieczeństwa narodowego są objęte zakresem RODO UK wyłącznie w stopniu, w jakim nie są prowadzone przez właściwy organ do celów ścigania przestępstw, w którym to przypadku zastosowanie ma część 3 DPA 2018, lub przez służbę wywiadowczą lub w jej imieniu, której działania są wyłączone z zakresu RODO UK i podlegają części 4 DPA 2018 zgodnie z art. 2 ust. 2 lit. c) RODO UK. Na przykład siły policyjne mogą przeprowadzać kontrole bezpieczeństwa wobec pracownika, aby upewnić się, że można mu powierzyć dostęp do materiałów związanych z bezpieczeństwem narodowym. Mimo że policja jest właściwym organem do celów ścigania przestępstw, przedmiotowe przetwarzanie nie służy celom ścigania przestępstw i zastosowanie miałoby RODO UK. Zob. Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Ramy dotyczące ochrony danych związanych z bezpieczeństwem narodowym i uprawnień dochodzeniowo-śledczych, s. 8, dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Art. 2 ust. 1 lit. a) i b) RODO UK.

zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (tzw. „cele ścigania przestępstw") – takie przetwarzanie reguluje natomiast część 3 DPA 2018, tak jak ma to miejsce w przypadku dyrektywy (UE) 2016/680 na gruncie prawa Unii Europejskiej – ani przetwarzania danych osobowych przez służby wywiadowcze (Służbę Bezpieczeństwa, Tajną Służbę Wywiadowczą i Centralę Łączności Rządowej), które obejmuje część 4 DPA 2018 ([33]).

(22) Zakres terytorialny RODO UK jest opisany w art. 3 RODO UK ([34]) i obejmuje przetwarzanie danych osobowych (niezależnie od miejsca, w którym się ono odbywa) w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Zjednoczonym Królestwie, jak również przetwarzanie danych osobowych osób przebywających w Zjednoczonym Królestwie, jeżeli czynności przetwarzania dotyczą oferowania towarów lub usług takim osobom lub monitorowania ich zachowania ([35]). Odzwierciedla to podejście przyjęte w art. 3 rozporządzenia (UE) 2016/679.

### 2.4. **Definicje danych osobowych i pojęć administratora i podmiotu przetwarzającego**

(23) Definicje danych osobowych, przetwarzania, administratora, podmiotu przetwarzającego, a także definicja pseudonimizacji, określone w rozporządzeniu (UE) 2016/679, są zachowane w RODO UK bez istotnych zmian ([36]). Ponadto szczególne kategorie danych są zdefiniowane w art. 9 ust. 1 RODO UK w taki sam sposób, jak w rozporządzeniu (UE) 2016/679 („ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby"). Art. 205 DPA 2018 zawiera definicję „danych biometrycznych" ([37]), „danych dotyczących zdrowia" ([38]) i „danych genetycznych" ([39]).

### 2.5. **Zabezpieczenia, prawa i obowiązki**

#### 2.5.1. *Zgodność z prawem i rzetelność przetwarzania*

(24) Dane osobowe powinno się przetwarzać zgodnie z prawem i rzetelnie.

(25) Zasady zgodności z prawem, rzetelności i przejrzystości oraz podstawy zgodności przetwarzania z prawem są zagwarantowane w prawie Zjednoczonego Królestwa poprzez art. 5 ust. 1 lit. a) i art. 6 ust. 1 RODO UK, które są identyczne z odpowiednimi przepisami rozporządzenia (UE) 2016/679 ([40]). Art. 8 DPA 2018 uzupełnia art. 6 ust. 1 lit. e), stanowiąc, że przetwarzanie danych osobowych na podstawie art. 6 ust. 1 lit. e) RODO UK (niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej przez

([33]) Art. 2 ust. 2 lit. b) i c) RODO UK.

([34]) Ten sam zakres terytorialny ma zastosowanie do przetwarzania danych osobowych na podstawie części 2 DPA 2018, która uzupełnia RODO UK (art. 207 ust. 1A).

([35]) Oznacza to w szczególności, że DPA 2018, a tym samym niniejsza decyzja nie ma zastosowania do terytoriów zależnych Korony Brytyjskiej (Jersey, Guernsey i Wyspy Man) ani innych terytoriów zamorskich Zjednoczonego Królestwa, takich jak Falklandy i terytorium Gibraltaru.

([36]) Art. 4 ust. 1, 2, 5, 7 i 8 RODO UK.

([37]) „Dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

([38]) „Dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

([39]) „Dane genetyczne" oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

([40]) Zgodnie z art. 6 ust. 1 RODO UK przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim: a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

administratora) obejmuje przetwarzanie danych osobowych, które jest niezbędne do sprawowania wymiaru sprawiedliwości, sprawowania funkcji przez którąkolwiek z izb parlamentu, sprawowania funkcji powierzonej danej osobie na mocy przepisu prawa stanowionego lub precedensowego, sprawowania władzy królewskiej, funkcji ministerstwa lub departamentu rządowego bądź działania wspierającego lub promującego zaangażowanie demokratyczne.

(26) W odniesieniu do zgody (jednej z podstaw zgodności przetwarzania z prawem) w RODO UK również zachowano warunki przewidziane w art. 7 rozporządzenia (UE) 2016/679 w niezmienionej formie, tj. administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę, pisemne zapytanie o zgodę musi być przedstawione jasnym i prostym językiem, osoba, której dane dotyczą, musi mieć prawo w dowolnym momencie wycofać zgodę, a oceniając, czy zgodę wyrażono dobrowolnie, należy wziąć pod uwagę, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy. Ponadto zgodnie z art. 8 RODO UK, w związku ze świadczeniem usług społeczeństwa informacyjnego zgoda dziecka jest zgodna z prawem tylko wtedy, gdy wiek dziecka wynosi co najmniej 13 lat. Mieści się to w przedziale wiekowym ustanowionym w art. 8 rozporządzenia (UE) 2016/679.

2.5.2. *Przetwarzanie szczególnych kategorii danych osobowych*

(27) Jeżeli przetwarzane są „szczególne kategorie" danych, powinny istnieć szczególne zabezpieczenia.

(28) RODO UK i DPA 2018 zawierają przepisy szczególne dotyczące przetwarzania szczególnych kategorii danych osobowych, które zdefiniowano w art. 9 ust. 1 RODO UK w taki sam sposób, jak w rozporządzeniu (UE) 2016/679 (zob. motyw 23 powyżej). Zgodnie z art. 9 RODO UK przetwarzanie szczególnych kategorii danych jest zasadniczo zabronione, chyba że ma zastosowanie szczególny wyjątek.

(29) W wyjątkach tych (wymienionych w art. 9 ust. 2 i 3 RODO UK) nie wprowadzono żadnych zmian merytorycznych w stosunku do wyjątków zawartych w art. 9 ust. 2 i 3 rozporządzenia (UE) 2016/679. O ile osoba, której dane dotyczą, nie wyraziła wyraźnej zgody na przetwarzanie tych danych osobowych, przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne tylko w szczególnych i ograniczonych okolicznościach. W większości przypadków przetwarzanie danych wrażliwych musi być niezbędne do konkretnego celu określonego w odpowiednim przepisie (zob. art. 9 ust. 2 lit. b), c), f), g), h), i) oraz j)).

(30) Ponadto, w przypadku gdy wyjątek na podstawie art. 9 ust. 2 RODO UK wymaga zezwolenia z mocy prawa lub odnosi się do interesu publicznego, w art. 10 DPA 2018 oraz w załączniku 1 do tej ustawy dodatkowo określono warunki, które muszą być spełnione, aby można było powołać się na te wyjątki. Na przykład w przypadku przetwarzania danych wrażliwych w celu ochrony „zdrowia publicznego" (art. 9 ust. 2 lit. i) RODO UK), w załączniku 1 część 1 pkt 3 lit. b) wymaga się, aby oprócz kryterium niezbędności takie przetwarzanie było prowadzone „przez pracownika służby zdrowia lub na jego odpowiedzialność" lub „przez inną osobę, która jest zobowiązana do zachowania poufności na mocy przepisu prawa stanowionego lub precedensowego", w tym na mocy ugruntowanego w *common law* obowiązku zachowania poufności.

(31) W przypadku przetwarzania danych wrażliwych ze względów związanych z ważnym interesem publicznym (art. 9 ust. 2 lit. g) RODO UK), część 2 załącznika 1 do DPA 2018 zawiera wyczerpujący wykaz celów, które można uznać za leżące w ważnym interesie publicznym, oraz określa – dla każdego z tych celów – konkretne warunki dodatkowe. Za ważny interes publiczny uznaje się na przykład promowanie różnorodności rasowej i etnicznej na wyższych szczeblach organizacji. Przetwarzanie danych wrażliwych w tym konkretnym celu podlega szczegółowym wymogom, w tym wymogowi, aby przetwarzanie odbywało się w ramach procesu identyfikacji osób odpowiednich do zajmowania wyższych stanowisk, było niezbędne do promowania różnorodności rasowej i etnicznej oraz aby wyrządzenie znacznej szkody lub spowodowanie znaczących niedogodności dla osoby, której dane dotyczą, nie było prawdopodobne.

(32) W art. 11 ust. 1 DPA 2018 ustanowiono warunki przetwarzania danych osobowych w okolicznościach opisanych w art. 9 ust. 3 RODO UK odnoszącym się do obowiązku zachowania tajemnicy. Obejmuje to okoliczności, w których przetwarzanie jest prowadzone przez pracownika służby zdrowia lub pracownika opieki społecznej bądź przez inną osobę, która w tych okolicznościach jest zobowiązana do zachowania poufności na mocy przepisu prawa stanowionego lub precedensowego, lub na odpowiedzialność takiego pracownika lub takiej osoby.

(33) Ponadto korzystanie z wielu wyjątków wymienionych w art. 9 ust. 2 RODO UK wymaga odpowiednich i szczególnych zabezpieczeń. W zależności od charakteru przetwarzania i poziomu ryzyka dla praw i wolności osób, których dane dotyczą, w warunkach przetwarzania przewidzianych w załączniku 1 do DPA 2018 ustanowiono różne zabezpieczenia. Z kolei w załączniku 1 określono warunki dla każdej sytuacji przetwarzania.

(34) W niektórych przypadkach DPA 2018 reguluje i ogranicza rodzaj danych wrażliwych, które można przetwarzać pod kątem spełnienia konkretnej podstawy prawnej. W pkt 8 załącznika 1 zezwala się na przykład na przetwarzanie danych wrażliwych do celów promowania równości szans lub równego traktowania. Ten warunek przetwarzania można zastosować tylko wtedy, gdy dane ujawniają pochodzenie rasowe lub etniczne, przekonania religijne lub światopoglądowe, orientację seksualną lub gdy są to dane dotyczące zdrowia.

(35) W niektórych przypadkach w DPA 2018 ograniczono możliwość stosowania tego warunku przetwarzania do określonego rodzaju administratora. W pkt 23 załącznika 1 przewidziano na przykład przetwarzanie danych wrażliwych w związku z odpowiedziami wybieranych przedstawicieli na pytania obywateli Ten warunek przetwarzania można zastosować tylko wtedy, gdy administrator jest wybranym przedstawicielem lub działa z jego upoważnienia.

(36) W niektórych innych przypadkach w DPA 2018 określono ograniczenia dotyczące kategorii osób, których dane dotyczą, w odniesieniu do warunku przetwarzania, który ma być stosowany. Pkt 21 załącznika 1 reguluje na przykład przetwarzanie danych wrażliwych na potrzeby pracowniczych programów emerytalnych. Warunek ten można zastosować wyłącznie wówczas, gdy osoba, której dane dotyczą, jest siostrą lub bratem bądź jednym z rodziców, dziadków lub pradziadków członka programu.

(37) Ponadto w przypadku powoływania się na wyjątki zawarte w art. 9 ust. 2 RODO UK, które doprecyzowano w art. 10 DPA 2018 wraz z załącznikiem 1 do tej ustawy, administrator w większości przypadków jest zobowiązany do sporządzenia „odpowiedniego dokumentu dotyczącego polityki". W dokumencie tym muszą się znaleźć procedury administratora danych mające na celu zapewnienie zgodności z zasadami określonymi w art. 5 RODO UK. Muszą się w nim również znaleźć zasady dotyczące zatrzymywania i usuwania danych, ze wskazaniem prawdopodobnego okresu przechowywania. W stosownych przypadkach administratorzy muszą dokonać przeglądu i aktualizacji tego dokumentu. Administrator musi przechowywać dokument programowy przez sześć miesięcy po zakończeniu przetwarzania i musi udostępnić go na żądanie Komisarzowi ds. Informacji ([41]).

(38) Zgodnie z pkt 41 załącznika 1 do DPA 2018 dokumentowi dotyczącemu polityki musi zawsze towarzyszyć rozszerzony rejestr przetwarzania. W rejestrze tym należy odnotowywać wywiązywanie się z zobowiązań zawartych w dokumencie dotyczącym polityki, tj. czy dane są usuwane lub zatrzymywane zgodnie z przyjętą polityką. Jeśli nie stosowano się do przyjętej polityki, w rejestrze należy odnotować przyczyny. W rejestrze należy również opisać, w jaki sposób przetwarzanie spełnia warunki określone w art. 6 RODO UK (zgodność przetwarzania z prawem) i konkretny warunek określony w załączniku 1 do DPA 2018, na który się powołano.

(39) Ponadto, podobnie jak rozporządzenie (UE) 2016/679, RODO UK przewiduje również ogólne zabezpieczenia niektórych operacji przetwarzania szczególnych kategorii danych. W art. 35 RODO UK znajduje się wymóg przeprowadzenia oceny skutków dla ochrony danych, jeśli przetwarzanie szczególnych kategorii danych odbywa się na dużą skalę. Zgodnie z art. 37 RODO UK administrator lub podmiot przetwarzający musi wyznaczyć inspektora ochrony danych, gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu szczególnych kategorii danych na dużą skalę.

(40) W odniesieniu do danych osobowych dotyczących wyroków skazujących i czynów zabronionych art. 10 RODO UK ma takie samo brzmienie jak art. 10 rozporządzenia (UE) 2016/679. Umożliwia przetwarzanie danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem krajowym przewidującym odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

(41) Jeśli przetwarzanie danych dotyczących wyroków skazujących oraz czynów zabronionych nie odbywa się pod nadzorem władz publicznych, art. 10 ust. 5 DPA 2018 stanowi, że takie przetwarzanie może odbywać się wyłącznie w konkretnych celach lub sytuacjach określonych w częściach 1, 2 i 3 załącznika 1 do DPA 2018 i podlega szczegółowym wymogom, które określono dla każdego z tych celów/każdej z tych sytuacji. Na przykład przetwarzanie danych dotyczących wyroków skazujących przez podmioty niezarobkowe może odbywać się, jeśli przetwarzania dokonuje się a) w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, b) pod warunkiem że (i) przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że (ii) dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą.

([41]) Pkt 38–40 załącznika 1 do DPA 2018.

(42) Ponadto w części 3 załącznika 1 do DPA 2018 określono dalsze okoliczności, w których można wykorzystywać dane dotyczące wyroków skazujących, odpowiadające podstawom prawnym przetwarzania danych wrażliwych określonym w art. 9 ust. 2 rozporządzenia (UE) 2016/679 i RODO UK (np. zgoda osoby, której dane dotyczą, żywotne interesy osoby fizycznej, jeśli osoba, której dane dotyczą, jest prawnie lub fizycznie niezdolna do wyrażenia zgody, jeśli dane zostały już w sposób oczywisty upublicznione przez osobę, której dane dotyczą, jeśli przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczenia itp.).

2.5.3. *Ograniczenie celu, prawidłowość, minimalizacja danych, ograniczenie przechowywania i bezpieczeństwo danych*

(43) Dane osobowe powinny być przetwarzane w określonym celu, a następnie wykorzystywane tylko w takim zakresie, w jakim nie jest to niezgodne z celem przetwarzania.

(44) Zasadę tę przewidziano w art. 5 ust. 1 lit. b) rozporządzenia (UE) 2016/679 i zachowano bez zmian w art. 5 ust. 1 lit. b) RODO UK. Warunki dotyczące dalszego zgodnego z celem przetwarzania, o których mowa w art. 6 ust. 4 rozporządzenia (UE) 2016/679, zachowano również bez istotnych zmian w art. 6 ust. 4 lit. a)–e) RODO UK.

(45) Ponadto dane powinny być prawidłowe i w razie potrzeby uaktualniane. Powinny być również adekwatne, stosowne oraz ograniczone do celów, w których są przetwarzane, a także co do zasady przechowywane przez okres nie dłuższy niż jest to niezbędne do celów, w których przetwarza się dane osobowe.

(46) Te zasady minimalizacji danych, prawidłowości i ograniczenia przechowywania określono w art. 5 ust. 1 lit. c)–e) rozporządzenia (UE) 2016/679 i zachowano bez zmian w art. 5 ust. 1 lit. c)–e) RODO UK.

(47) Dane osobowe powinny być również przetwarzane w sposób zapewniający im bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. W tym celu podmioty gospodarcze powinny wdrożyć odpowiednie środki techniczne lub organizacyjne, aby chronić dane osobowe przed ewentualnymi zagrożeniami. Środki te należy ocenić, biorąc pod uwagę stan wiedzy technicznej oraz koszty ich wdrożenia.

(48) Bezpieczeństwo danych jest zapisane w prawie Zjednoczonego Królestwa za pomocą zasady integralności i poufności w art. 5 ust. 1 lit. f) RODO UK oraz w art. 32 RODO UK dotyczącym bezpieczeństwa przetwarzania. Przepisy te są takie same jak odpowiednie przepisy rozporządzenia (UE) 2016/679. Ponadto, na tych samych warunkach, jak określone w art. 33 i 34 rozporządzenia (UE) 2016/679, RODO UK zawiera wymóg zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO UK) oraz zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO UK).

2.5.4. *Przejrzystość*

(49) Osoby, których dane dotyczą, powinny być informowane o głównych cechach przetwarzania ich danych osobowych.

(50) Zapewniają to art. 13 i 14 RODO UK, które, oprócz ogólnej zasady przejrzystości, określają przepisy dotyczące informacji, których należy udzielać osobom, których dane dotyczą ([42]). W RODO UK nie wprowadzono żadnych istotnych zmian tych przepisów w porównaniu z odpowiednimi artykułami rozporządzenia (UE) 2016/679. Podobnie jak w przypadku rozporządzenia (UE) 2016/679, wymogi dotyczące przejrzystości zawarte w tych artykułach podlegają jednak kilku wyjątkom określonym w DPA 2018 (zob. motywy 55–72).

([42]) W art. 13 ust. 1 lit. f) i art. 14 ust. 1 lit. f) odniesienia do decyzji Komisji stwierdzających odpowiedni stopień ochrony zastąpiono odniesieniami do równoważnego aktu Zjednoczonego Królestwa, tj. rozporządzeń stwierdzających odpowiedni stopień ochrony na podstawie DPA 2018. Ponadto w art. 14 ust. 5 lit. c)–d) odniesienia do prawa Unii lub prawa państwa członkowskiego zastąpiono odniesieniem do prawa krajowego (jako przykłady takiego przepisu krajowego, który może wchodzić w zakres stosowania art. 14 ust. 5 lit. c), Zjednoczone Królestwo wymieniło art. 7 ustawy o sprzedawcach złomu z 2013 r., w którym określono przepisy dotyczące rejestru pozwoleń na obrót złomem, lub część 35 ustawy o spółkach z 2006 r., w której to części określono przepisy dotyczące urzędnika rejestru spółek. Podobnie przykładem przepisu krajowego, który może wchodzić w zakres stosowania art. 14 ust. 5 lit. d), mogą być przepisy określające zasady tajemnicy zawodowej, zobowiązania odzwierciedlone w umowach o pracę lub wynikający z *common law* obowiązek zachowania poufności (np. dane osobowe przetwarzane przez pracowników służby zdrowia, działy zasobów ludzkich, pracowników socjalnych itp.).

2.5.5. *Prawa indywidualne*

(51) Osobom, których dane dotyczą, powinny przysługiwać określone prawa, które można egzekwować wobec administratora lub podmiotu przetwarzającego, w szczególności prawo dostępu do zebranych danych, prawo do sprzeciwu wobec przetwarzania oraz prawo do sprostowania i usunięcia danych. Jednocześnie prawa te mogą podlegać ograniczeniom w zakresie, w jakim ograniczenia te są niezbędne i proporcjonalne do ochrony bezpieczeństwa publicznego lub innych ważnych celów leżących w ogólnym interesie publicznym.

2.5.5.1. Prawa podmiotowe

(52) W RODO UK osobom fizycznym przyznano te same egzekwowalne prawa co w rozporządzeniu (UE) 2016/679. Przepisy zapewniające prawa osób fizycznych utrzymano w RODO UK bez istotnych zmian.

(53) Prawa te obejmują prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO UK), prawo do sprostowania danych (art. 16 RODO UK), prawo do usunięcia danych (art. 17 RODO UK), prawo do ograniczenia przetwarzania (art. 18 RODO UK), obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO UK), prawo do przenoszenia danych (art. 20 RODO UK) oraz prawo do sprzeciwu (art. 21 RODO UK) ([43]). Prawo do sprzeciwu obejmuje również prawo osoby, której dane dotyczą, do sprzeciwu wobec przetwarzania danych osobowych na potrzeby marketingu bezpośredniego przewidziane w art. 21 ust. 2 i 3 rozporządzenia (UE) 2016/679. Ponadto, zgodnie z art. 122 DPA 2018, Komisarz ds. Informacji musi przygotować kodeks postępowania dotyczący prowadzenia marketingu bezpośredniego zgodnie z wymogami zawartymi w ustawodawstwie w dziedzinie ochrony danych (oraz rozporządzeniu w sprawie prywatności i łączności elektronicznej w związku z dyrektywą WE z 2003 r.) oraz innymi tego rodzaju wytycznymi służącymi promowaniu dobrych praktyk w zakresie marketingu bezpośredniego, które Komisarz uzna za stosowne. Biuro Komisarza ds. Informacji opracowuje obecnie kodeks marketingu bezpośredniego ([44]).

(54) W RODO UK bez istotnych zmian zachowano również prawo osoby, której dane dotyczą, do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, które wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa zgodnie z art. 22 RODO. Dodano jednak nowy ustęp 3A, aby uwzględnić fakt, że w art. 14 DPA 2018 określono zabezpieczenia praw, wolności i uzasadnionych interesów osób, których dane dotyczą, w przypadku gdy przetwarzanie odbywa się na podstawie art. 22 ust. 2 lit. b) RODO UK. Dotyczy to wyłącznie sytuacji, w której podstawą takiej decyzji jest zezwolenie lub wymóg wynikający z prawa Zjednoczonego Królestwa, i nie dotyczy sytuacji, w której decyzja jest niezbędna na podstawie umowy lub osoba, której dane dotyczą, wyraziła wyraźną zgodę na jej podjęcie. W przypadkach gdy ma zastosowanie art. 14 DPA 2018, administrator musi, w możliwie najkrótszym czasie, powiadomić na piśmie osobę, której dane dotyczą, że decyzję podjęto wyłącznie na podstawie zautomatyzowanego przetwarzania. Osoba, której dane dotyczą, ma prawo zwrócić się do administratora – w terminie miesiąca od otrzymania zawiadomienia – o ponowne rozpatrzenie decyzji lub podjęcie nowej decyzji, która nie będzie oparta wyłącznie na zautomatyzowanym przetwarzaniu. Sekretarz Stanu jest uprawniony do przyjęcia dalszych gwarancji w odniesieniu do zautomatyzowanego podejmowania decyzji. Uprawnienie to nie jest jeszcze wykonywane.

2.5.5.2. Ograniczenia praw indywidualnych i inne przepisy

(55) W DPA 2018 określono kilka ograniczeń praw indywidualnych, które mieszczą się w ramach art. 23 RODO UK. We wspomnianych ramach nie wprowadza się żadnych ograniczeń dotyczących prawa do sprzeciwu wobec marketingu bezpośredniego przewidzianego w art. 21 ust. 2 i 3 RODO UK ani prawa do tego, by nie podlegać zautomatyzowanemu podejmowaniu decyzji, o którym mowa w art. 22 RODO UK.

(56) Ograniczenia te określono w załącznikach 2–4 do DPA 2018. Władze Zjednoczonego Królestwa wyjaśniły, że kierują się dwiema zasadami: zasadą szczegółowości (przyjmowanie szczegółowego podejścia, dzielenie szeroko zakrojonych ograniczeń na liczne bardziej szczegółowe przepisy) i zasadą warunkowości (każdemu przepisowi towarzyszą zabezpieczenia w formie ograniczeń lub warunków w celu zapobiegania nadużyciom) ([45]).

([43]) W art. 17 ust. 1 lit. e) i art. 17 ust. 3 lit. b) odniesienia do prawa UE lub państwa członkowskiego zastąpiono odniesieniem do prawa krajowego (jako przykłady takiego prawa krajowego na podstawie art. 17 ust. 1 lit. e) Zjednoczone Królestwo wymieniło rozporządzenie w sprawie informacji o edukacji i uczniach w Anglii z 2006 r., w którym ustanowiono wymóg usunięcia nazwisk uczniów z rejestrów szkolnych po opuszczeniu przez nich szkoły, lub art. 34F ustawy medycznej z 1983 r., w którym określono zasady usuwania nazwisk z rejestru lekarzy ogólnych i rejestru lekarzy specjalistów.

([44]) Projekt kodeksu postępowania jest dostępny pod następującym adresem: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja E: Ograniczenia, s. 1, dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) Ograniczenia opisane w art. 23 ust. 1 RODO UK mają z założenia być stosowane wyłącznie w określonych okolicznościach, w których są one niezbędne w demokratycznym społeczeństwie, oraz w sposób proporcjonalny do wyznaczonego, prawnie uzasadnionego celu. Ponadto zgodnie z utrwalonym orzecznictwem dotyczącym wykładni ograniczeń wyłączenie z zakresu stosowania systemu ochrony danych można zastosować w każdym konkretnych przypadku wyłącznie wtedy, gdy jest to niezbędne i proporcjonalne ([46]). Wymaga się, aby kryterium niezbędności było „rygorystyczne i wymagało, by ingerencja w prawa podmiotu była proporcjonalna do wagi zagrożenia interesu publicznego. W tym celu należy zatem przeprowadzić klasyczną analizę proporcjonalności ([47])".

(58) Cele, jakim mają służyć opisane ograniczenia, odpowiadają celom wymienionym w art. 23 rozporządzenia (UE) 2016/679, z wyjątkiem ograniczeń dotyczących bezpieczeństwa narodowego i obrony, które uregulowano w art. 26 DPA 2018, ale które podlegają tym samym wymogom niezbędności i proporcjonalności (zob. motywy 63–66).

(59) Niektóre ograniczenia, np. ograniczenia związane z zapobieganiem przestępstwom lub ich wykrywaniem, zatrzymywaniem i ściganiem przestępców oraz wymiarem lub pobieraniem podatków lub ceł ([48]), pozwalają na ograniczenie wszystkich praw indywidualnych i obowiązków w zakresie przejrzystości (z wyjątkiem praw określonych w art. 21 ust. 2 i art. 22). Zakres stosowania innych ograniczeń ogranicza się do obowiązków w zakresie przejrzystości i praw dostępu, takich jak ograniczenia związane z prawniczą tajemnicą zawodową ([49]), prawem do wolności od wymogu udzielenia informacji, które prowadziłyby do samooskarżenia ([50]), oraz finansowaniem przedsiębiorstw, w szczególności z zapobieganiem wykorzystywaniu informacji wewnętrznych ([51]). Niewiele z tych ograniczeń pozwala na ograniczenie obowiązku administratora w zakresie informowania osoby, której dane dotyczą, o naruszeniu ochrony danych oraz zasad ograniczenia celu, a także zgodności z prawem, rzetelności i przejrzystości przetwarzania ([52]).

(60) Niektóre ograniczenia są „w pełni" automatycznie stosowane do określonego rodzaju przetwarzania danych osobowych (np. stosowanie obowiązków w zakresie przejrzystości i praw indywidualnych jest wyłączone, w przypadku gdy dane osobowe są przetwarzane do celów oceny, czy dana osoba ma odpowiednie kwalifikacje do pełnienia urzędu sądowego, lub dane osobowe są przetwarzane przez sąd, trybunał lub osobę fizyczną w ramach sprawowania przez nie wymiaru sprawiedliwości).

(61) W większości przypadków w odpowiednim punkcie załącznika 2 do DPA 2018 określono jednak, że ograniczenie ma zastosowanie wyłącznie w przypadku, gdy (i w takim zakresie, w jakim) zastosowanie przepisów „prawdopodobnie byłoby sprzeczne" z prawnie uzasadnionym celem tego ograniczenia: na przykład wymienione przepisy RODO UK nie mają zastosowania do danych osobowych przetwarzanych w celu zapobiegania przestępstwom lub ich wykrywania, zatrzymywania lub ścigania przestępców lub wymiaru lub pobierania podatków lub ceł „w zakresie, w jakim zastosowanie tych przepisów prawdopodobnie byłoby sprzeczne z którąkolwiek z tych kwestii" ([53]).

(62) Zgodnie z wykładnią dokonywaną konsekwentnie przez sądy Zjednoczonego Królestwa sformułowanie „prawdopodobnie byłoby sprzeczne" oznacza „bardzo znaczącą i dużą szansę uszczerbku dla określonych interesów publicznych" ([54]). Na ograniczenie podlegające kryterium sprzeczności można się zatem powołać tylko wówczas i tylko w takim zakresie, w jakim istnieje bardzo znacząca i duża szansa, że przyznanie określonego prawa naruszyłoby określony interes publiczny. Administrator jest odpowiedzialny za ocenę w poszczególnych przypadkach, czy warunki te zostały spełnione ([55]).

(63) Oprócz ograniczeń zawartych w załączniku 2 do DPA 2018 w art. 26 DPA 2018 przewidziano wyłączenie, które można stosować w odniesieniu do określonych przepisów RODO UK i DPA 2018, jeżeli wyłączenie to jest wymagane do celów ochrony bezpieczeństwa narodowego lub do celów obrony. Wspomniane wyłączenie ma zastosowanie do zasad ochrony danych (z wyjątkiem zasady zgodności z prawem), obowiązków w zakresie przejrzystości, praw osoby, której dane dotyczą, obowiązku powiadomienia o naruszeniu ochrony danych, zasad dotyczących międzynarodowego przekazywania danych, niektórych obowiązków i uprawnień Komisarza ds. Informacji, a także

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

([47]) Guriev przeciwko Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), pkt 43. W tej kwestii zob. również Lin przeciwko Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), pkt 80.

([48]) Pkt 2 załącznika 2 do DPA 2018.

([49]) Pkt 19 załącznika 2 do DPA 2018.

([50]) Pkt 20 załącznika 2 do DPA 2018.

([51]) Pkt 21 załącznika 2 do DPA 2018.

([52]) Na przykład ograniczenia prawa do powiadomienia o naruszeniu ochrony danych są dopuszczalne wyłącznie w odniesieniu do przestępczości i podatków (pkt 2 załącznika 2 do DPA 2018), przywileju parlamentarnego (pkt 13 załącznika 2 do DPA 2018) oraz przetwarzania do celów dziennikarskich, akademickich, artystycznych i literackich (art. 26 załącznika 2 do DPA 2018).

([53]) Pkt 2 załącznika 2 do DPA 2018.

([54]) Korona (Lord) przeciwko Secretary of State for the Home Department [2003] EWHC 2073 (Admin), pkt 100 oraz Guriev przeciwko Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), pkt 43.

([55]) Open Rights Group i in., Korona (powodowie) przeciwko Secretary of State for the Home Department i in., pkt 31.

zasad dotyczących środków ochrony prawnej, odpowiedzialności i sankcji, z wyjątkiem przepisu dotyczącego ogólnych warunków nakładania administracyjnych kar pieniężnych określonego w art. 83 RODO UK oraz przepisu dotyczącego sankcji określonego w art. 84 RODO UK. Ponadto w art. 28 DPA 2018 zmieniono zastosowanie art. 9 ust. 1, aby umożliwić przetwarzanie szczególnych kategorii danych określonych w art. 9 ust. 1 RODO UK w zakresie, w jakim przetwarzanie odbywa się w celu zapewnienia bezpieczeństwa narodowego lub w celach obrony oraz przy zapewnieniu odpowiednich zabezpieczeń w odniesieniu do praw i wolności osób, których dane dotyczą ([56]).

(64) Wyłączenie można stosować wyłącznie w zakresie, w jakim jest to wymagane do zapewnienia bezpieczeństwa narodowego lub obronności. Ponieważ dotyczy to również pozostałych wyłączeń określonych w DPA 2018, administrator musi rozpatrywać je i powoływać się na nie w każdym przypadku z osobna. Ponadto każde zastosowanie wyłączenia musi być zgodne ze standardami praw człowieka (opartymi na ustawie o prawach człowieka z 1998 r.), według których w demokratycznym społeczeństwie każda ingerencja w prawo do prywatności powinna być niezbędna i proporcjonalna ([57]).

(65) Taką wykładnię zwolnienia potwierdza Komisarz ds. Informacji, który wydał szczegółowe wytyczne dotyczące stosowania wyłączenia dotyczącego bezpieczeństwa narodowego i obronności, stwierdzając w nich, że administrator musi rozpatrywać je i powoływać się na nie w każdym przypadku z osobna ([58]). W wytycznych podkreślono w szczególności, że „[n]ie jest to wyłączenie ogólne" i że do jego zastosowania „nie wystarczy, aby dane były przetwarzane do celów bezpieczeństwa narodowego". Administrator danych, powołując się na to wyłączenie, musi „wykazać, że istnieje realna możliwość negatywnego wpływu na bezpieczeństwo narodowe", a w razie potrzeby wymaga się od administratora danych „dostarczenia [Komisarzowi ds. Informacji] uzasadnienia skorzystania z tego wyłączenia". Wytyczne zawierają listę kontrolną i szereg przykładów służących dalszemu doprecyzowaniu warunków, na jakich można powoływać się na to wyłączenie.

(66) Fakt, że dane są przetwarzane do celów bezpieczeństwa narodowego lub obrony, nie jest zatem sam w sobie wystarczający do zastosowania wyłączenia. Administrator musi uwzględnić faktyczne konsekwencje dla bezpieczeństwa narodowego, gdyby musiał zastosować się do konkretnego przepisu dotyczącego ochrony danych. Wyłączenie można stosować wyłącznie do przepisów szczegółowych, które określono jako stwarzające ryzyko, i należy je stosować w możliwie najbardziej restrykcyjny sposób ([59]).

(67) Podejście to potwierdził Trybunał ds. Ochrony Danych (Information Tribunal) ([60]). W sprawie Baker przeciwko Secretary of State for the Home Department („Baker przeciwko Secretary of State") Trybunał orzekł, że zastosowanie wyłączenia dotyczącego bezpieczeństwa narodowego jako wyłączenia ogólnego w odniesieniu do wniosków o udzielenie dostępu otrzymanych przez służby wywiadowcze jest niezgodne z prawem. Wyłączenie należy stosować w każdym przypadku z osobna, rozpatrując każdy wniosek indywidualnie i w świetle prawa osób fizycznych do poszanowania ich życia prywatnego ([61]).

([56]) Zgodnie z informacjami dostarczonymi przez władze Zjednoczonego Królestwa, jeżeli przetwarzanie odbywa się w kontekście bezpieczeństwa narodowego, administratorzy będą zazwyczaj stosować wzmocnione zabezpieczenia i środki bezpieczeństwa w odniesieniu do przetwarzania, odzwierciedlające wrażliwy charakter przetwarzania. To, które zabezpieczenia są odpowiednie, będzie zależało od ryzyka związanego z przetwarzaniem. Mogą one obejmować ograniczenia dostępu do danych, tak aby miały do nich dostęp wyłącznie osoby upoważnione posiadające odpowiednie poświadczenie bezpieczeństwa, ścisłe ograniczenia w zakresie udostępniania danych oraz wysoki standard bezpieczeństwa stosowany w procedurach dotyczących przechowywania danych i postępowania z danymi.

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

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

([59]) Zgodnie z przykładem przedstawionym przez władze Zjednoczonego Królestwa, jeżeli osoba podejrzana o terroryzm, w sprawie której MI5 prowadzi dochodzenie, złożyłaby do Home Office wniosek o udzielenie dostępu (np. z uwagi na fakt, że jest zaangażowana w spór z Home Office dotyczący kwestii imigracyjnych), niezbędne byłoby zapewnienie ochrony przed ujawnieniem tej osobie, jakichkolwiek danych, które MI5 ewentualnie udostępniło wcześniej Home Office w związku z trwającymi dochodzeniami, co mogłoby narazić na szwank wrażliwe źródła, metody lub techniki lub prowadzić do zwiększenia zagrożenia stwarzanego przez daną osobę. W takich okolicznościach prawdopodobnie zostałby osiągnięty próg wymagany do zastosowania wyłączenia określonego w art. 26 i wyłączenie od ujawniania informacji byłoby konieczne w celu ochrony bezpieczeństwa narodowego. Jeżeli jednak Home Office posiadałoby również dane osobowe dotyczące wspomnianej osoby, które nie były związane z dochodzeniem MI5 i które to informacje mogłyby zostać przekazane bez ryzyka naruszenia bezpieczeństwa narodowego, wówczas wyłączenie dotyczące bezpieczeństwa narodowego nie miałoby zastosowania przy rozważaniu ujawnienia informacji tej osobie. Komisarz ds. Informacji opracowuje obecnie wytyczne dotyczące sposobu, w jaki administratorzy powinni podchodzić do stosowania wyłączenia przewidzianego w art. 26. Oczekuje się, że wytyczne zostaną opublikowane do końca marca 2021 r.

([60]) Trybunał ds. Ochrony Danych ustanowiono w celu rozpatrywania odwołań w sprawach dotyczących ochrony danych osobowych na mocy ustawy o ochronie danych z 1984 r. W 2010 r. Trybunał ds. Ochrony Danych stał się częścią Izby ds. Regulatorów Trybunału Pierwszej Instancji (General Regulatory Chamber of the First Tier Tribunal) w ramach reformy struktury systemu sądowego Zjednoczonego Królestwa.

([61]) Zob. Baker przeciwko Secretary of State for the Home Department [2001] UKIT NSA2 („Baker przeciwko Secretary of State").

2.5.6. *Ograniczenia dotyczące danych osobowych przetwarzanych do celów dziennikarskich, artystycznych, akademickich i literackich, do celów archiwalnych oraz do celów badań naukowych*

(68) Zgodnie z art. 85 ust. 2 RODO UK możliwe jest wyłączenie danych osobowych przetwarzanych do celów dziennikarskich, artystycznych, akademickich i literackich z szeregu przepisów RODO UK. W części 5 załącznika 2 do DPA 2018 określono wyłączenia dotyczące przetwarzania w tych celach. Przewidziano w niej wyłączenia z zasad ochrony danych (z wyjątkiem zasady integralności i poufności), podstaw prawnych przetwarzania (w tym szczególnych kategorii danych i danych dotyczących wyroków skazujących itp.), warunków wyrażenia zgody, obowiązków w zakresie przejrzystości, praw osób, których dane dotyczą, obowiązku powiadomienia o naruszeniu ochrony danych, wymogu przeprowadzenia konsultacji z Komisarzem ds. Informacji przed przetwarzaniem wysokiego ryzyka oraz zasad dotyczących międzynarodowego przekazywania danych ([62]). W tym zakresie RODO UK nie odbiega w istotny sposób od rozporządzenia (UE) 2016/679, w którym w art. 85 przewidziano możliwość wyłączenia przetwarzania dokonywanego dla potrzeb dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej z szeregu wymogów określonych w rozporządzeniu (UE) 2016/679. Przepisy DPA 2018, zwłaszcza część 5 załącznika 2, są zgodne z RODO UK.

(69) Podstawowy proces ważenia interesów, który należy przeprowadzić zgodnie z art. 85 RODO UK, dotyczy tego, czy wyłączenie od przepisów o ochronie danych wymienionych w motywie 68 jest „niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji" ([63]). Zgodnie z pkt 26 ppkt 2 i 3 załącznika 2 do DPA 2018 Zjednoczone Królestwo stosuje kryterium „zasadnego przekonania" w celu osiągnięcia tej równowagi. Aby wyłączenie było uzasadnione, administrator musi być zasadnie przekonany, (i) że publikacja leży w interesie publicznym; oraz (ii) że zastosowanie odpowiedniego przepisu RODO byłoby niezgodne z celem dziennikarskim, akademickim, artystycznym lub literackim. Jak potwierdzono w orzecznictwie, kryterium „zasadnego przekonania" obejmuje zarówno element subiektywny, jak i obiektywny ([64]): nie wystarczy, aby administrator wykazał, że sam uznał zachowanie zgodności z przepisem za niezgodne z określonym celem. Jego przekonanie musi być uzasadnione, tj. takie, które mogłaby podzielać racjonalnie myśląca osoba, znająca istotne fakty. W związku z tym administrator musi dołożyć należytej staranności, dochodząc do swojego przekonania, aby być w stanie wykazać jego zasadność. Zgodnie z wyjaśnieniami przedstawionymi przez władze Zjednoczonego Królestwa kryterium „zasadnego przekonania" należy stosować w odniesieniu do każdego wyłączenia z osobna ([65]). W przypadku spełnienia warunków wyłączenie uznaje się za niezbędne i proporcjonalne w rozumieniu prawa Zjednoczonego Królestwa.

(70) Zgodnie z art. 124 DPA 2018 Komisarz ds. Informacji ma opracować kodeks postępowania w zakresie ochrony danych i dziennikarstwa. Trwają prace nad tym kodeksem. Na podstawie ustawy o ochronie danych z 1998 r. wydano w tej sprawie wytyczne, w których podkreślono w szczególności, że aby powołać się na opisane wyłączenie, nie wystarczy jedynie stwierdzić, że zgodność z przepisami stanowiłaby utrudnienie dla działalności dziennikarskiej, lecz należy przedstawić wyraźny argument świadczący o tym, że dany przepis stanowi

([62]) Zob. art. 85 RODO UK i część 5 pkt 26 ppkt 9 załącznika 2 do DPA 2018.

([63]) Zgodnie z częścią 5 pkt 26 ppkt 2 załącznika 2 do DPA 2018 wyłączenie ma zastosowanie do przetwarzania danych osobowych dokonywanego w szczególnych celach (dziennikarskich, akademickich, artystycznych i literackich), jeżeli przetwarzanie odbywa się w celu opublikowania przez osobę materiału dziennikarskiego, akademickiego, artystycznego lub literackiego, a administrator jest zasadnie przekonany, że publikacja tego materiału będzie leżała w interesie publicznym. Ustalając, czy publikacja leżałaby w interesie publicznym, administrator musi wziąć pod uwagę szczególne znaczenie interesu publicznego w zakresie wolności wypowiedzi i informacji. Ponadto administrator musi uwzględnić kodeksy postępowania lub wytyczne mające zastosowanie do danej publikacji (wytyczne redakcyjne BBC [BBC Editorial Guidelines], kodeks nadawania Ofcom [Ofcom Broadcasting Code] oraz kodeks postępowania redaktorów [Editors' Code of Practice]). Ponadto, aby wyłączenie miało zastosowanie, administrator musi mieć zasadne przekonanie, że zachowanie zgodności z odpowiednim przepisem byłoby niezgodne ze szczególnymi celami (pkt 26 ppkt 3 załącznika 2 do DPA 2018).

([64]) W wyroku w sprawie NT1 przeciwko Google [2018] EWHC 799 (QB), pkt 102 odniesiono się do dyskusji na temat tego, czy administrator danych był zasadnie przekonany, że publikacja leży w interesie publicznym, a zachowanie zgodności z odpowiednimi przepisami jest niezgodne ze szczególnymi celami. Trybunał stwierdził, że art. 32 ust. 1 lit. b) i c) ustawy o ochronie danych z 1998 r. zawiera element subiektywny i obiektywny: administrator danych musi wykazać, że był przekonany, iż publikacja leży w interesie publicznym, oraz że przekonanie to było obiektywnie zasadne; musi on dojść do subiektywnego przekonania, że zgodność z przepisami, w odniesieniu do których zamierza skorzystać z wyłączenia, byłaby sprzeczna z odnośnymi szczególnymi celami.

([65]) Przykład sposobu zastosowania kryterium „zasadnego przekonania" przedstawiono w decyzji Komisarza ds. Informacji o nałożeniu grzywny na True Visions Productions, którą podjęto na podstawie ustawy o ochronie danych z 1998 r. Komisarz ds. Informacji przyjął, że administrator mediów miał subiektywne przekonanie, że zgodność z pierwszą zasadą ochrony danych (rzetelność i zgodność z prawem) była sprzeczna z celami dziennikarskimi. Komisarz ds. Informacji nie uznał jednak tego przekonania za obiektywnie zasadne. Decyzja Komisarza ds. Informacji jest dostępna pod adresem: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

przeszkodę w prowadzeniu odpowiedzialnego dziennikarstwa ([66]). Organ regulacyjny Zjednoczonego Królestwa ds. telekomunikacji, OFCOM, oraz BBC – w ramach swoich wytycznych redakcyjnych – również opublikowały wytyczne dotyczące stosowania kryterium interesu publicznego i równoważenia interesu publicznego z interesem osoby fizycznej w zakresie ochrony prywatności ([67]). W wytycznych przedstawiono przykłady informacji, które można uznać za leżące w interesie publicznym, oraz wyjaśniono konieczność wykazania, że w szczególnych okolicznościach konkretnej sprawy interes publiczny przeważa nad prawem do prywatności.

(71) Podobnie do przepisów art. 89 RODO dane osobowe przetwarzane do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych można również wyłączyć z zakresu stosowania szeregu wymienionych przepisów RODO UK ([68]). W odniesieniu do badań naukowych i celów statystycznych możliwe jest zastosowanie wyłączeń od przepisów RODO UK dotyczących potwierdzenia przetwarzania, dostępu do danych i zabezpieczeń w przypadku przekazywania danych do państw trzecich; prawa do sprostowania; ograniczenia przetwarzania i sprzeciwu wobec przetwarzania. W odniesieniu do archiwizacji w interesie publicznym możliwe są również wyłączenia z zakresu stosowania obowiązku powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania oraz prawa do przenoszenia danych.

(72) Zgodnie z pkt 27 ppkt 1 i pkt 28 ppkt 1 załącznika 2 do DPA 2018 wyłączenia z zakresu stosowania wymienionych przepisów RODO UK są możliwe, gdy zastosowanie przepisów „uniemożliwiłoby lub poważnie utrudniłoby osiągnięcie" wspomnianych celów ([69]).

(73) Biorąc pod uwagę znaczenie wyżej wymienionych wyłączeń dla skutecznego wykonywania praw indywidualnych, wszelkie istotne zmiany dotyczące wykładni tych wyłączeń i ich stosowania w praktyce (oprócz wyjaśnionego w motywie 6 wyłączenia dotyczącego utrzymania skutecznej kontroli imigracji), w tym wszelkie dalsze zmiany w orzecznictwie oraz wytycznych Komisarza ds. Informacji i jego działań w zakresie egzekwowania przepisów, zostaną należycie uwzględnione w kontekście ciągłego monitorowania niniejszej decyzji ([70]).

2.5.7. *Ograniczenia dotyczące dalszego przekazywania danych*

(74) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii Europejskiej administratorom lub podmiotom przetwarzającym w Zjednoczonym Królestwie nie może zostać obniżony wskutek dalszego przekazywania takich danych odbiorcom z państw trzecich. Takie „dalsze przekazywanie danych", które z perspektywy administratora lub podmiotu przetwarzającego ze Zjednoczonego Królestwa stanowi międzynarodowe przekazywanie danych ze Zjednoczonego Królestwa, powinno być dozwolone wyłącznie wówczas, gdy kolejny odbiorca spoza Zjednoczonego Królestwa sam podlega przepisom zapewniającym stopień ochrony zbliżony do poziomu gwarantowanego w porządku prawnym Zjednoczonego Królestwa. Z tego powodu stosowanie przepisów RODO UK i DPA 2018 dotyczących międzynarodowego przekazywania danych osobowych jest ważnym czynnikiem zapewniającym ciągłość ochrony w przypadku przekazywania danych osobowych z Unii Europejskiej do Zjednoczonego Królestwa na podstawie niniejszej decyzji.

([66]) Zgodnie z wytycznymi organizacje muszą być w stanie wyjaśnić, dlaczego przestrzeganie odpowiedniego przepisu ustawy o ochronie danych z 1998 r. jest niezgodne z celami dziennikarskimi. W szczególności administratorzy muszą zrównoważyć szkodliwy wpływ, jaki przestrzeganie przepisów miałoby na dziennikarstwo, ze szkodliwym wpływem, jaki nieprzestrzeganie przepisów miałoby na prawa osoby, której dane dotyczą. Jeżeli dziennikarz jest w stanie racjonalnie osiągnąć swoje cele redakcyjne w sposób zgodny ze standardowymi przepisami ustawy o ochronie danych, ma obowiązek tak postąpić. Organizacje muszą być w stanie uzasadnić zastosowanie ograniczenia w odniesieniu do każdego przepisu, którego nie przestrzegają. „Ochrona danych i dziennikarstwo: wytyczne dla mediów", dostępne pod adresem: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Przykłady interesu publicznego obejmują ujawnienie lub wykrycie przestępstwa, ochronę zdrowia lub bezpieczeństwa publicznego, ujawnienie wprowadzających w błąd oświadczeń składanych przez osoby fizyczne lub organizacje lub ujawnienie niekompetencji mającej wpływ na społeczeństwo. Zob. wytyczne OFCOM dostępne pod adresem: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf i wytyczne redakcyjne BBC dostępne pod adresem: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Zob. art. 89 RODO UK oraz część 6 pkt 27 ppkt 2 i pkt 28 ppkt 2 załącznika 2 do DPA 2018.

([69]) Odbywa się to z zastrzeżeniem wymogu, aby dane osobowe były przetwarzane zgodnie z art. 89 ust. 1 RODO UK uzupełnionego art. 19 DPA 2018.

([70]) Zob. motywy 281–287.

(75) System międzynarodowego przekazywania danych osobowych ze Zjednoczonego Królestwa określono w art. 44–49 RODO UK, uzupełnionego DPA 2018; system ten jest zasadniczo identyczny z zasadami określonymi w rozdziale V rozporządzenia (UE) 2016/679 ([71]). Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może odbywać się wyłącznie na podstawie rozporządzenia stwierdzającego odpowiedni stopień ochrony (obowiązujący w Zjednoczonym Królestwie odpowiednik decyzji stwierdzającej odpowiedni stopień ochrony na podstawie rozporządzenia (UE) 2016/679) lub – w przypadku braku takiego rozporządzenia – pod warunkiem zapewnienia przez administratora lub podmiot przetwarzający odpowiednich zabezpieczeń zgodnie z art. 46 RODO UK. W przypadku braku rozporządzenia stwierdzającego odpowiedni stopień ochrony lub odpowiednich zabezpieczeń przekazywanie danych może nastąpić wyłącznie na podstawie wyjątków określonych w art. 49 RODO UK.

(76) Rozporządzenia stwierdzające odpowiedni stopień ochrony, wydawane przez Sekretarza Stanu, mogą stanowić, że państwo trzecie (lub terytorium lub sektor w państwie trzecim), organizacja międzynarodowa lub opis ([72]) takiego państwa, terytorium, sektora lub takiej organizacji zapewniają odpowiedni stopień ochrony danych osobowych. Dokonując oceny odpowiedniości stopnia ochrony, Sekretarz Stanu musi wziąć pod uwagę dokładnie te same elementy, które Komisja jest zobowiązana ocenić na mocy art. 45 ust. 2 lit. a)–c) rozporządzenia (UE) 2016/679 w związku z motywem 104 rozporządzenia (UE) 2016/679 oraz pozostającym w mocy orzecznictwem UE. Oznacza to, że przy ocenie odpowiedniości stopnia ochrony państwa trzeciego właściwym standardem będzie to, czy dane państwo trzecie zapewnia stopień ochrony „zasadniczo odpowiadający" stopniowi gwarantowanemu w Zjednoczonym Królestwie.

(77) Co się tyczy procedury, rozporządzenia stwierdzające odpowiedni stopień ochrony podlegają „ogólnym" wymogom proceduralnym określonym w art. 182 DPA 2018. W ramach wspomnianej procedury Sekretarz Stanu musi przeprowadzić konsultacje z Komisarzem ds. Informacji, gdy proponuje przyjęcie rozporządzeń Zjednoczonego Królestwa stwierdzających odpowiedni stopień ochrony ([73]). Po przyjęciu przez Sekretarza Stanu rozporządzenia te są przedkładane parlamentowi i podlegają procedurze „odrzucenia przez obie izby parlamentu", w ramach której obie izby parlamentu mogą poddać rozporządzenie kontroli i mają możliwość przyjęcia wniosku o jego unieważnienie w ciągu 40 dni ([74]).

(78) Zgodnie z art. 17B ust. 1 DPA 2018 rozporządzenia stwierdzające odpowiedni stopień ochrony należy poddawać przeglądowi co najmniej raz na cztery lata, a Sekretarz Stanu musi na bieżąco monitorować zmiany zachodzące w państwach trzecich i organizacjach międzynarodowych, które mogłyby wpłynąć na decyzje w sprawie wprowadzenia rozporządzeń stwierdzających odpowiedni stopień ochrony lub w sprawie zmiany lub uchylenia takich przepisów. Jeżeli Sekretarz Stanu uzyska wiedzę, że określone państwo lub organizacja nie zapewnia już odpowiedniego stopnia ochrony danych osobowych, musi zmienić lub uchylić – w niezbędnym zakresie – rozporządzenie i rozpocząć konsultacje z danym państwem trzecim lub organizacją międzynarodową w celu rozwiązania kwestii braku odpowiedniego stopnia ochrony. Te aspekty proceduralne odzwierciedlają również odpowiednie wymogi określone w rozporządzeniu (UE) 2016/679.

---

([71]) Z wyjątkiem art. 48 rozporządzenia (UE) 2016/679, którego Zjednoczone Królestwo postanowiło nie włączać do RODO UK. W tym względzie należy przede wszystkim przypomnieć, że standard, który należy uznać za zapewniający odpowiedni poziom ochrony, to standard „zasadniczej równoważności", a nie identyczności, jak wyjaśnił Trybunał Sprawiedliwości Unii Europejskiej (Schrems I, pkt 73–74) i jak uznała EROD (Odpowiedni stopień ochrony przekazywanych danych osobowych, s. 3). W związku z tym, jak wyjaśniła Europejska Rada Ochrony Danych w swoich wytycznych dotyczących odpowiedniego stopnia ochrony przekazywanych danych osobowych, „celem nie jest odzwierciedlenie punkt po punkcie prawodawstwa europejskiego, ale ustanowienie zasadniczych, tj. podstawowych, wymogów tego prawodawstwa". W związku z tym należy zauważyć, że chociaż porządek prawny Zjednoczonego Królestwa formalnie nie zawiera przepisu identycznego z art. 48, taki sam skutek gwarantują inne przepisy i zasady: w odpowiedzi na wniosek o przekazanie danych osobowych, złożony przez sąd lub organ administracyjny państwa trzeciego, dane osobowe mogą zostać przekazane do tego państwa trzeciego jedynie wówczas, gdy istnieje umowa międzynarodowa, na podstawie której orzeczenie lub decyzja administracyjna tego państwa trzeciego są uznawane lub wykonywane w Zjednoczonym Królestwie, bądź gdy przekazanie danych opiera się na jednym z mechanizmów przekazania określonych w rozdziale V RODO UK. Ściślej rzecz ujmując, aby wykonać orzeczenie zagraniczne, sądy w Zjednoczonym Królestwie muszą być w stanie wskazać zasadę prawa precedensowego (*common law*) lub ustawę, które pozwalają na jego wykonalność. Niemniej jednak ani prawo precedensowe (zob. Adams i in. przeciwko Cape Industries Plc., [1990] 2 W.L.R. 657), ani ustawy nie przewidują wykonywania orzeczeń zagranicznych wymagających przekazania danych w przypadku braku obowiązującej umowy międzynarodowej. W związku z tym wnioski o przekazanie danych są na mocy prawa Zjednoczonego Królestwa bezskuteczne w sytuacji braku takiej umowy międzynarodowej. Ponadto każde przekazanie danych osobowych do państw trzecich – w tym na wniosek zagranicznego sądu lub organu administracyjnego – nadal podlega ograniczeniom określonym w rozdziale V RODO UK, które są identyczne z odpowiednimi przepisami rozporządzenia (UE) 2016/679, i w związku z tym musi opierać się na jednej z podstaw przekazania określonych w rozdziale V, zgodnie ze szczególnymi warunkami, którym takie przekazanie podlega na mocy tego rozdziału.

([72]) Władze Zjednoczonego Królestwa wyjaśniły, że opis państwa lub organizacji międzynarodowej odnosi się do sytuacji, w której konieczne byłoby dokonanie szczegółowego i częściowego określenia odpowiedniości ochrony przy konkretnych ograniczeniach (np. rozporządzeniu stwierdzającym odpowiedni stopień ochrony wyłącznie w odniesieniu do określonych rodzajów przekazywania danych).

([73]) Zob. protokół ustaleń między Sekretarzem Stanu Departamentu Cyfryzacji, Kultury, Mediów i Sportu a Biurem Komisarza ds. Informacji w sprawie roli Komisarza ds. Informacji w zakresie nowej oceny adekwatności w Zjednoczonym Królestwie, dostępny pod adresem: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) W przypadku przyjęcia takiego wniosku w drodze głosowania, rozporządzenia ostatecznie przestaną wywoływać jakikolwiek dalszy skutek prawny.

(79) W przypadku braku rozporządzeń stwierdzających odpowiedni stopień ochrony międzynarodowe przekazywanie danych może mieć miejsce, jeżeli administrator lub podmiot przetwarzający zapewnili odpowiednie zabezpieczenia zgodnie z art. 46 RODO UK. Zabezpieczenia te są podobne do tych, określonych w art. 46 rozporządzenia (UE) 2016/679. Obejmują one prawnie wiążące i możliwe do wyegzekwowania instrumenty między organami lub podmiotami publicznymi, wiążące reguły korporacyjne ([75]), standardowe klauzule o ochronie danych, zatwierdzone kodeksy postępowania, zatwierdzone mechanizmy certyfikacji oraz – za zgodą Komisarza ds. Informacji – klauzule umowne między administratorami (lub podmiotami przetwarzającymi) lub porozumienia administracyjne między organami publicznymi. Z proceduralnego punktu widzenia zmieniono jednak reguły, aby funkcjonowały w ramach Zjednoczonego Królestwa, w szczególności Sekretarz Stanu (art. 17C) lub Komisarz ds. Informacji (art. 119A) mogą przyjąć standardowe klauzule o ochronie danych zgodnie z DPA 2018.

(80) W przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony lub odpowiednich zabezpieczeń, przekazywanie danych może nastąpić wyłącznie na podstawie wyjątków określonych w art. 49 RODO UK ([76]). W RODO UK nie wprowadzono żadnych istotnych zmian w zakresie wyjątków w porównaniu z odpowiednimi przepisami rozporządzenia (UE) 2016/679. Zgodnie z RODO UK, podobnie jak w przypadku rozporządzenia (UE) 2016/679, na określone wyjątki można się powoływać wyłącznie w przypadku gdy przekazywanie danych ma charakter sporadyczny ([77]). Ponadto Komisarz ds. Informacji w swoich wytycznych dotyczących międzynarodowego przekazywania danych wyjaśnia, że: „Należy je stosować wyłącznie jako faktyczne »wyjątki« od ogólnej zasady, zgodnie z którą nie należy przekazywać danych w sposób ograniczony, chyba że jest to przedmiotem decyzji stwierdzającej odpowiedni stopień ochrony lub istnieją odpowiednie zabezpieczenia" ([78]). W odniesieniu do przekazania, które jest niezbędne ze względu na ważne względy interesu publicznego (art. 49 ust. 1 lit. d)), Sekretarz Stanu może przyjąć przepisy w celu określenia okoliczności, w których przekazywanie danych osobowych państwu trzeciemu lub organizacji międzynarodowej nie jest niezbędne ze względu na ważne względy interesu publicznego. Ponadto na mocy rozporządzenia Sekretarz Stanu może ograniczyć przekazywanie danej kategorii danych osobowych do państwa trzeciego lub organizacji międzynarodowej, jeżeli przekazanie nie może nastąpić na podstawie rozporządzeń stwierdzających odpowiedni stopień ochrony, a Sekretarz Stanu uważa, że ograniczenie jest niezbędne ze względu na ważne względy interesu publicznego. Dotychczas nie przyjęto takich przepisów.

(81) Wspomniane ramy dotyczące międzynarodowego przekazywania danych zaczęły obowiązywać na koniec okresu przejściowego ([79]). Pkt 4 załącznika 21 do DPA 2018 (wprowadzony na mocy rozporządzenia w sprawie ochrony danych, prywatności i łączności elektronicznej) stanowi jednak, że do zakończenia okresu przejściowego określone przekazania danych osobowych są traktowane tak, jakby opierały się na rozporządzeniach stwierdzających odpowiedni stopień ochrony. Przekazania te obejmują przekazania danych do państwa EOG, na terytorium Gibraltaru, do instytucji, organu i jednostki organizacyjnej UE ustanowionych na mocy lub na podstawie Traktatu o Unii Europejskiej oraz do państw trzecich będących przedmiotem decyzji UE stwierdzającej odpowiedni stopień ochrony na koniec okresu przejściowego. W związku z tym przekazywanie danych do tych państw może nadal się odbywać na takich samych zasadach jak przed wystąpieniem Zjednoczonego Królestwa z Unii Europejskiej. Po zakończeniu

([75]) W RODO UK pozostawiono w mocy reguły określone w art. 47 rozporządzenia (UE) 2016/679, wprowadzając wyłącznie zmiany służące dostosowaniu przepisów do kontekstu krajowego, np. poprzez zastąpienie odniesień do właściwego organu nadzorczego odniesieniami do Komisarza ds. Informacji, usunięcie odniesienia do mechanizmu spójności, o którym mowa w ust. 1, oraz usunięcie całego ust. 3.

([76]) Zgodnie z art. 49 RODO UK przekazanie danych jest możliwe, jeżeli spełniono jeden z poniższych warunków: a) osoba, której dane dotyczą, poinformowana o ewentualnym ryzyku, z którym – ze względu na brak decyzji stwierdzającej odpowiedni stopień ochrony oraz na brak odpowiednich zabezpieczeń – może się dla niej wiązać proponowane przekazanie, wyraźnie wyraziła na nie zgodę; b) przekazanie jest niezbędne do wykonania umowy między osobą, której dane dotyczą, a administratorem lub do wprowadzenia w życie środków przedumownych podejmowanych na żądanie osoby, której dane dotyczą; c) przekazanie jest niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, których dane dotyczą, między administratorem a inną osobą fizyczną lub prawną; d) przekazanie jest niezbędne ze względu na ważne względy interesu publicznego; e) przekazanie jest niezbędne do ustalenia, dochodzenia lub ochrony roszczeń; f) przekazanie jest niezbędne do ochrony żywotnych interesów osoby, których dane dotyczą, lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody; lub g) przekazanie następuje z rejestru, który zgodnie z prawem krajowym ma służyć za źródło informacji dla ogółu obywateli i który jest dostępny dla ogółu obywateli lub dla każdej osoby mogącej wykazać prawnie uzasadniony interes – ale wyłącznie w zakresie, w jakim w danym przypadku spełnione zostały warunki takiego dostępu określone w prawie krajowym. Ponadto, jeżeli nie ma zastosowania żaden z wymienionych wyżej warunków, przekazanie może nastąpić wyłącznie, gdy przekazanie nie jest powtarzalne, dotyczy tylko ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa i wolności osoby, której dane dotyczą, a administrator ocenił wszystkie okoliczności przekazania danych i na podstawie tej oceny zapewnił odpowiednie zabezpieczenia w zakresie ochrony danych osobowych.

([77]) W motywie 111 RODO UK stwierdza się, że przekazywanie danych w związku z umową lub roszczeniami może nastąpić tylko wtedy, gdy ma charakter sporadyczny.

([78]) Wytyczne Komisarza ds. Informacji dotyczące międzynarodowego przekazywania danych, dostępne pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) Przez maksymalny okres sześciu miesięcy kończący się najpóźniej 30 czerwca 2021 r. stosowanie tych nowych ram należy interpretować w świetle 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 (L 444/14 z 31.12.2020) („umowa o handlu i współpracy między Unią Europejską a Zjednoczonym Królestwem"), dostępnej pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22020A1231(01)&from=PL.

okresu przejściowego Sekretarz Stanu ma obowiązek przeprowadzić przegląd tych ustaleń dotyczących odpowiedniego stopnia ochrony w terminie czterech lat, tj. do końca grudnia 2024 r. Zgodnie z wyjaśnieniem przedstawionym przez władze Zjednoczonego Królestwa, mimo że Sekretarz Stanu ma obowiązek przeprowadzić taki przegląd do końca grudnia 2024 r., przepisy przejściowe nie obejmują przepisu dotyczącego „wygaśnięcia" i odpowiednie przepisy przejściowe nie przestaną automatycznie obowiązywać, jeżeli przegląd nie zostanie zakończony do końca grudnia 2024 r.

(82) Jeśli chodzi wreszcie o przyszłą ewolucję międzynarodowego systemu Zjednoczonego Królestwa w zakresie przekazywania danych – czy to poprzez przyjęcie nowych rozporządzeń stwierdzających odpowiedni stopień ochrony, zawieranie umów międzynarodowych lub wypracowanie innych mechanizmów przekazywania – Komisja będzie ściśle monitorować sytuację, oceniać, czy poszczególne mechanizmy transferu są wykorzystywane w sposób zapewniający ciągłość ochrony, oraz, w razie konieczności, podejmować odpowiednie środki w celu zaradzenia ewentualnym negatywnym skutkom dla takiej ciągłości (zob. motywy 278–287). Ponieważ UE i Zjednoczone Królestwo mają podobne zasady dotyczące międzynarodowego przekazywania danych, można się spodziewać, że problematycznym rozbieżnościom będzie można również zapobiec dzięki współpracy oraz wymianie informacji i doświadczeń, m.in. między Komisarzem ds. Informacji a EROD.

2.5.8. *Rozliczalność*

(83) Zgodnie z zasadą rozliczalności podmioty przetwarzające dane są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby skutecznie przestrzegać swoich obowiązków w zakresie ochrony danych oraz być w stanie wykazać taką zgodność, zwłaszcza wobec właściwego organu nadzorczego.

(84) Zasadę rozliczalności przewidzianą w rozporządzeniu (UE) 2016/679 zachowano bez istotnych zmian w art. 5 ust. 2 RODO UK i to samo odnosi się do art. 24 dotyczącego obowiązków administratora, art. 25 dotyczącego uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych, a także art. 30 dotyczącego rejestrowania czynności przetwarzania. Zachowano również art. 35 i 36 dotyczące oceny skutków dla ochrony danych i uprzednich konsultacji z organem nadzorczym. W RODO UK zachowano bez istotnych zmian przepisy art. 37–39 rozporządzenia (UE) 2016/679 dotyczące wyznaczenia inspektora ochrony danych i jego zadań. Ponadto w RODO UK zachowano przepisy art. 40 i 42 rozporządzenia (UE) 2016/679 dotyczące kodeksu postępowania i certyfikacji ([80]).

## 2.6. **Nadzór i egzekwowanie przepisów**

### 2.6.1. *Niezależny nadzór*

(85) Aby zagwarantować w praktyce odpowiedni stopień ochrony danych, należy ustanowić niezależny organ nadzorczy, uprawniony do monitorowania i egzekwowania zgodności z przepisami o ochronie danych. W ramach wykonywanych obowiązków i realizowanych uprawnień organ ten powinien być całkowicie niezależny i bezstronny.

(86) W Zjednoczonym Królestwie za nadzór i egzekwowanie zgodności z przepisami RODO UK i DPA 2018 odpowiada Komisarz ds. Informacji. Komisarz ds. Informacji jest „pojedynczą osobą prawną": odrębnym podmiotem prawnym składającym się z jednej osoby. Komisarza ds. Informacji wspiera w pracy biuro. W dniu 31 marca 2020 r. Biuro Komisarza ds. Informacji zatrudniało 768 stałych pracowników ([81]). Departamentem finansującym Komisarza ds. Informacji jest Departament Cyfryzacji, Kultury, Mediów i Sportu ([82]).

(87) Kwestię niezależności Komisarza ds. Informacji wyraźnie uregulowano w art. 52 RODO UK, w którym nie wprowadzono żadnych istotnych zmian względem art. 52 ust. 1–3 RODO. Komisarz musi działać z zachowaniem pełnej niezależności, wykonując swoje zadania i uprawnienia zgodnie z RODO UK, pozostawać wolny od bezpośrednich lub pośrednich wpływów zewnętrznych w odniesieniu do tych zadań i uprawnień oraz nie może zwracać się do

([80]) W stosownych przypadkach odniesienia te zastępuje się odniesieniami do władz Zjednoczonego Królestwa. Na przykład zgodnie z art. 17 DPA 2018 Komisarz ds. Informacji lub krajowa jednostka akredytująca Zjednoczonego Królestwa może udzielić akredytacji osobie spełniającej wymogi określone w art. 43 RODO UK do celów monitorowania zgodności z certyfikacją.

([81]) Sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2019–2020, dostępne pod adresem: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Relacje między tymi dwoma podmiotami reguluje umowa o zarządzanie. W szczególności kluczowe obowiązki Departamentu Cyfryzacji, Kultury, Mediów i Sportu jako departamentu finansującego obejmują: zapewnienie Komisarzowi ds. Informacji odpowiedniego finansowania i odpowiednich zasobów; reprezentowanie interesów Komisarza ds. Informacji przed parlamentem i innymi departamentami rządowymi; zapewnienie solidnych krajowych ram ochrony danych oraz zapewnienie wytycznych i wsparcia na rzecz Biura Komisarza ds. Informacji w zakresie kwestii korporacyjnych, taki jak kwestie dotyczące nieruchomości, najmu i zamówień publicznych (umowa o zarządzanie na lata 2018–2021, dostępna pod adresem: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

nikogo o instrukcje ani ich od nikogo przyjmować. Komisarz musi również powstrzymać się od wszelkich czynności sprzecznych ze swoimi obowiązkami i w okresie sprawowania urzędu nie może podejmować żadnego zajęcia zarobkowego ani niezarobkowego sprzecznego z tymi obowiązkami.

(88) Warunki powoływania i odwoływania Komisarza ds. Informacji określono w załączniku 12 do DPA 2018. Komisarz ds. Informacji jest powoływany przez Jej Królewską Mość na wniosek rządu w wyniku uczciwego i otwartego konkursu. Kandydat musi posiadać odpowiednie kwalifikacje, umiejętności i kompetencje. Zgodnie z kodeksem zarządzania w zakresie nominacji publicznych ([83]) zespół doradczy ds. oceny sporządza wykaz ewentualnych kandydatów. Zanim Sekretarz Stanu w Departamencie Cyfryzacji, Kultury, Mediów i Sportu podejmie ostateczną decyzję, właściwa komisja specjalna parlamentu musi przeprowadzić kontrolę poprzedzającą nominację. Stanowisko komisji podaje się do wiadomości publicznej ([84]).

(89) Kadencja Komisarza ds. Informacji trwa maksymalnie siedem lat. Ta sama osoba nie może zostać powołana na stanowisko Komisarza ds. Informacji więcej niż jeden raz. Jej Królewska Mość może odwołać Komisarza ds. Informacji ze stanowiska na podstawie oświadczenia obu izb parlamentu ([85]). Wniosek o odwołanie Komisarza ds. Informacji może zostać przedstawiony jednej z izb parlamentu jedynie w wypadku, gdy minister przedstawi sprawozdanie, w którym wyrazi przekonanie, że Komisarz ds. Informacji jest winny poważnego uchybienia lub nie spełnia już warunków wymaganych do sprawowania funkcji Komisarza ([86]).

(90) Środki na finansowanie działalności Komisarza ds. Informacji pochodzą z trzech źródeł: (i) opłat za ochronę danych wnoszonych przez administratorów, które są ustalane na podstawie rozporządzeń wydanych przez Sekretarza Stanu ([87]) (rozporządzenie dotyczące opłat i informacji związanych z ochroną danych z 2018 r.) i wynoszą 85–90 % rocznego budżetu Biura ([88]); (ii) subwencji wypłacanych przez rząd na rzecz Komisarza ds. Informacji, wykorzystywanych głównie do finansowania kosztów operacyjnych Komisarza ds. Informacji w odniesieniu do zadań niezwiązanych z ochroną danych ([89]); oraz (iii) opłat pobieranych z tytułu świadczenia usług ([90]). Obecnie nie pobiera się takich opłat.

(91) Ogólne funkcje Komisarza ds. Informacji dotyczące przetwarzania danych osobowych, do których ma zastosowanie ogólne rozporządzenie o ochronie danych Zjednoczonego Królestwa, określono w art. 57 RODO UK, wiernie odzwierciedlając odpowiednie przepisy rozporządzenia (UE) 2016/679. Jego funkcje obejmują monitorowanie i egzekwowanie przepisów RODO UK, promowanie świadomości społecznej, rozpatrywanie skarg wnoszonych przez osoby, których dane dotyczą, prowadzenie postępowań itp. Ponadto w art. 115 DPA 2018 określono inne ogólne funkcje Komisarza, które obejmują obowiązek doradzania parlamentowi, rządowi i innym instytucjom i organom w sprawie środków prawnych i administracyjnych związanych z ochroną praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych, oraz uprawnienia do wydawania, z inicjatywy Komisarza lub na wniosek, opinii przeznaczonych dla parlamentu, rządu lub innych instytucji i organów, a także ogółu społeczeństwa we

([83]) Kodeks zarządzania w zakresie nominacji publicznych, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) Drugie sprawozdanie z sesji Komisji Kultury, Mediów i Sportu 2015–2016 w Izbie Gmin, dostępne pod adresem: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) „Oświadczenie" oznacza wniosek składany w parlamencie, służący zapoznaniu monarchy z opiniami parlamentu na dany temat.

([86]) Punkt 3 ppkt 3 załącznika 12 do DPA 2018.

([87]) Art. 137 DPA 2018, zob. motyw 17.

([88]) Art. 137 i 138 DPA 2018 zawiera szereg zabezpieczeń służących zapewnieniu ustalenia opłat na odpowiednim poziomie. W szczególności w art. 137 ust. 4 wymieniono kwestie, jakie Sekretarz Stanu musi uwzględnić przy tworzeniu przepisów określających kwotę, którą muszą zapłacić różne organizacje. Po drugie, art. 138 ust. 1 i art. 182 DPA 2018 zawierają również wymóg prawny, aby Sekretarz Stanu przed wprowadzeniem przepisów zasięgnął opinii Komisarza ds. Informacji i innych przedstawicieli osób, których przepisy te mogą dotyczyć. Ponadto zgodnie z art. 138 ust. 2 DPA 2018 Komisarz ds. Informacji jest zobowiązany do prowadzenia stałego przeglądu funkcjonowania rozporządzenia w sprawie opłat i może przedstawić Sekretarzowi Stanu propozycje zmian, które należy wprowadzić do rozporządzenia. Z wyjątkiem przypadków gdy przepisy są tworzone w celu uwzględnienia wzrostu wskaźnika cen towarów i usług konsumpcyjnych (w którym to przypadku podlegają one procedurze milczącej zgody [*negative resolution procedure*]), przepisy podlegają ponadto procedurze wyraźnej zgody (*affirmative resolution procedure*), a ich przyjęcie jest możliwe po zatwierdzeniu ich uchwałą każdej izby parlamentu.

([89]) W umowie o zarządzanie wyjaśniono, że „Sekretarz Stanu może dokonywać płatności na rzecz Komisarza ds. Informacji ze środków zapewnianych przez Parlament na mocy pkt 9 załącznika 12 do DPA 2018. Po konsultacji z Komisarzem ds. Informacji Departament Cyfryzacji, Kultury, Mediów i Sportu wypłaci Komisarzowi ds. Informacji odpowiednią kwotę (subwencję) na pokrycie kosztów administracyjnych Komisarza ds. Informacji i kosztów związanych z pełnieniem funkcji Komisarza ds. Informacji w odniesieniu do szeregu konkretnych funkcji, w tym swobodnego dostępu do informacji" (umowa o zarządzanie na lata 2018–2021, pkt 1.12, zob. przypis 82).

([90]) Zob. art. 134 DPA 2018.

wszelkich sprawach związanych z ochroną danych osobowych. Aby utrzymać niezależność sądów, Komisarz ds. Informacji nie jest uprawniony do wykonywania swoich funkcji w odniesieniu do przetwarzania danych osobowych przez osobę fizyczną sprawującą wymiar sprawiedliwości bądź sąd lub trybunał sprawujący wymiar sprawiedliwości. Nadzór nad sądownictwem zapewniają wyspecjalizowane organy (zob. motywy 99–103).

2.6.2. *Egzekwowanie przepisów, w tym sankcje*

(92) Uprawnienia Komisarza ds. Informacji określono w art. 58 RODO UK, w którym nie wprowadzono żadnych istotnych zmian w porównaniu z odpowiednim artykułem rozporządzenia (UE) 2016/679. DPA 2018 zawiera przepisy uzupełniające dotyczące sposobu wykonywania tych uprawnień. W szczególności Komisarz posiada uprawnienia w zakresie: a) nakazania administratorowi i podmiotowi przetwarzającemu (a w określonych okolicznościach każdej innej osobie) dostarczenia niezbędnych informacji poprzez publikację zawiadomienia informacyjnego („zawiadomienie informacyjne") ([91]); b) prowadzenia postępowań i audytów poprzez wydanie zawiadomienia oceniającego, na mocy którego administrator lub podmiot przetwarzający może być zobowiązany do zezwolenia Komisarzowi na wejście do określonych pomieszczeń, przeprowadzenie inspekcji lub analizy dokumentów lub sprzętu, przesłuchanie osób przetwarzających dane osobowe w imieniu administratora itp. („zawiadomienie oceniające") ([92]); c) uzyskania w inny sposób dostępu do dokumentów itp. administratorów i podmiotów przetwarzających oraz dostępu do ich pomieszczeń zgodnie z art. 154 DPA 2018 („uprawnienia do wstępu i inspekcji"); d) wykonywania uprawnień naprawczych, w tym za pomocą ostrzeżeń i upomnień lub wydawania nakazów w postaci zawiadomienia egzekucyjnego, w ramach którego zobowiązuje się administratorów/podmioty przetwarzające do podjęcia lub powstrzymania się od podjęcia konkretnych kroków, w tym nakazuje się administratorowi lub podmiotowi przetwarzającemu podjęcie działań określonych w art. 58 ust. 2 lit. c)–g) i j) RODO UK („zawiadomienie egzekucyjne") ([93]); e) oraz nakładania administracyjnych kar pieniężnych w drodze zawiadomienia w sprawie sankcji („zawiadomienie w sprawie sankcji") ([94]). Kary takie mogą zostać nałożone również w przypadku nieprzestrzegania przez organ publiczny przepisów RODO UK ([95]).

(93) W ramach polityki działań regulacyjnych Komisarza ds. Informacji określono okoliczności, w których Komisarz ds. Informacji może wydać zawiadomienie informacyjne, oceniające, egzekucyjne lub w sprawie sankcji ([96]). W ramach zawiadomienia egzekucyjnego wydanego w odpowiedzi na uchybienie administratora lub podmiotu przetwarzającego możliwe jest nakładanie wyłącznie wymogów, które Komisarz uzna za właściwe w celu zaradzenia uchybieniu. Zawiadomienia egzekucyjne i w sprawie sankcji można wydać w odniesieniu do administratora lub podmiotu przetwarzającego w związku z naruszeniem przepisów rozdziału II RODO UK (zasady przetwarzania), art. 12–22 (prawa osoby, której dane dotyczą), art. 25–39 (obowiązki administratorów i podmiotów przetwarzających) oraz art. 44–49 (międzynarodowe przekazywanie danych) RODO UK. Zawiadomienie egzekucyjne można również wydać w przypadku gdy administrator nie spełnił wymogu uiszczenia opłaty określonej w przepisach zawartych w art. 137 DPA 2018. Ponadto podmiot monitorujący, o którym mowa w art. 41, lub podmiot świadczący usługi certyfikacyjne mogą otrzymać zawiadomienie egzekucyjne, jeżeli nie wypełnili swoich zobowiązań wynikających z RODO UK. Zawiadomienie w sprawie sankcji można również wydać w odniesieniu do osoby, która nie zastosowała się do zawiadomienia informacyjnego, oceniającego ani egzekucyjnego.

(94) W ramach zawiadomienia w sprawie sankcji zobowiązuje się daną osobę do wpłacenia na rzecz Komisarza ds. Informacji kwoty określonej w zawiadomieniu. Podejmując decyzję o wydaniu zawiadomienia w sprawie sankcji danej osobie i określając kwotę sankcji, Komisarz ds. Informacji musi uwzględnić kwestie wymienione w art. 83 ust. 1 i 2 RODO UK, które są identyczne z odpowiednimi przepisami rozporządzenia (UE) 2016/679 ([97]). Zgodnie z art. 83 ust. 4 i 5 maksymalne kwoty administracyjnych kar pieniężnych w przypadku niewypełnienia zobowiązań, o których mowa we wspomnianych przepisach, wynoszą odpowiednio 8 700 000 GBP lub 17 500 000 GBP. W przy-

([91]) Art. 142 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 143 DPA 2018).
([92]) Art. 146 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 147 DPA 2018).
([93]) Art. 149–151 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 152 DPA 2018).
([94]) Art. 155 DPA 2018 i art. 83 RODO UK.
([95]) Wynika to z art. 155 ust. 1 DPA 2018 w związku z art. 149 ust. 2 i 5 DPA 2018 oraz z art. 156 ust. 4 DPA 2018, który ogranicza wydawanie zawiadomień w sprawie sankcji wyłącznie w odniesieniu do komisarzy majątku Korony i administratorów dworu królewskiego na podstawie art. 209 ust. 4 DPA 2018.
([96]) Polityka działań regulacyjnych, dostępna pod adresem: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) W tym charakter i wagę naruszenia (przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody), umyślny lub nieumyślny charakter naruszenia, wszelkie działania podjęte przez administratora w celu zminimalizowania szkody poniesionej przed osoby, których dane dotyczą, stopień odpowiedzialności administratora lub podmiotu przetwarzającego (z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich), wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego; stopień współpracy z Komisarzem ds. Informacji, kategorie danych osobowych, których dotyczyło naruszenie, wszelkie inne czynniki obciążające lub łagodzące mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

padku przedsiębiorstwa Komisarz ds. Informacji może również nałożyć grzywnę stanowiącą odsetek rocznego światowego obrotu, przy czym zastosowanie ma kwota wyższa. Podobnie jak w równoważnych przepisach rozporządzenia (UE) 2016/679, kwoty te ustalono w art. 83 ust. 4 i 5 odpowiednio na poziomie 2 % i 4 %. W przypadku niezastosowania się do zawiadomienia informacyjnego, oceniającego lub egzekucyjnego maksymalna kwota sankcji, jaką można nałożyć w ramach zawiadomienia w sprawie sankcji, jest równa wyższej z następujących kwot: 17 500 000 GBP lub – w przypadku przedsiębiorstwa – 4 % rocznego światowego obrotu.

(95) RODO UK wraz z DPA 2018 przyczyniły się również do wzmocnienia innych uprawnień Komisarza ds. Informacji. Przykładowo Komisarz może obecnie przeprowadzać obowiązkowe kontrole w odniesieniu do wszystkich administratorów i podmiotów przetwarzających w drodze zawiadomień oceniających, podczas gdy na mocy poprzednich przepisów – ustawy o ochronie danych z 1998 r. – Komisarz miał takie uprawnienia wyłącznie w odniesieniu do instytucji rządowych na szczeblu centralnym i organizacji zajmujących się ochroną zdrowia, zaś pozostałe podmioty musiały wyrazić zgodę na kontrolę.

(96) Od czasu wprowadzenia rozporządzenia (UE) 2016/679 Komisarz ds. Informacji rozpatruje rocznie około 40 000 skarg od osób, których dane dotyczą ([98]), a ponadto prowadzi około 2 000 postępowań z urzędu ([99]). Większość skarg dotyczy praw dostępu do danych i praw do ich ujawniania. W następstwie prowadzonych postępowań Komisarz podejmuje środki egzekucyjne w wielu sektorach. Mówiąc ściślej, według ostatniego sprawozdania rocznego Komisarza ds. Informacji (2019–2020) ([100]), w okresie sprawozdawczym Komisarz wydał 54 zawiadomienia informacyjne, 8 zawiadomień oceniających, 7 zawiadomień egzekucyjnych, 4 ostrzeżenia, doprowadził do 8 oskarżeń i nałożył 15 kar ([101]).

(97) Obejmują one szereg znaczących kar pieniężnych nałożonych na podstawie rozporządzenia (UE) 2016/679 i DPA 2018. W szczególności w październiku 2020 r. Komisarz ds. Informacji nałożył na brytyjskie przedsiębiorstwo lotnicze karę w wysokości 20 mln GBP za naruszenie ochrony danych dotyczące ponad 400 000 klientów. Pod koniec października 2020 r. na międzynarodową sieć hoteli nałożono grzywnę w wysokości 18,4 mln GBP za niedopełnienie obowiązku zapewnienia bezpieczeństwa danych osobowych milionów klientów, a w listopadzie 2020 r. na brytyjskiego usługodawcę sprzedającego w internecie bilety wstępu na imprezy nałożono grzywnę w wysokości 1,25 mln GBP za niedopełnienie obowiązku ochrony danych klientów dotyczących płatności ([102]).

(98) Oprócz opisanych w motywie 92 uprawnień Komisarza ds. Informacji do egzekwowania przestrzegania przepisów, niektóre naruszenia ustawodawstwa w dziedzinie ochrony danych stanowią przestępstwo i mogą tym samym podlegać sankcjom karnym (art. 196 DPA 2018). Dotyczy to na przykład świadomego lub nieopatrznego uzyskania lub ujawnienia danych osobowych bez zgody administratora, doprowadzenia do ujawnienia danych osobowych innej osobie bez zgody administratora ([103]), deanonimizacji informacji będących zanonimizowanymi danymi osobowymi bez zgody administratora odpowiedzialnego za anonimizację danych osobowych ([104]), umyślnego utrudniania Komisarzowi wykonywania jego uprawnień w zakresie kontroli danych osobowych zgodnie z zobowiązaniami międzynarodowymi ([105]), składania fałszywych oświadczeń w odpowiedzi na zawiadomienie informacyjne lub niszczenia informacji w związku z zawiadomieniem informacyjnym i oceniającym ([106]).

---

([98]) Według informacji przekazanych przez władze Zjednoczonego Królestwa, w okresie objętym rocznym sprawozdaniem Komisarza ds. Informacji za lata 2019–2020 w ok. 25 % spraw nie stwierdzono naruszenia; w ok. 29 % spraw zwrócono się do osoby, której dane dotyczą, o zgłoszenie problemu w pierwszej kolejności administratorowi danych, i wstrzymanie się z dalszymi działaniami do czasu uzyskania odpowiedzi administratora albo o dalszy dialog z administratorem danych; w ok. 17 % spraw nie stwierdzono żadnego naruszenia, ale udzielono porady administratorowi danych; w ok. 25 % spraw Komisarz ds. Informacji stwierdził naruszenie i udzielił porady administratorowi danych albo zobowiązał go do podjęcia określonych działań; w ok. 3 % spraw ustalono, że skarga nie jest objęta zakresem stosowania rozporządzenia (UE) 2016/679, a ok. 1 % spraw przekazano innemu organowi ochrony danych w ramach Europejskiej Rady Ochrony Danych.

([99]) Komisarz ds. Informacji może wszczynać takie postępowania na podstawie informacji otrzymanych z różnych źródeł, w tym ze zgłoszeń dotyczących naruszenia ochrony danych osobowych, wniosków o wydanie opinii od innych organów publicznych Zjednoczonego Królestwa lub zagranicznych organów ochrony danych oraz ze skarg od osób fizycznych lub organizacji społeczeństwa obywatelskiego.

([100]) Sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2019–2020 (zob. przypis 81).

([101]) Zgodnie z poprzednim sprawozdaniem rocznym obejmującym okres 2018–2019, w okresie sprawozdawczym Komisarz ds. Informacji wydał 22 zawiadomienia w sprawie sankcji na podstawie DPA 1998; nałożone grzywny wyniosły łącznie 3 010 610 GBP, w tym dwie grzywny w wysokości 500 000 GBP (maksymalna dozwolona kwota na mocy DPA 1998). W 2018 r. w następstwie doniesień dotyczących Cambridge Analytica Komisarz ds. Informacji przeprowadził w szczególności postępowanie w sprawie wykorzystania analizy danych do celów politycznych. W wyniku postępowania sporządzono sprawozdanie dotyczące polityki, zestaw zaleceń, nałożono karę w wysokości 500 000 GBP na Facebook oraz wydano zawiadomienie egzekucyjne skierowane do Aggregate IQ, kanadyjskiego brokera informacji, w którym nakazano przedsiębiorstwu usunięcie posiadanych przez nie danych osobowych dotyczących obywateli i mieszkańców Zjednoczonego Królestwa (zob. sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2018–2019, dostępne pod adresem: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Podsumowanie podjętych działań w zakresie egzekwowania przepisów znajduje się na stronie internetowej Komisarza ds. Informacji pod adresem: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Art. 170 DPA 2018.

([104]) Art. 171 DPA 2018.

([105]) Art. 119 DPA 2018.

([106]) Art. 144 i 148 DPA 2018.

2.6.3. *Nadzór nad wymiarem sprawiedliwości*

(99) Nadzór nad przetwarzaniem danych osobowych przez sądy i wymiar sprawiedliwości ma dwojaki charakter. W przypadku gdy osoby zajmujące stanowisko sędziowskie lub sąd nie sprawują wymiaru sprawiedliwości, nadzór sprawuje Komisarz ds. Informacji. W przypadku gdy administrator sprawuje wymiar sprawiedliwości, Komisarz ds. Informacji nie może wykonywać swoich funkcji nadzorczych ([107]), a nadzór sprawują organy specjalne. Odzwierciedla to podejście przyjęte w rozporządzeniu (UE) 2016/679 (art. 55 ust. 3).

(100) W szczególności w drugim scenariuszu w przypadku sądów Anglii i Walii i trybunału pierwszej instancji i wyższych trybunałów Anglii i Walii, taki nadzór sprawuje panel sądowy ds. ochrony danych (Judicial Data Protection Panel) ([108]). Ponadto Lord Chief Justice (zwierzchnik sądownictwa Anglii i Walii) i Senior President of Tribunals (zwierzchnik trybunałów pozasądowych) wydali oświadczenie o ochronie prywatności ([109]), w którym określili sposób, w jaki sądy w Anglii i Walii przetwarzają dane osobowe w związku z pełnieniem funkcji sądowych. Podobne oświadczenie wydano w systemach sądownictwa Irlandii Północnej ([110]) i Szkocji ([111]).

(101) Ponadto w Irlandii Północnej Lord Chief Justice Irlandii Północnej mianował sędziego Wysokiego Trybunału na stanowisko sędziego sprawującego nadzór nad ochroną danych osobowych ([112]). Wydano również wytyczne dla kadr wymiaru sprawiedliwości Irlandii Północnej dotyczące postępowania w przypadku utraty lub ewentualnej utraty danych oraz procedury rozwiązywania wszelkich kwestii z tym związanych ([113]).

(102) W Szkocji Lord President (zwierzchnik sądownictwa) wyznaczył sędziego sprawującego nadzór nad ochroną danych osobowych, który rozpatruje wszelkie skargi dotyczące ochrony danych. Odbywa się to na zasadach rozpatrywania skarg sądowych, które odzwierciedlają zasady określone dla Anglii i Walii ([114]).

(103) Natomiast jeżeli chodzi o Sąd Najwyższy, wyznaczono jednego z sędziów tego sądu do sprawowania nadzoru nad ochroną danych.

2.6.4. *Środki zaskarżenia*

(104) W celu zapewnienia odpowiedniej ochrony, a zwłaszcza egzekwowania praw indywidualnych, osoba, której dane dotyczą, powinna mieć możliwość korzystania ze skutecznych administracyjnych i sądowych środków zaskarżenia, w tym dochodzenia odszkodowania.

---

([107]) Art. 117 DPA 2018.

([108]) Panel jest odpowiedzialny za zapewnienie wytycznych i szkoleń dla wymiaru sprawiedliwości. Rozpatruje on również skargi wniesione przez osoby, których dane dotyczą, dotyczące przetwarzania danych osobowych przez sądy, trybunały i osoby fizyczne w ramach sprawowania przez nie wymiaru sprawiedliwości. Celem panelu jest zapewnienie środków umożliwiających rozpatrzenie wszelkich skarg. Jeżeli skarżący nie jest zadowolony z decyzji podjętej przez panel i dostarcza dodatkowy materiał dowodowy, panel może ponownie rozważyć swoją decyzję. Chociaż sam panel nie nakłada sankcji finansowych, jeżeli uzna, że doszło do wystarczająco poważnego naruszenia przepisów DPA 2018, może skierować sprawę do Biura ds. Badania Funkcjonowania Wymiaru Sprawiedliwości (Judicial Conduct Investigation Office, JCIO), które rozpatrzy skargę. Jeżeli skarga zostanie podtrzymana, lord kanclerz (Lord Chancellor) i Lord Chief Justice (lub sędzia wyższego szczebla upoważniony do działania w jego imieniu) decydują o tym, jakie działania należy podjąć wobec osoby sprawującej urząd. Działania te mogą obejmować, według stopnia powagi: formalną opinię, formalne ostrzeżenie i upomnienie, a w ostateczności usunięcie ze stanowiska. Jeżeli dana osoba jest niezadowolona ze sposobu rozpatrzenia skargi przez JCIO, może złożyć dalszą skargę do Rzecznika Praw Obywatelskich ds. mianowań sądowych i postępowania sądowego (Judicial Appointments and Conduct Ombudsman) (zob. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Rzecznik Praw Obywatelskich jest uprawniony do zwrócenia się do JCIO o ponowne rozpatrzenie skargi i może zaproponować wypłatę odszkodowania na rzecz skarżącego, jeżeli uważa, że poniósł on szkodę w wyniku niewłaściwego administrowania.

([109]) Oświadczenie o ochronie prywatności wydane przez Lord Chief Justice i Senior President of Tribunals jest dostępne pod adresem: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([110]) Oświadczenie o ochronie prywatności wydane przez Lord Chief Justice Irlandii Północnej jest dostępne pod adresem: https://judiciaryni.uk/data-privacy.

([111]) Oświadczenie o ochronie prywatności szkockich sądów i trybunałów jest dostępne pod adresem: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([112]) Sędzia sprawujący nadzór nad ochroną danych osobowych udziela wskazówek kadrom wymiaru sprawiedliwości i bada naruszenia lub skargi dotyczące przetwarzania danych osobowych przez sądy lub osoby fizyczne w ramach sprawowania przez nie wymiaru sprawiedliwości.

([113]) W przypadku uznania, że skarga lub naruszenie są poważne, przekazuje się je urzędnikowi ds. skarg sądowych w celu przeprowadzenia dalszego dochodzenia zgodnie z kodeksem postępowania w sprawie skarg opublikowanym przez Lord Chief Justice Irlandii Północnej. Skutkiem takiej skargi może być: zaniechanie dalszych działań, porada, szkolenie lub opieka mentorska, nieformalne ostrzeżenie, formalne ostrzeżenie, ostatnie ostrzeżenie, ograniczenie praktyki lub skierowanie sprawy do ustawowego trybunału. Kodeks postępowania w sprawie skarg opublikowany przez Lord Chief Justice Irlandii Północnej jest dostępny pod adresem: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp.._1.pdf.

([114]) Każda uzasadniona skarga jest badana przez sędziego sprawującego nadzór nad ochroną danych osobowych i kierowana do Lord President, który ma prawo udzielić porady, formalnego ostrzeżenia lub nagany, jeśli uzna to za konieczne (równoważne zasady obowiązują członków trybunałów i są dostępne pod adresem: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Po pierwsze, osoba, której dane dotyczą, ma prawo do wniesienia skargi do Komisarza ds. Informacji, jeżeli uważa, że doszło do naruszenia RODO UK w odniesieniu do danych osobowych, które jej dotyczą ([115]). W RODO UK zachowano bez istotnych zmian przepisy dotyczącego tego prawa, określone w art. 77 rozporządzenia (UE) 2016/679. To samo dotyczy art. 57 ust. 1 lit. f) i art. 57 ust. 2, w których określono zadania Komisarza w odniesieniu do rozpatrywania skarg. Jak opisano w motywach 92–98 powyżej, Komisarz ds. Informacji jest uprawniony do oceny przestrzegania RODO UK i DPA 2018 przez administratora i podmiot przetwarzający, wezwania ich do podjęcia lub zaniechania koniecznych kroków w przypadku nieprzestrzegania przepisów i nałożenia grzywien.

(106) Po drugie, RODO UK i DPA 2018 zapewniają prawo do środka ochrony prawnej przeciwko Komisarzowi ds. Informacji. Zgodnie z art. 78 ust. 1 RODO UK osoba fizyczna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji Komisarza jej dotyczącej. W ramach kontroli sądowej sędzia bada decyzję zaskarżoną w pozwie i sprawdza, czy Komisarz ds. Informacji działał zgodnie z prawem. Ponadto, zgodnie z art. 78 ust. 2 RODO UK, jeżeli Komisarz nie rozpatrzy odpowiednio skargi złożonej przez osobę, której dane dotyczą, ([116]) skarżący może skorzystać z środka ochrony prawnej przed sądem. Może on wystąpić do trybunału pierwszej instancji o nakazanie Komisarzowi podjęcia odpowiednich kroków w celu udzielenia odpowiedzi na skargę lub poinformowania skarżącego o postępach w rozpatrywaniu skargi ([117]). Ponadto każda osoba, której Komisarz doręczył jedno z wyżej wymienionych zawiadomień (zawiadomienie informacyjne, oceniające, egzekucyjne lub w sprawie sankcji), może odwołać się do trybunału pierwszej instancji ([118]). Jeżeli Trybunał uzna, że decyzja Komisarza ds. Informacji nie jest zgodna z prawem lub że Komisarz powinien był skorzystać z przysługującej mu swobody uznania w inny sposób, Trybunał uwzględnia odwołanie lub zastępuje zawiadomienie lub decyzję innym zawiadomieniem lub decyzją, które Komisarz mógł wydać.

(107) Po trzecie, osoby fizyczne mogą wnieść środki zaskarżenia przeciwko administratorom i podmiotom przetwarzającym bezpośrednio do sądu na podstawie art. 79 RODO UK i art. 167 DPA 2018. Jeżeli po otrzymaniu wniosku osoby, której dane dotyczą, sąd stwierdzi, że doszło do naruszenia jej praw wynikających z ustawodawstwa w dziedzinie ochrony danych, sąd może nakazać administratorowi w odniesieniu do tego przetwarzania lub podmiotowi przetwarzającemu działającemu w imieniu tego administratora podjęcie kroków określonych w nakazie lub zaniechanie podejmowania kroków określonych w nakazie.

(108) Ponadto, zgodnie z art. 82 RODO UK i art. 168 DPA 2018 każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO UK, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Przepisy dotyczące odszkodowania i odpowiedzialności zawarte w art. 82 ust. 1–5 RODO UK są identyczne z odpowiadającymi im przepisami rozporządzenia (UE) 2016/679. Zgodnie z art. 168 DPA 2018 szkody niemajątkowe obejmują również cierpienie. Zgodnie z art. 80 RODO UK osoba, której dane dotyczą, ma również prawo do upoważnienia reprezentatywnego organu lub reprezentatywnej organizacji do złożenia do Komisarza skargi w jej imieniu (na podstawie art. 77 RODO UK) oraz do wykonywania w jej imieniu praw, o których mowa w art. 78 (prawo do skutecznego środka ochrony prawnej przed sądem przeciwko Komisarzowi), art. 79 (prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu) oraz art. 82 (prawo do odszkodowania i pociągnięcia do odpowiedzialności) RODO UK.

(109) Po czwarte, oprócz opisanych powyżej możliwości wniesienia środków zaskarżenia każda osoba, która uważa, że jej prawa, w tym prawa do prywatności i ochrony danych, zostały naruszone przez organy publiczne, może dochodzić roszczeń przed sądami Zjednoczonego Królestwa na podstawie ustawy o prawach człowieka z 1998 r. ([119]) Osoba fizyczna, która twierdzi, że organ publiczny działał (lub zamierza działać) w sposób niezgodny z prawem określonym w konwencji, a w rezultacie niezgodny z prawem w rozumieniu art. 6 ust. 1 ustawy o prawach człowieka z 1998 r., może wytoczyć powództwo przeciwko temu organowi przed właściwy sąd lub trybunał lub powołać się na dane prawa w dowolnym postępowaniu sądowym, jeśli jest (lub byłaby) ofiarą działania niezgodnego z prawem.

(110) Jeśli sąd stwierdzi, że jakiekolwiek działanie organu publicznego jest niezgodne z prawem, może – w ramach swojej właściwości – zastosować taki środek zabezpieczający lub środek ochrony prawnej lub wydać taki nakaz, jaki uzna za sprawiedliwy i właściwy ([120]). Sąd może również orzec, że przepis ustawodawczy jest niezgodny z prawem określonym w konwencji.

---

([115]) Art. 77 RODO UK.

([116]) Art. 166 DPA 2018 odnosi się w szczególności do następujących sytuacji: a) gdy Komisarz nie podejmie odpowiednich kroków w celu udzielenia odpowiedzi na skargę; b) gdy Komisarz nie przekaże skarżącemu informacji o postępach w rozpatrywaniu skargi lub o skutkach rozpatrzenia skargi w terminie trzech miesięcy od chwili otrzymania skargi przez Komisarza; lub c) jeżeli, w przypadku niezakończenia rozpatrywania skargi w tym okresie, Komisarz nie poinformuje o tym skarżącego w okresie kolejnych trzech miesięcy.

([117]) Art. 78 ust. 2 RODO UK i art. 166 DPA 2018.

([118]) Art. 78 ust. 1 RODO UK i art. 162 DPA 2018.

([119]) Art. 7 ust. 1 ustawy o prawach człowieka z 1998 r. Zgodnie z art. 7 ust. 7 osoba jest ofiarą działania niezgodnego z prawem tylko wówczas, gdy byłaby ofiarą w rozumieniu art. 34 Konwencji o ochronie praw człowieka i podstawowych wolności, gdyby w związku z tym działaniem wszczęto postępowanie przed Europejskim Trybunałem Praw Człowieka.

([120]) Art. 8 ust. 1 ustawy o prawach człowieka z 1998 r.

(111) Ponadto po wyczerpaniu krajowych środków ochrony prawnej osobie fizycznej przysługuje środek zaskarżenia przed Europejskim Trybunałem Praw Człowieka z tytułu naruszeń praw gwarantowanych na mocy Konwencji o ochronie praw człowieka i podstawowych wolności.

### 3. DOSTĘP DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII EUROPEJSKIEJ I ICH WYKORZYSTYWANIE PRZEZ ORGANY PUBLICZNE W ZJEDNOCZONYM KRÓLESTWIE

(112) Komisja oceniła również ramy prawne Zjednoczonego Królestwa dotyczące gromadzenia danych osobowych przekazywanych podmiotom gospodarczym w Zjednoczonym Królestwie i późniejszego ich wykorzystywania przez organy publiczne Zjednoczonego Królestwa w interesie publicznym, w szczególności do celów ścigania przestępstw i do celów dotyczących bezpieczeństwa narodowego (zwanego dalej „dostępem rządowym"). Oceniając, czy warunki dostępu rządowego do danych przekazywanych do Zjednoczonego Królestwa na podstawie niniejszej decyzji spełniałyby kryterium „zasadniczej odpowiedniości" zgodnie z art. 45 ust. 1 rozporządzenia (UE) 2016/679, zgodnie z wykładnią dokonaną przez Trybunał Sprawiedliwości Unii Europejskiej w świetle Karty praw podstawowych, Komisja wzięła pod uwagę w szczególności następujące kryteria.

(113) Po pierwsze, każde ograniczenie prawa do ochrony danych osobowych musi być przewidziane ustawą, a podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa ([121]).

(114) Po drugie, aby spełnić wymóg proporcjonalności, zgodnie z którym wyjątki od ochrony danych osobowych i ograniczenia tej ochrony mogą być stosowane tylko w takim zakresie, w jakim jest to absolutnie niezbędne w demokratycznym społeczeństwie do osiągnięcia szczególnych celów leżących w interesie ogólnym równoważnych z celami uznanymi przez Unię, ustawodawstwo danego państwa trzeciego, które zezwala na ingerencję, musi określać jasne i precyzyjne reguły dotyczące zakresu i stosowania danych środków oraz ustanawiać minimalne wymagania służące temu, aby osoby, których dane osobowe zostały przekazane, były zaopatrzone w wystarczające zabezpieczenia umożliwiające rzeczywistą ochronę ich danych przed ryzykiem nadużyć ([122]). Ustawodawstwo powinno w szczególności wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych ([123]), a także obejmować spełnienie takich wymogów niezależnym nadzorem ([124]).

(115) Po trzecie, ustawodawstwo to musi być prawnie wiążące na mocy prawa krajowego, a wspomniane wymogi prawne muszą być nie tylko wiążące dla władz, ale także egzekwowalne wobec władz danego państwa trzeciego przed sądami ([125]). W szczególności osobom, których dane dotyczą, powinna przysługiwać możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących ich danych osobowych lub spowodowania korekty lub usunięcia takich danych ([126]).

#### 3.1. **Ogólne ramy prawne**

(116) Dostęp rządowy w Zjednoczonym Królestwie, w ramach wykonywania uprawnień przez organ publiczny, musi się odbywać z pełnym poszanowaniem prawa. Zjednoczone Królestwo ratyfikowało Konwencję o ochronie praw człowieka i podstawowych wolności (zob. motyw 9) i wszystkie organy publiczne w Zjednoczonym Królestwie są zobowiązane do działania zgodnie z jej postanowieniami ([127]). Art. 8 konwencji stanowi, że jakakolwiek ingerencja w prywatność musi być zgodna z prawem, musi służyć osiągnięciu jednego z celów określonych w art. 8 ust. 2 oraz musi być proporcjonalna w odniesieniu do tego celu. Art. 8 wymaga również, aby ingerencja była „przewidywalna", tj. miała jasną, dostępną podstawę prawną, oraz aby prawo obejmowało odpowiednie zabezpieczenia zapobiegające nadużyciom.

(117) Ponadto Europejski Trybunał Praw Człowieka określił w swoim orzecznictwie, że wszelkie ingerencje w prawo do prywatności i ochrony danych powinny podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru, który musi być zapewniony albo przez sędziego, albo przez inny niezależny organ ([128]) (np. organ administracji lub organ parlamentarny).

---

([121]) Zob. Schrems II, pkt 174–175 i przywołane tam orzecznictwo. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również sprawa C-623/17 Privacy International, ECLI:EU:C:2020:790, pkt 65 oraz sprawy połączone C-511/18, C-512/18 i C-520/18 La Quadrature du Net i in., ECLI:EU:C:2020:791, pkt 175.

([122]) Zob. Schrems II, pkt 176 i 181, oraz przywołane tam orzecznictwo. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również Privacy International, pkt 68, oraz La Quadrature du Net i in., pkt 132.

([123]) Zob. Schrems II, pkt 176. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również Privacy International, pkt 68, oraz La Quadrature du Net i in., pkt 132.

([124]) Zob. Schrems II, pkt 179.

([125]) Zob. Schrems II, pkt 181–182.

([126]) Zob. Schrems I, pkt 95, i Schrems II, pkt 194. W tym zakresie TSUE podkreślił w szczególności, że poszanowanie art. 47 Karty praw podstawowych, gwarantującego prawo do skutecznego środka prawnego przed niezawisłym i bezstronnym sądem, „przyczynia się do wypracowania wymaganego w Unii stopnia ochrony i [jego] poszanowanie Komisja musi stwierdzić, zanim wyda na podstawie art. 45 ust. 1 rozporządzenia (UE) 2016/679 decyzję stwierdzającą odpowiedni stopień ochrony" (Schrems II, pkt 186).

([127]) Art. 6 ustawy o prawach człowieka z 1998 r.

([128]) Europejski Trybunał Praw Człowieka, Klass i in./Niemcy, skarga nr 5029/71, pkt 17–51.

(118) Ponadto osobom fizycznym musi przysługiwać skuteczny środek ochrony prawnej, a Europejski Trybunał Praw Człowieka wyjaśnił, że środek ten musi zapewniać niezależny i bezstronny organ, który przyjął własny regulamin, w którego skład muszą wchodzić członkowie zajmujący (obecnie lub w przeszłości) wysokie stanowiska sędziowskie lub będący doświadczonymi prawnikami, a złożenie skargi do tego organu nie może wiązać się z ciężarem dowodu po stronie skarżącego. Przy rozpatrywaniu skarg od osób fizycznych niezależny i bezstronny organ powinien mieć dostęp do wszystkich istotnych informacji, w tym do materiałów niejawnych. Organ ten powinien wreszcie posiadać uprawnienia do usuwania niezgodności ([129]).

(119) W 2018 r. Zjednoczone Królestwo ratyfikowało również Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108) i podpisało protokół zmieniający Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (znany jako konwencja nr 108+) ([130]). Art. 9 konwencji nr 108 stanowi, że odstępstwa od ogólnych zasad ochrony danych (art. 5 – Jakość danych), zasad regulujących szczególne kategorie danych (art. 6 – Szczególne kategorie danych) i praw osób, których dane dotyczą, (art. 8 – Dodatkowe prawa osób, których dane dotyczą) są dopuszczalne tylko wtedy, gdy takie odstępstwo jest przewidziane przez prawo strony konwencji i jest środkiem niezbędnym w demokratycznym społeczeństwie w celu ochrony bezpieczeństwa państwa, bezpieczeństwa publicznego, interesów finansowych państwa lub zwalczania przestępstw lub w celu ochrony osoby, której dane dotyczą, lub praw i wolności innych osób ([131]).

(120) W związku z tym dzięki członkostwu w Radzie Europy, przystąpieniu do Konwencji o ochronie praw człowieka i podstawowych wolności i poddaniu się jurysdykcji Europejskiego Trybunału Praw Człowieka Zjednoczone Królestwo podlega szeregowi zobowiązań zapisanych w prawie międzynarodowym, które kształtują jego system dostępu rządowego w oparciu o zasady, zabezpieczenia i prawa indywidualne podobne do tych gwarantowanych w prawie Unii i mających zastosowanie do państw członkowskich. Jak podkreślono w motywie 19, nieprzerwane przestrzeganie takich instrumentów stanowi zatem szczególnie istotny element oceny, na której opiera się niniejsza decyzja.

(121) Ponadto szczególne zabezpieczenia służące ochronie danych i prawa do ochrony danych zagwarantowano w DPA 2018 w odniesieniu do sytuacji, gdy dane są przetwarzane przez organy publiczne, w tym przez organy ścigania i bezpieczeństwa narodowego.

(122) W szczególności system przetwarzania danych osobowych w kontekście ścigania przestępstw określono w części 3 DPA 2018, którą uchwalono w celu transpozycji dyrektywy (UE) 2016/680. Część 3 DPA 2018 ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom ([132]).

(123) Pojęcie „właściwego organu" zdefiniowano w art. 30 DPA 2018 jako osobę wymienioną w załączniku 7 do DPA 2018, a także jako wszelką inną osobę w zakresie, w jakim pełni ona funkcje ustawowe do jakichkolwiek celów ścigania przestępstw ([133]). Jak wyjaśniono poniżej (zob. motyw 139), niektóre właściwe organy (np. Krajowa Agencja ds. Zwalczania Przestępczości) mogą pod pewnymi warunkami korzystać z uprawnień przewidzianych w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. (IPA 2016). W takim przypadku zabezpieczenia przewidziane w IPA 2016 będą miały zastosowanie w uzupełnieniu zabezpieczeń przewidzianych w części 3 DPA 2018. Służby wywiadowcze (Tajna Służba Wywiadowcza, Służba Bezpieczeństwa i Centrala Łączności Rządowej) nie są „właściwymi organami" ([134]) w rozumieniu części 3 DPA 2018 i w związku z tym przepisy tej części nie mają zastosowania do żadnych ich działań. Odrębna część organu ochrony danych z 2018 r. (część 4) poświęcona jest przetwarzaniu danych osobowych przez służby wywiadowcze (więcej szczegółów w motywie 125).

([129]) Europejski Trybunał Praw Człowieka, Kennedy/Zjednoczone Królestwo, skarga nr 26839/05, („Kennedy"), pkt 167 i 190.

([130]) Więcej informacji na temat Konwencji o ochronie praw człowieka i podstawowych wolności i wprowadzenia jej do prawa Zjednoczonego Królestwa ustawą o prawach człowieka z 1998 r., jak również na temat konwencji nr 108, można znaleźć w motywie 9.

([131]) Podobnie, zgodnie z art. 11 konwencji nr 108+, ograniczenia niektórych szczególnych praw i obowiązków wynikających z konwencji do celów bezpieczeństwa narodowego lub zapobiegania przestępczości, prowadzenia postępowań przygotowawczych i ścigania czynów zabronionych i wykonywania kar są dopuszczalne wyłącznie wtedy, gdy takie ograniczenie jest przewidziane prawem, nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym. Czynności przetwarzania do celów bezpieczeństwa narodowego i obrony muszą również podlegać niezależnemu i skutecznemu przeglądowi i nadzorowi na mocy ustawodawstwa krajowego danej strony konwencji.

([132]) Art. 31 DPA 2018.

([133]) Właściwe organy wymienione w załączniku 7 obejmują nie tylko siły policyjne, ale również wszystkie ministerialne departamenty rządowe Zjednoczonego Królestwa, a także inne organy pełniące funkcje dochodzeniowo-śledcze (np. Commissioner for Her Majesty's Revenue and Customs (organ podatkowy i celny Zjednoczonego Królestwa), National Crime Agency (Krajową Agencję ds. Zwalczania Przestępczości), Welsh Revenue Authority (walijski organ skarbowy), Competition and Markets Authority (urząd ds. konkurencji i rynków) lub Her Majesty's Land Register (rejestr gruntów Zjednoczonego Królestwa), organy prokuratorskie, inne organy wymiaru sprawiedliwości w sprawach karnych i inne podmioty uprawnione lub organizacje, które prowadzą działania związane ze ściganiem przestępstw (m.in. wymienieni w załączniku 7 DPA 2018 dyrektorzy prokuratury, Dyrektor Urzędu Prokuratury Irlandii Północnej lub Komisarz ds. Informacji).

([134]) Art. 30 ust. 2 DPA 2018.

(124) Podobnie jak w przypadku dyrektywy (UE) 2016/680 w części 3 DPA 2018 określono zasady dotyczące zgodności z prawem i rzetelności ([135]), ograniczenia celu ([136]), minimalizacji danych ([137]), prawidłowości ([138]), ograniczenia przechowywania ([139]) i bezpieczeństwa ([140]). W ustawodawstwie określono szczególne obowiązki w zakresie przejrzystości ([141]) i zapewniono osobom fizycznym prawo dostępu do danych ([142]), prawo do sprostowania i usunięcia danych ([143]) oraz prawo do niepodlegania zautomatyzowanemu podejmowaniu decyzji ([144]). Właściwe organy są również zobowiązane do uwzględniania ochrony danych w fazie projektowania oraz stosowania domyślnej ochrony danych, do rejestrowania czynności przetwarzania oraz, w przypadku niektórych operacji przetwarzania, do przeprowadzania ocen skutków dla ochrony danych i do uprzedniego konsultowania się z Komisarzem ds. Informacji ([145]). Zgodnie z art. 56 DPA 2018 organy muszą wykazać, że przestrzegają przepisów. Ponadto są one zobowiązane do wprowadzenia odpowiednich środków zapewniających bezpieczeństwo przetwarzania ([146]) i podlegają szczegółowym obowiązkom w przypadku naruszenia ochrony danych, w tym mają obowiązek zgłaszania takich naruszeń Komisarzowi ds. Informacji i osobom, których dane dotyczą ([147]). Podobnie jak w przypadku dyrektywy (UE) 2016/680 istnieje również wymóg wyznaczenia przez administratora (chyba że jest nim sąd lub inny organ sądowy sprawujący wymiar sprawiedliwości) inspektora ochrony danych ([148]), który pomaga administratorowi wywiązać się z jego obowiązków, a także monitoruje ich wypełnianie ([149]). Ponadto aby zapewnić ciągłość ochrony, w ustawodawstwie określono szczegółowe wymogi dotyczące międzynarodowego przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych do celów ścigania przestępstw ([150]). W dniu przyjęcia niniejszej decyzji Komisja [przyjęła] decyzję stwierdzającą odpowiedni stopień ochrony 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 zapewnia stopień ochrony, który zasadniczo odpowiada ochronie zagwarantowanej na mocy dyrektywy (UE) 2016/680.

(125) Część 4 DPA 2018 ma zastosowanie do wszelkiego przetwarzania danych przez służby wywiadowcze lub w ich imieniu. W szczególności określono w niej główne zasady ochrony danych (zgodność z prawem, rzetelność i przejrzystość ([151]); ograniczenie celu ([152]); minimalizacja danych ([153]); prawidłowość ([154]); ograniczenie przechowywania ([155]) i bezpieczeństwo ([156])), określono warunki dotyczące przetwarzania szczególnych kategorii danych ([157]), zapewniono prawa osób, których dane dotyczą ([158]), określono obowiązek uwzględniania

([135]) Art. 35 DPA 2018.
([136]) Art. 36 DPA 2018.
([137]) Art. 37 DPA 2018.
([138]) Art. 38 DPA 2018.
([139]) Art. 39 DPA 2018.
([140]) Art. 40 DPA 2018.
([141]) Art. 44 DPA 2018.
([142]) Art. 45 DPA 2018.
([143]) Art. 46 i 47 DPA 2018.
([144]) Art. 49 i 50 DPA 2018.
([145]) Art. 56–65 DPA 2018.
([146]) Art. 66 DPA 2018.
([147]) Art. 67–68 DPA 2018.
([148]) Art. 69-71 DPA 2018.
([149]) Art. 67–68 DPA 2018.
([150]) Część 3 rozdział 5 DPA 2018.
([151]) Zgodnie z art. 86 ust. 6 DPA 2018, aby stwierdzić rzetelność i przejrzystość przetwarzania, należy uwzględnić metodę wykorzystaną do uzyskania tych danych. W tym sensie wymóg rzetelności i przejrzystości jest spełniony, jeśli dane uzyskano od osoby, która jest zgodnie z prawem upoważniona lub zobowiązana do ich dostarczenia.
([152]) Zgodnie z art. 87 DPA 2018 cele przetwarzania muszą być konkretne, wyraźne i prawnie uzasadnione. Danych nie można przetwarzać w sposób niezgodny z celami, dla których zostały zebrane. Zgodnie z art. 87 ust. 3 DPA 2018 dalsze zgodne z celami przetwarzanie danych osobowych może być dozwolone tylko wtedy, gdy administrator jest prawnie upoważniony do przetwarzania danych w tym celu, a przetwarzanie jest niezbędne i proporcjonalne do tego innego celu. Przetwarzanie należy uznać za zgodne z celami, jeśli polega ono na przetwarzaniu do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych i podlega odpowiednim zabezpieczeniom (art. 87 ust. 4 DPA 2018).
([153]) Dane osobowe muszą być adekwatne, stosowne i ograniczone do celów, dla których są przetwarzane (art. 88 DPA 2018).
([154]) Dane osobowe muszą być prawidłowe i aktualne (art. 89 DPA 2018).
([155]) Danych osobowych nie wolno przechowywać dłużej niż jest to niezbędne (art. 90 DPA 2018).
([156]) Szósta zasada ochrony danych polega na tym, że dane osobowe muszą być przetwarzane w sposób obejmujący zastosowanie odpowiednich środków bezpieczeństwa w celu zabezpieczenia przed ryzykiem wynikającym z przetwarzania danych osobowych. Ryzyko to obejmuje m.in. przypadkowy lub nieuprawniony dostęp do danych osobowych lub ich zniszczenie, utratę, wykorzystanie, modyfikację lub ujawnienie (art. 91 DPA 2018). W art. 107 wymaga się również, aby: 1) każdy administrator wdrożył odpowiednie środki bezpieczeństwa adekwatne do ryzyka wynikającego z przetwarzania danych osobowych oraz aby 2) w przypadku zautomatyzowanego przetwarzania każdy administrator i każdy podmiot przetwarzający wdrożyli środki zapobiegawcze lub zaradcze na podstawie oceny ryzyka.
([157]) Art. 86 ust. 2 lit. b) i załącznik 10 do DPA 2018.
([158]) Część 4 rozdział 3 DPA 2018, mianowicie prawa: do dostępu, sprostowania i usunięcia, do wniesienia sprzeciwu wobec przetwarzania i niepodlegania zautomatyzowanemu podejmowaniu decyzji, do interwencji w zautomatyzowane podejmowanie decyzji oraz do uzyskania informacji o podejmowaniu decyzji w taki sposób. Administrator musi ponadto udzielić osobie, której dane dotyczą, informacji na temat przetwarzania jej danych osobowych. Jak wyjaśniono w wytycznych Komisarza ds. Informacji dotyczących przetwarzania danych przez służby wywiadowcze, osoby fizyczne mogą wykonywać wszystkie swoje prawa (w tym dotyczące złożenia wniosku o sprostowanie) poprzez złożenie skargi do Komisarza ds. Informacji lub wniesienie sprawy do sądu (zob. wytyczne Komisarza ds. Informacji dotyczące przetwarzania danych przez służby wywiadowcze, dostępne pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

ochrony danych w fazie projektowania ([159]) i uregulowano międzynarodowe przekazywanie danych osobowych ([160]). Komisarz ds. Informacji wydał niedawno szczegółowe wytyczne dotyczące przetwarzania danych przez agencje wywiadowcze na podstawie części 4 DPA 2018 ([161]).

(126) Jednocześnie w art. 110 DPA 2018 przewidziano wyłączenie stosowania określonych przepisów zawartych w części 4 tej ustawy ([162]), gdy takie wyłączenie jest wymagane do ochrony bezpieczeństwa narodowego. Na wyłączenie to można się powołać na podstawie analizy poszczególnych przypadków ([163]). Jak wyjaśniły władze Zjednoczonego Królestwa i jak potwierdzono w orzecznictwie, „administrator musi uwzględnić faktyczne konsekwencje dla bezpieczeństwa narodowego lub obrony narodowej, wynikające z ewentualnego zastosowania się do konkretnego przepisu dotyczącego ochrony danych, z uwzględnieniem racjonalnej możliwości przestrzegania zwykłej zasady bez narażania bezpieczeństwa narodowego lub obrony narodowej" ([164]). Komisarz ds. Informacji sprawuje nadzór nad tym, czy wyłączenie zostało zastosowane prawidłowo ([165]).

(127) Ponadto jeżeli chodzi o możliwość ograniczenia stosowania określonych powyżej przepisów zgodnie z częścią 111 DPA 2018 ze względu na ochronę „bezpieczeństwa narodowego", administrator może ubiegać się o podpisane przez ministra lub Prokuratora Generalnego poświadczenie potwierdzające, że ograniczenie takich praw jest niezbędnym i proporcjonalnym środkiem służącym ochronie bezpieczeństwa narodowego ([166]).

(128) Rząd Zjednoczonego Królestwa opublikował wytyczne w celu ułatwienia administratorom podjęcia decyzji o ewentualnym wystąpieniu o wydanie poświadczenia bezpieczeństwa narodowego na podstawie DPA 2018, w których to wytycznych w szczególności podkreślono, że wszelkie ograniczenia praw osób, których dane dotyczą, do celów ochrony bezpieczeństwa narodowego muszą być proporcjonalne i niezbędne ([167]). Wszelkie poświadczenia bezpieczeństwa narodowego muszą być publikowane na stronie internetowej Komisarza ds. Informacji ([168]).

([159]) Art. 103 DPA 2018.

([160]) Art. 109 DPA 2018. Przekazywanie danych osobowych do organizacji międzynarodowych lub państw poza terytorium Zjednoczonego Królestwa jest możliwe, jeśli przekazanie jest środkiem niezbędnym i proporcjonalnym stosowanym do celów wykonywania przez administratora funkcji ustawowych lub do innych celów przewidzianych w określonych artykułach ustawy o Służbie Bezpieczeństwa z 1989 r. i ustawy o służbach wywiadowczych z 1994 r.

([161]) Wytyczne Komisarza ds. Informacji, zob. przypis 158.
Art. 30 DPA 2018 i załącznik 7 do DPA 2018.

([162]) W art. 110 ust. 2 DPA 2018 wymieniono przepisy, w przypadku których dopuszcza się wyłączenie stosowania. Obejmują one zasady ochrony danych (z wyjątkiem zasady zgodności z prawem), prawa osób, których dane dotyczą, obowiązek informowania Komisarza ds. Informacji o naruszeniu ochrony danych, uprawnienia Komisarza ds. Informacji do przeprowadzania kontroli zgodnie z zobowiązaniami międzynarodowymi, określone uprawnienia Komisarza ds. Informacji do egzekwowania przestrzegania przepisów, przepisy, zgodnie z którymi niektóre naruszenia ochrony danych stanowią czyn zabroniony, oraz przepisy dotyczące szczególnych celów przetwarzania, takich jak przetwarzanie do celów dziennikarskich, akademickich czy artystycznych.

([163]) Zob. Baker przeciwko Secretary of State, zob. przypis 61.

([164]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Ramy dotyczące ochrony danych związanych z bezpieczeństwem narodowym i uprawnień dochodzeniowo-śledczych, s. 15–16 (zob. przypis 31). Zob. również sprawa Baker przeciwko Secretary of State (zob. przypis 61), w której sąd unieważnił poświadczenie bezpieczeństwa narodowego wydane przez Home Secretary (ministra spraw wewnętrznych) i potwierdzające zastosowanie wyjątku dotyczącego bezpieczeństwa narodowego, stwierdzając, że nie ma powodów do określenia ogólnego wyjątku od obowiązku odpowiadania na wnioski o udzielenie dostępu oraz że dopuszczenie takiego wyjątku we wszystkich okolicznościach bez analizy poszczególnych przypadków wykracza poza to, co jest niezbędne i proporcjonalne do ochrony bezpieczeństwa narodowego.

([165]) Zob. protokół ustaleń między Komisarzem ds. Informacji a wspólnotą wywiadowczą Zjednoczonego Królestwa (UKIC), zgodnie z którym „po otrzymaniu przez Komisarza ds. Informacji skargi od osoby, której dane dotyczą, Komisarz upewnia się, że sprawę rozstrzygnięto prawidłowo i, w stosownych przypadkach, że wszelkie wyłączenia zastosowano w odpowiedni sposób". Protokół ustaleń między Biurem Komisarza ds. Informacji a wspólnotą wywiadowczą Zjednoczonego Królestwa, pkt 16, dostępny pod adresem: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) W DPA 2018 uchylono możliwość wydawania poświadczenia na podstawie art. 28 ust. 2 ustawy o ochronie danych z 1998 r. Możliwość wydawania „starych poświadczeń" nadal istnieje jednak w zakresie związanym z ewentualnym zaskarżeniem dotyczącym przeszłości na mocy ustawy z 1998 r. (zob. pkt 17 części 5 załącznika 20 do DPA 2018). Ta możliwość wydaje się jednak mieć zastosowanie jedynie w rzadkich przypadkach, np. gdy osoba, której dane dotyczą, kwestionuje korzystanie z wyłączenia dotyczącego bezpieczeństwa narodowego w odniesieniu do przetwarzania danych przez organ publiczny na mocy ustawy z 1998 r. Należy zauważyć, że w takich przypadkach art. 28 ustawy o ochronie danych z 1998 r. będzie miał zastosowanie w całości, włączając w to możliwość zaskarżenia poświadczenia przed sądem przez osobę, której dane dotyczą.

([167]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego wydawanych na podstawie DPA 2018, dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Zgodnie z wyjaśnieniem przedstawionym przez władze Zjednoczonego Królestwa, chociaż poświadczenie stanowi jednoznaczny dowód na to, że wyłączenie ma zastosowanie do danych lub przetwarzania określonych w poświadczeniu, nie zwalnia ono administratora z obowiązku zbadania, czy w danym przypadku istnieje potrzeba korzystania z przedmiotowego wyłączenia.

([168]) Zgodnie z sekcją 130 DPA 2018 Komisarz ds. Informacji może podjąć decyzję o niepublikowaniu całości lub części tekstu poświadczenia, jeżeli byłoby to sprzeczne z interesem bezpieczeństwa narodowego lub interesem publicznym bądź mogłoby zagrozić bezpieczeństwu jakiejkolwiek osoby. W takich przypadkach Komisarz ds. Informacji publikuje jednak informację o wydaniu poświadczenia.

(129) Poświadczenie powinno być wydawane na czas określony, nie dłuższy niż pięć lat, tak aby podlegało regularnej ocenie przez władzę wykonawczą ([169]). W poświadczeniu określa się dane osobowe lub kategorie danych osobowych podlegające wyłączeniu, a także przepisy DPA 2018, do których wyłączenie ma zastosowanie ([170]).

(130) Należy zauważyć, że poświadczenie bezpieczeństwa narodowego nie stanowią dodatkowej podstawy ograniczania praw do ochrony danych ze względów bezpieczeństwa narodowego. Innymi słowy, administrator lub podmiot przetwarzający może powołać się na poświadczenie wyłącznie wówczas, gdy stwierdzi, że konieczne jest skorzystanie z wyłączenia dotyczącego bezpieczeństwa narodowego, co – jak wyjaśniono powyżej – jest możliwe jedynie na podstawie oceny każdego przypadku z osobna ([171]). Nawet jeżeli do danej sprawy zastosowanie ma poświadczenie bezpieczeństwa narodowego, Komisarz ds. Informacji może zbadać, czy w tym konkretnym przypadku skorzystanie z wyłączenia dotyczącego bezpieczeństwa narodowego było uzasadnione ([172]).

(131) Każdy, na kogo wydanie poświadczenia wywarło bezpośredni wpływ, może odwołać się do Wyższego Trybunału ([173]) od wydania poświadczenia ([174]) lub, gdy w poświadczeniu dane określono za pomocą ogólnego opisu, zaskarżyć stosowanie poświadczenia w odniesieniu do konkretnych danych ([175]). W takiej sytuacji Trybunał bada decyzję o wydaniu poświadczenia i orzeka, czy istniały uzasadnione podstawy do jego wydania ([176]). Może rozważyć wiele różnych aspektów, w tym niezbędność, proporcjonalność i zgodność z prawem, uwzględniając wpływ na prawa osób, których dane dotyczą, oraz wyważając potrzebę ochrony bezpieczeństwa narodowego. W rezultacie Trybunał może stwierdzić, że poświadczenie nie ma zastosowania do konkretnych danych osobowych będących przedmiotem odwołania ([177]).

(132) Inny zbiór możliwych ograniczeń dotyczy wyłączeń, które na podstawie załącznika 11 do DPA 2018 stosuje się do określonych przepisów zawartych w części 4 DPA 2018 ([178]) na potrzeby zabezpieczenia innych ważnych celów leżących w ogólnym interesie publicznym lub chronionych interesów, takich jak np. przywilej parlamentarny, prawnicza tajemnica zawodowa, przebieg postępowania sądowego lub skuteczność bojowa sił zbrojnych ([179]). Wyłączenia stosowania tych przepisów dokonuje się albo w odniesieniu do określonych kategorii informacji („ze względu na klasę"), albo w zakresie, w jakim stosowanie tych przepisów mogłoby zaszkodzić chronionemu interesowi („ze względu na szkodę") ([180]). Na wyłączenia ze względu na szkodę można się powoływać tylko w takim zakresie,

([169]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, pkt 15, zob. przypis 167.

([170]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, pkt 5, zob. przypis 167.

([171]) Zob. przypis 164.

([172]) Zgodnie z art. 102 DPA 2018 administrator musi być w stanie wykazać, że zastosował się do przepisów tej ustawy. Oznacza to, że służba wywiadowcza musiałaby wykazać Komisarzowi ds. Informacji, że korzystając z wyłączenia, uwzględniła szczególne okoliczności sprawy. Komisarz ds. Informacji publikuje również rejestr poświadczeń bezpieczeństwa narodowego, dostępny pod adresem: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) Wyższy Trybunał jest sądem właściwym do rozpoznawania odwołań od orzeczeń sądów administracyjnych niższej instancji i ma właściwość szczególną w odniesieniu do bezpośrednich odwołań od decyzji określonych organów rządowych.

([174]) Art. 111 ust. 3 DPA 2018.

([175]) Art. 111 ust. 5 DPA 2018.

([176]) W sprawie Baker przeciwko Secretary of State (zob. przypis 61) Trybunał ds. Ochrony Danych unieważnił poświadczenie bezpieczeństwa narodowego wydane przez Home Secretary (ministra spraw wewnętrznych), stwierdzając, że nie ma powodów do określenia ogólnego wyjątku od obowiązku odpowiadania na wnioski o udzielenie dostępu oraz że dopuszczenie takiego wyjątku we wszystkich okolicznościach bez analizy poszczególnych przypadków wykracza poza to, co jest niezbędne i proporcjonalne do ochrony bezpieczeństwa narodowego.

([177]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, pkt 25, zob. przypis 167.

([178]) Obejmuje to: (i) zasady ochrony danych określone w części 4 z wyjątkiem wymogu zgodności przetwarzania z prawem zawartego w pierwszej zasadzie oraz z wyjątkiem faktu, że przetwarzanie musi spełniać jeden z odpowiednich warunków określonych w załącznikach 9 i 10; (ii) prawa osób, których dane dotyczą, oraz (iii) obowiązki związane ze zgłaszaniem naruszeń Komisarzowi ds. Informacji.

([179]) Część 4 DPA 2018 zawiera ramy prawne, które mają zastosowanie do wszystkich rodzajów przetwarzania danych osobowych przez agencje wywiadowcze (a nie tylko do wykonywania ich zadań związanych z bezpieczeństwem narodowym). W związku z tym część 4 ma zastosowanie również wówczas, gdy agencje wywiadowcze przetwarzają dane np. do celów zarządzania zasobami ludzkimi, w kontekście sporów sądowych lub w kontekście zamówień publicznych. Ograniczenia wymienione w załączniku 11 mają w założeniu mieć zastosowanie głównie we wspomnianych innych kontekstach. Przykładowo w kontekście sporów z pracownikiem można powołać się na ograniczenie do celów „postępowania sądowego"; w kontekście zamówień publicznych można powołać się na ograniczenie do celów „negocjacji" itp. Jest to odzwierciedlone w wytycznych Komisarza ds. Informacji dotyczących przetwarzania danych przez służby wywiadowcze, w których jako przykład zastosowania ograniczeń na podstawie załącznika 11 podane jest negocjowanie ugody między agencją wywiadowczą a byłym pracownikiem, który występuje z roszczeniem związanym z zatrudnieniem (zob. przypis 161). Należy również zauważyć, że z tych samych ograniczeń mogą korzystać inne organy publiczne zgodnie z załącznikiem 2 do części 2 DPA 2018.

([180]) Zgodnie z ramami wyjaśniającymi Zjednoczonego Królestwa wyjątki „ze względu na klasę" są następujące: (i) informacje dotyczące nadawania tytułów i zaszczytów królewskich; (ii) prawnicza tajemnica zawodowa; (iii) poufne referencje zawodowe, szkoleniowe lub edukacyjne oraz (iv) arkusze egzaminacyjne i uzyskane oceny. Wyjątki „ze względu na szkodę" dotyczą takich kwestii jak: (i) zapobieganie przestępstwom lub ich wykrywanie; zatrzymywanie i ściganie przestępców; (ii) przywilej parlamentarny; (iii) postępowania sądowe; (iv) skuteczność bojowa Sił Zbrojnych Korony; (v) dobrobyt gospodarczy Zjednoczonego Królestwa; (vi) negocjacje z osobą, której dane dotyczą; (vii) badania naukowe lub historyczne lub cele statystyczne; (viii) archiwizacja w interesie publicznym. Zob. Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Bezpieczeństwo narodowe, s. 13, zob. przypis 31.

w jakim zastosowanie wymienionego przepisu dotyczącego ochrony danych prawdopodobnie zaszkodziłoby danemu interesowi. Stosowanie wyłączenia musi być zatem zawsze uzasadnione poprzez wskazanie odpowiedniej szkody, która prawdopodobnie powstałaby w danym przypadku. Na wyłączenia ze względu na klasę można się powoływać wyłącznie w odniesieniu do konkretnej, ściśle zdefiniowanej kategorii informacji, dla której przyznano wyłączenie. Wyłączenia te są podobne pod względem celu i skutku do szeregu wyjątków od RODO UK (określonych w załączniku 2 do DPA 2018), które z kolei odzwierciedlają cel i skutek przewidziane w art. 23 RODO.

(133) Z powyższego wynika, że w rozumieniu obowiązujących w Zjednoczonym Królestwie przepisów prawnych – oraz zgodnie z wykładnią sądów i interpretacją Komisji ds. Informacji – istnieją ograniczenia i warunki zapewniające, aby wspomniane wyłączenia i ograniczenia pozostawały w zakresie niezbędnym i proporcjonalnym do ochrony bezpieczeństwa narodowego.

### 3.2. **Dostęp organów publicznych Zjednoczonego Królestwa do danych na potrzeby ścigania przestępstw i wykorzystywanie danych przez te organy w tym celu**

(134) W prawie Zjednoczonego Królestwa ustanowiono szereg ograniczeń w zakresie dostępu do danych osobowych i korzystania z nich na potrzeby ścigania przestępstw, a także mechanizmy nadzoru i środki zaskarżenia, które są zgodne z wymogami określonymi w motywach 113–115 niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach.

#### 3.2.1. *Podstawy prawne i właściwe ograniczenia/zabezpieczenia*

(135) Zgodnie z zasadą zgodności z prawem zagwarantowaną na podstawie art. 35 DPA 2018 przetwarzanie danych osobowych do jakichkolwiek celów ścigania przestępstw jest zgodne z prawem tylko wtedy, gdy opiera się na przepisach prawa oraz albo osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie w tym celu ([181]), albo przetwarzanie jest niezbędne do wykonania zadania realizowanego w tym celu przez właściwy organ.

##### 3.2.1.1. Nakazy przeszukania i nakazy wydania dowodów

(136) W ramach prawnych Zjednoczonego Królestwa pobieranie danych osobowych od podmiotów gospodarczych – w tym tych, które przetwarzałyby dane przekazywane z UE na podstawie niniejszej decyzji stwierdzającej odpowiedni stopień ochrony – do celów ścigania przestępstw jest dopuszczalne na podstawie nakazów przeszukania ([182]) i nakazów wydania dowodów ([183]).

(137) Nakazy przeszukania wydaje sąd, zazwyczaj na wniosek funkcjonariusza prowadzącego postępowanie przygotowawcze. Nakazy umożliwiają funkcjonariuszowi wejście do pomieszczeń w celu poszukiwania materiałów lub osób istotnych dla prowadzonego przez niego postępowania przygotowawczego oraz zatrzymanie wszystkiego, co wskazano w ramach zezwolenia na przeszukanie, w tym wszelkich istotnych dokumentów lub materiałów zawierających dane osobowe ([184]). Nakaz wydania dowodów, który również musi wydać sąd, zobowiązuje wskazaną w nakazie osobę do wydania lub udostępnienia materiałów, które znajdują się w jej posiadaniu lub nad którymi sprawuje kontrolę. Wnioskodawca musi uzasadnić przed sądem, dlaczego nakaz jest niezbędny, a także dlaczego leży on w interesie publicznym. Istnieje szereg uprawnień ustawowych, które pozwalają na wydawanie

([181]) Przetwarzanie na podstawie zgody nie wydaje się istotne w kontekście odpowiedniego stopnia ochrony, ponieważ w sytuacji obejmującej przekazanie danych organ ścigania Zjednoczonego Królestwa nie pobiera danych bezpośrednio od znajdującej się w UE osoby, której dane dotyczą, na podstawie jej zgody.

([182]) Jeżeli chodzi o odpowiednią podstawę prawną, zob. art. 8 i nast. ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r. (PACE 1984) (w odniesieniu do Anglii i Walii), art. 10 i nast. zarządzenia w sprawie policji i dowodów w sprawach karnych dotyczącego Irlandii Północnej z 1989 r., a w przypadku Szkocji nakaz uzyskuje się na podstawie prawa precedensowego (zob. art. 46 ustawy w sprawie szkockiego wymiaru sprawiedliwości w sprawach karnych z 2016 r.) oraz art. 23B wersji skonsolidowanej szkockiego kodeksu karnego. Jeżeli chodzi o nakaz przeszukania wydany po zatrzymaniu, podstawę prawną stanowią art. 18 i nast. PACE 1984 (w odniesieniu do Anglii i Walii), art. 20 i nast. zarządzenia w sprawie policji i dowodów w sprawach karnych dotyczącego Irlandii Północnej z 1989 r., a w przypadku Szkocji nakaz uzyskuje się na podstawie prawa precedensowego (zob. art. 46 ustawy w sprawie szkockiego wymiaru sprawiedliwości w sprawach karnych z 2016 r.). Władze Zjednoczonego Królestwa wyjaśniły, że nakazy przeszukania wydaje sąd na wniosek funkcjonariusza prowadzącego postępowanie przygotowawcze. Nakazy umożliwiają funkcjonariuszowi wejście do pomieszczeń w celu poszukiwania materiałów lub osób istotnych dla prowadzonego przez niego postępowania przygotowawczego; wykonanie nakazu często wymaga wsparcia ze strony funkcjonariusza policji.

([183]) Jeżeli postępowanie przygotowawcze dotyczy prania pieniędzy (co obejmuje postępowania w sprawie konfiskaty i przepadku mienia w trybie postępowania cywilnego), odpowiednią podstawą prawną do wystąpienia o nakaz wydania dowodów są art. 345 i nast. ustawy o dochodach z przestępstwa z 2002 r. w przypadku Anglii, Walii i Irlandii Północnej oraz art. 380 i nast. w przypadku Szkocji. Jeżeli postępowanie przygotowawcze dotyczy spraw innych niż pranie pieniędzy, wniosek o nakaz wydania dowodów można złożyć na podstawie art. 9 i załącznika 1 do PACE 1984 w przypadku Anglii i Walii oraz art. 10 i nast. zarządzenia w sprawie policji i dowodów w sprawach karnych dotyczącego Irlandii Północnej z 1989 r. w przypadku Irlandii Północnej. W przypadku Szkocji nakaz uzyskuje się na podstawie prawa precedensowego (zob. art. 46 ustawy w sprawie szkockiego wymiaru sprawiedliwości w sprawach karnych z 2016 r.) oraz art. 23B wersji skonsolidowanej szkockiego kodeksu karnego. Władze Zjednoczonego Królestwa wyjaśniły, że nakaz wydania dowodów zobowiązuje wskazaną w nakazie osobę do wydania lub udostępnienia materiałów, które znajdują się w jej posiadaniu lub nad którymi sprawuje ona kontrolę (zob. pkt 4 załącznika 1 do PACE 1984).

([184]) Na przykład w art. 8 i 18 PACE 1984 przewidziano uprawnienia do zajęcia i zatrzymania każdej rzeczy wskazanej w zezwoleniu na przeszukanie.

nakazów przeszukania i nakazów wydania dowodów. Z każdym przepisem wiąże się osobny zbiór warunków ustawowych, które należy spełnić, aby można było wydać nakaz przeszukania ([185]) lub nakaz wydania dowodów ([186]).

(138) Nakazy wydania dowodów oraz nakazy przeszukania mogą zostać zaskarżone w ramach kontroli sądowej ([187]). Jeśli chodzi o zabezpieczenia, wszystkie organy ścigania objęte zakresem części 3 DPA 2018, mogą uzyskać dostęp do

([185]) Na przykład art. 8 i 18 PACE regulują, odpowiednio, uprawnienia sędziego pokoju do wydania nakazu oraz uprawnienia funkcjonariusza policji do przeszukania nieruchomości. W pierwszym przypadku (art. 8) przed wydaniem nakazu sędzia pokoju musi najpierw upewnić się, że istnieją uzasadnione podstawy, by sądzić, że: (i) popełniono przestępstwo podlegającego oskarżeniu publicznemu; (ii) w pomieszczeniach znajdują się materiały, które mogą mieć znaczną wartość (w odosobnieniu lub wraz z innymi materiałami) dla postępowania przygotowawczego w sprawie przestępstwa; (iii) materiały te mogą być istotnymi dowodami; (iv) nie składają się one z materiałów objętych prawniczą tajemnicą zawodową, materiałów wyłączonych lub materiałów objętych specjalną procedurą ani ich nie zawierają; oraz (v) wejście nie byłoby możliwe bez zastosowania nakazu. Jeżeli chodzi o drugi z wymienionych przypadków, art. 18 zezwala funkcjonariuszowi policji na przeszukanie pomieszczeń osoby, którą zatrzymano w związku z przestępstwem podlegającym oskarżeniu publicznemu, w poszukiwaniu materiałów innych niż materiały objęte prawniczą tajemnicą zawodową, jeżeli ma on uzasadnione podstawy, aby podejrzewać, że w pomieszczeniach znajdują się dowody dotyczące tego przestępstwa lub innego przestępstwa podlegającego oskarżeniu publicznemu, które jest podobne lub powiązane. Takie przeszukanie musi być ograniczone do odnalezienia wskazanych materiałów i musi zostać zatwierdzone na piśmie przez funkcjonariusza policji w stopniu co najmniej inspektora, chyba że jest niezbędne dla prowadzenia postępowania przygotowawczego w sprawie przestępstwa. W takim przypadku funkcjonariusz w stopniu co najmniej inspektora musi zostać poinformowany o przeszukaniu najszybciej, jak to możliwe po jego przeprowadzeniu. Należy udokumentować przyczyny przeszukania i charakter poszukiwanych dowodów. Ponadto w art. 15 i 16 PACE 1984 przewidziano zabezpieczenia ustawowe, których należy przestrzegać przy składaniu wniosku o nakaz przeszukania. W art. 15 określono wymogi mające zastosowanie do uzyskania nakazu przeszukania (w tym treść wniosku składanego przez funkcjonariusza policji oraz fakt, że w nakazie należy wskazać m. in. przepis prawa stanowionego, na podstawie którego wydano nakaz, oraz określić, w miarę możliwości, przedmioty i osoby, które mają być obiektem poszukiwań, oraz pomieszczenia, które mają być przeszukane). Art. 16 reguluje sposób przeprowadzenia przeszukania na podstawie nakazu (na przykład: art. 16 ust. 5 stanowi, że funkcjonariusz wykonujący nakaz przekazuje osobie zajmującej pomieszczenia kopię nakazu; art. 16 ust. 11 zawiera wymóg przechowywania nakazu przez okres 12 miesięcy po jego wykonaniu; art. 16 ust. 12 zapewnia osobie zajmującej pomieszczenia prawo wglądu do nakazu w tym okresie na jej wniosek). Artykuły te pomagają zapewnić zgodność z art. 8 EKPC (zob. np. Kent Pharmaceuticals przeciwko Director of the Serious Fraud Office [2002] EWHC 3023 (QB) pkt [30], Lord Woolf CJ). Nieprzestrzeganie tych zabezpieczeń może skutkować uznaniem przeszukania za niezgodne z prawem (np. Korona (Brook) przeciwko Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; Korona (Superior Import/Export Ltd) przeciwko Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; oraz Korona (F) przeciwko Blackfriars Crown Court [2014] EWHC 1541 (Admin)). Art. 15 i 16 PACE 1984 uzupełniono kodeksem postępowania (Code B) PACE, który reguluje wykonywanie uprawnień policyjnych do przeszukiwania pomieszczeń.

([186]) Na przykład przy wydawaniu nakazu wydania dowodów na podstawie ustawy o dochodach z przestępstwa z 2002 r. oprócz konieczności posiadania uzasadnionych podstaw do spełnienia warunków określonych w art. 346 ust. 2 tej ustawy powinny istnieć uzasadnione podstawy do stwierdzenia, że dana osoba jest w posiadaniu określonego w ten sposób materiału lub sprawuje nad nim kontrolę oraz że materiał ten może mieć znaczną wartość. Ponadto inny wymóg dotyczący wydania nakazu wydania dowodów przewiduje, że muszą istnieć uzasadnione podstawy, by sądzić, że wydanie lub udostępnienie materiału leży w interesie publicznym, biorąc pod uwagę: a) prawdopodobną korzyść dla postępowania przygotowawczego oraz b) określone we wniosku okoliczności posiadania lub kontrolowania danych materiałów przez osobę, co do której domniemywa się, że posiada lub kontroluje te materiały. Podobnie, sąd rozpatrujący wniosek o wydanie nakazu wydania dowodów na podstawie załącznika 1 do PACE 1984 musi upewnić się, że spełniono określone warunki. W szczególności w załączniku 1 do PACE określono dwie odrębne alternatywne grupy warunków, z których jedna musi zostać spełniona, aby sędzia mógł wydać nakaz wydania dowodów. Zgodnie z pierwszą grupą warunków sędzia musi mieć uzasadnione podstawy, by sądzić, że (i) popełniono przestępstwo podlegającego oskarżeniu publicznemu; (ii) materiały poszukiwane w pomieszczeniach składają się z materiałów objętych specjalną procedurą, ale nie materiałów wyłączonych, lub zawierają takie materiały; (iii) mogą mieć znaczną wartość – w odosobnieniu lub wraz z innymi materiałami – dla postępowania przygotowawczego; (iv) oraz mogą być istotnymi dowodami; (v) próbowano zdobyć materiały innym sposobami lub nie podjęto takich prób, ponieważ nie miały szans zakończyć się powodzeniem; oraz (vi) po rozważeniu korzyści dla postępowania przygotowawczego oraz okoliczności dotyczące posiadania materiałów przez daną osobę stwierdzono, że wydanie materiałów lub uzyskanie dostępu do nich leży w interesie publicznym. Druga grupa warunków obejmuje następujące wymagania: (i) w pomieszczeniach znajdują się materiały, które składają się z materiałów objętych specjalną procedurą lub materiałów wyłączonych; (ii) nakaz przeszukania w celu zdobycia przedmiotowych materiałów zostałby wydany, gdyby nie zakaz przeszukiwania oparty na ustawodawstwie przyjętym przed PACE w odniesieniu do materiałów objętych specjalną procedurą, materiałów wyłączonych lub objętych prawniczą tajemnicą zawodową; oraz (iii) przeszukanie byłoby stosowne.

([187]) Kontrola sądowa to procedura prawna, w ramach której decyzje organu publicznego mogą być zaskarżone przed Wysokim Trybunałem. Sądy badają zaskarżoną decyzję i decydują, czy można twierdzić, że decyzja jest wadliwa pod względem prawnym, uwzględniając pojęcia i zasady prawa publicznego. Najważniejsze przesłanki do przeprowadzenia kontroli sądowej to: niezgodność z prawem, niezasadność, nieprawidłowość proceduralna, uzasadnione oczekiwania i prawa człowieka. Po pomyślnym zakończeniu kontroli sądowej sąd może zarządzić szereg różnych środków zaradczych; najczęstszym z nich jest orzeczenie o unieważnieniu (które uchyla lub unieważnia pierwotną decyzję – tj. decyzję o wydaniu nakazu przeszukania); w niektórych okolicznościach może to również obejmować przyznanie odszkodowania finansowego. Dodatkowe informacje na temat kontroli sądowej w Zjednoczonym Królestwie można znaleźć w publikacji rządowego departamentu prawnego „Judge Over Your Shoulder – a guide to good decision-making" [„Pod nadzorem sądów – poradnik właściwego podejmowania decyzji"], dostępnej pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

danych osobowych – co jest formą przetwarzania – wyłącznie zgodnie z zasadami i wymogami określonymi w DPA 2018 (zob. motywy 122 i 124). W związku z tym wniosek złożony przez jakikolwiek organ ścigania powinien być zgodny z zasadą, według której cele przetwarzania muszą być konkretne, wyraźne i prawnie uzasadnione ([188]), a dane osobowe przetwarzane przez właściwy organ muszą być stosowne oraz ograniczone do celu, w którym są przetwarzane ([189]).

3.2.1.2. Uprawnienia dochodzeniowo-śledcze do celów ścigania przestępstw

(139) W celu zapobiegania tylko poważnym przestępstwom lub ich wykrywania ([190]) niektórym organom ścigania, na przykład Krajowej Agencji ds. Zwalczania Przestępczości lub Komendantowi Głównemu Policji ([191]), przysługują ukierunkowane uprawnienia dochodzeniowo-śledcze na mocy IPA 2016. W takim przypadku zabezpieczenia przewidziane w IPA 2016 będą miały zastosowanie w uzupełnieniu zabezpieczeń przewidzianych w części 3 DPA 2018. Szczególne uprawnienia dochodzeniowe przysługujące wspomnianym organom ścigania to: ukierunkowane przechwytywanie (część 2 IPA 2016), ukierunkowane pozyskiwanie danych pochodzących z łączności (część 3 IPA 2016), ukierunkowane zatrzymywanie danych pochodzących z łączności (część 4 IPA 2016) oraz ukierunkowana ingerencja w urządzenia elektroniczne (część 5 IPA 2016). Przechwytywanie obejmuje pozyskanie treści wiadomości ([192]), natomiast pozyskiwanie i zatrzymywanie danych pochodzących z łączności nie ma na celu zdobycia treści wiadomości, ale ustalenie, kto, kiedy, gdzie i jak wysłał wiadomość. Obejmuje to na przykład czas i okres trwania połączenia, numery telefonu lub adresy e-mail nadawcy i odbiorcy wiadomości, a czasami lokalizację urządzeń, z których przesłano wiadomość, abonenta usługi telefonicznej lub szczegółowy rachunek ([193]). Ingerencja w urządzenia elektroniczne oznacza szereg technik stosowanych w celu uzyskania różnego rodzaju danych z urządzeń, w tym z komputerów, tabletów i smartfonów, a także kabli, przewodów i urządzeń pamięciowych ([194]).

(140) Z uprawnień do ukierunkowanego przechwytywania można również korzystać, gdy jest to „niezbędne do celów wykonania przepisów unijnego instrumentu wzajemnej pomocy lub międzynarodowej umowy o wzajemnej pomocy" (tzw. „nakaz w ramach wzajemnej pomocy" ([195])). Nakazy w ramach wzajemnej pomocy wydaje się wyłącznie w związku z przechwytywaniem, a nie pozyskiwaniem danych pochodzących z łączności lub ingerencji w urządzenia elektroniczne. Te ukierunkowane uprawnienia uregulowano ustawą o uprawnieniach dochodzeniowo-śledczych z 2016 r. (IPA 2016) ([196]), która wraz z ustawą regulującą uprawnienia dochodzeniowo-śledcze z 2000 r. (RIPA) w przypadku Anglii, Walii i Irlandii Północnej oraz ustawą regulującą uprawnienia dochodzeniowo-śledcze w Szkocji z 2000 r. (RIPSA), w przypadku Szkocji, zapewnia podstawę prawną i określa obowiązujące ograniczenia i zabezpieczenia dotyczące korzystania z takich uprawnień. W IPA 2016 przewidziano również system masowego korzystania z uprawnień dochodzeniowo-śledczych, chociaż nie jest on dostępny dla organów ścigania (mogą z niego korzystać wyłącznie agencje wywiadowcze) ([197]).

([188]) Art. 36 ust. 1 DPA 2018.
([189]) Art. 37 DPA 2018.
([190]) Art. 263 ust. 1 IPA 2016 stanowi, że „poważne przestępstwo" oznacza przestępstwo, w przypadku którego można racjonalnie oczekiwać, że osoba dorosła, która nie była wcześniej skazana, zostanie za nie skazana na karę pozbawienia wolności na okres 3 lat lub więcej lub czyn wiąże się z użyciem przemocy, powoduje znaczną korzyść finansową lub jest dokonywany przez znaczną liczbę osób. Ponadto – na potrzeby celów pozyskiwania danych pochodzących z łączności na podstawie części 4 IPA 2016 – art. 87 ust. 10B stanowi, że „poważne przestępstwo" oznacza przestępstwo, za które można wymierzyć karę pozbawienia wolności na okres 12 miesięcy lub więcej, lub przestępstwo popełnione przez osobę, która nie jest osobą fizyczną, lub które obejmuje, jako podstawowy element, wysyłanie wiadomości lub naruszenie prywatności osoby.
([191]) O wydanie nakazu ukierunkowanego przechwytywania mogą ubiegać się w szczególności następujące organy ścigania: Director General of the National Crime Agency (dyrektor generalny Krajowej Agencji ds. Zwalczania Przestępczości), Commissioner of Police of the Metropolis (komendant policji metropolitalnej), Chief Constable of the Police Service of Northern Ireland (szef policji Irlandii Północnej), Chief Constable of the Police Service of Scotland (szef szkockiej policji), Commissioner for Her Majesty's Revenue and Customs (organ podatkowy i celny Zjednoczonego Królestwa), Chief of Defence Intelligence (szef agencji wywiadu wojskowego) oraz podmiot będący właściwym organem państwa lub terytorium poza Zjednoczonym Królestwem do celów unijnego instrumentu wzajemnej pomocy lub międzynarodowej umowy o wzajemnej pomocy (art. 18 ust. 1 IPA 2016).
([192]) Zob. art. 4 IPA 2016.
([193]) Zob. art. 261 ust. 5 IPA 2016 oraz kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, pkt 2.9.
([194]) Kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, pkt 2.2.
([195]) Nakaz w ramach wzajemnej pomocy upoważnia organ Zjednoczonego Królestwa do udzielenia pomocy organowi spoza terytorium Zjednoczonego Królestwa w celu przechwycenia i ujawnienia przechwyconego materiału takiemu organowi, zgodnie z międzynarodowym instrumentem wzajemnej pomocy (art. 15 ust. 4 IPA 2016).
([196]) 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.
([197]) Art. 138 ust. 1, art. 158 ust. 1, art. 178 ust. 1, art. 199 ust. 1 IPA 2016.

(141) Aby skorzystać z tych uprawnień, organy muszą uzyskać nakaz ([198]) wydany przez właściwy organ ([199]) i zatwierdzony przez niezależnego komisarza sądowego ([200]) (tzw. procedura dwustopniowej autoryzacji nakazów). Uzyskanie takiego nakazu wymaga przeprowadzenia analizy niezbędności i proporcjonalności ([201]). Ponieważ te ukierunkowane uprawnienia dochodzeniowo-śledcze przewidziane w IPA 2016 są takie same jak uprawnienia, którymi dysponują agencje bezpieczeństwa narodowego, warunki, ograniczenia i zabezpieczenia mające zastosowanie do takich uprawnień zostały szczegółowo omówione w artykule dotyczącym uzyskiwania dostępu do danych osobowych i ich wykorzystywania przez organy publiczne Zjednoczonego Królestwa do celów bezpieczeństwa narodowego (zob. motyw 177 i następne).

3.2.2. *Dalsze wykorzystywanie zebranych informacji*

(142) Udostępnianie danych przez organ ścigania innemu organowi do celów innych niż te, dla których pierwotnie je zebrano (tzw. „dalsze przekazywanie"), podlega określonym warunkom.

(143) Podobnie do tego, co przewidziano w art. 4 ust. 2 dyrektywy (UE) 2016/680, art. 36 ust. 3 DPA 2018 dopuszcza aby dane osobowe zebrane przez właściwy organ do celów ścigania przestępstw były dalej przetwarzane (przez pierwotnego administratora lub innego administratora) do wszelkich innych celów ścigania przestępstw, pod warunkiem że administrator jest upoważniony na mocy prawa do przetwarzania danych w tym innym celu, a przetwarzanie jest niezbędne i proporcjonalne w odniesieniu tego celu ([202]). W takim przypadku wszystkie zabezpieczenia przewidziane w części 3 DPA 2018, o których mowa w motywach 122 i 124, mają zastosowanie do przetwarzania prowadzonego przez organ otrzymujący.

(144) W porządku prawnym Zjednoczonego Królestwa różne ustawy wyraźnie dopuszczają takie dalsze przekazywanie. W szczególności (i) ustawa o gospodarce cyfrowej z 2017 r. umożliwia udostępnianie danych między organami publicznymi do szeregu celów, na przykład w przypadku wszelkich nadużyć finansowych na szkodę sektora publicznego, które wiązałyby się ze stratą lub ryzykiem straty dla organów publicznych ([203]), lub w przypadku długu należnego na rzecz organu publicznego lub Korony ([204]); (ii) ustawa o przestępczości i sądach z 2013 r. zezwala na udostępnianie danych Krajowej Agencji ds. Zwalczania Przestępczości (NCA) ([205]) w celu zwalczania przestępczości poważnej i zorganizowanej, prowadzenia postępowań przygotowawczych w sprawie takich przestępstw i ich ścigania; (iii) ustawa o poważnej przestępczości z 2007 r. zezwala organom publicznym na ujawnianie informacji organizacjom zwalczającym nadużycia finansowe do celów zapobiegania nadużyciom finansowym ([206]).

(145) Ustawy te wyraźnie stanowią, że udostępnianie informacji musi być zgodne z zasadami określonymi w DPA 2018 Ponadto Kolegium Policyjne wydało zatwierdzone praktyki zawodowe dotyczące udostępniania informacji ([207]), aby pomóc policji w wypełnianiu obowiązków w zakresie ochrony danych

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

([199]) 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 urządzenia 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 urządzenia 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.

([200]) Komisarze sądowi wspierają Komisarza ds. Uprawnień Dochodzeniowo-Śledczych – niezależny organ, który sprawuje funkcje nadzorcze w kwestii wykorzystania uprawnień dochodzeniowo-śledczych przez agencje wywiadowcze (więcej informacji szczegółowych przedstawiono w motywie 162 i nast.).

([201]) Zob. w szczególności art. 19 i 23 IPA 2016.

([202]) Art. 36 ust. 3 DPA 2018.

([203]) Art. 56 ustawy o gospodarce cyfrowej z 2017 r., dostępnej pod adresem: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) Art. 48 ustawy o gospodarce cyfrowej z 2017 r.

([205]) Art. 7 ustawy o przestępczości i sądach z 2013 r., dostępnej pod adresem: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) Art. 68 ustawy o poważnej przestępczości z 2007 r., dostępnej pod adresem: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Zatwierdzone praktyki zawodowe dotyczące udostępniania informacji, dostępne pod adresem: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

wynikających z RODO UK, DPA oraz ustawy o prawach człowieka z 1998 r. Zgodność udostępniania informacji z obowiązującymi ramami prawnymi w zakresie ochrony danych podlega oczywiście kontroli sądowej ([208]).

(146) Ponadto podobnie do tego, co wynika z art. 9 dyrektywy (UE) 2016/680, DPA 2018 stanowi, że dane osobowe zebrane w jakimkolwiek celu związanym ze ściganiem przestępstw mogą być przetwarzane w celu, który nie jest celem związanym ze ściganiem przestępstw, jeżeli to przetwarzanie jest dozwolone przez prawo ([209]).

(147) Ten rodzaj udostępniania danych obejmuje dwa scenariusze: 1) gdy organ ścigania przekazuje dane organowi niebędącemu organem ścigania ani agencją wywiadowczą (np. organowi ds. regulacji finansowej, organowi podatkowemu, organowi ochrony konkurencji, urzędowi ds. młodzieży itp.) oraz 2) gdy organ ścigania przekazuje dane agencji wywiadowczej. W pierwszym scenariuszu przetwarzanie danych osobowych wchodzi w zakres RODO UK, jak również w zakres części 2 DPA 2018. Komisja oceniła zabezpieczenia przewidziane w RODO UK i części 2 DPA 2018 w motywach 12–111 i stwierdziła, że Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych zgodnie z zakresem stosowania rozporządzenia (UE) 2016/679 z Unii Europejskiej do Zjednoczonego Królestwa.

(148) W drugim scenariuszu, w odniesieniu do udostępniania danych zebranych przez organ ścigania agencji wywiadowczej do celów bezpieczeństwa narodowego, podstawą prawną upoważniającą do takiego udostępniania jest art. 19 ustawy o zwalczaniu terroryzmu z 2008 r. (CTA 2008) ([210]). Zgodnie z tą ustawą każdy może przekazać informacje którejkolwiek ze służb wywiadowczych na potrzeby wykonywania którejkolwiek z funkcji tej służby, w tym dotyczącej „bezpieczeństwa narodowego".

(149) Jeśli chodzi o warunki, na jakich dane można udostępniać do celów bezpieczeństwa narodowego, ustawa o służbach wywiadowczych ([211]) oraz ustawa o Służbie Bezpieczeństwa ([212]) ograniczają możliwości służb wywiadowczych w zakresie uzyskiwania danych do tego, co jest niezbędne do wykonywania ich funkcji ustawowych. Organy ścigania zamierzające udostępniać dane służbom wywiadowczym będą musiały uwzględnić szereg czynników/ograniczeń oprócz ustawowych funkcji agencji określonych w ustawie o służbach wywiadowczych i ustawie o Służbie Bezpieczeństwa ([213]). W art. 20 ustawy o zwalczaniu terroryzmu z 2008 r. wyraźnie wskazano, że wszelkie udostępnianie danych na podstawie art. 19 musi być również zgodne z ustawodawstwem w dziedzinie ochrony danych; oznacza to, że mają zastosowanie wszystkie ograniczenia i wymogi określone w części 3 DPA 2018. Ponadto ponieważ właściwe organy są organami publicznymi w rozumieniu ustawy o prawach człowieka z 1998 r., organy te muszą zagwarantować, że działają zgodnie z prawami określonymi w konwencji, w tym z art. 8 EKPC. Ograniczenia te służą temu, aby wszelkie udostępnianie danych między organami ścigania a służbami wywiadowczymi było zgodne z ustawodawstwem w dziedzinie ochrony danych i EKPC.

([208]) Zob. np. sprawa M, Korona przeciwko Chief Constable of Sussex Police [2019] EWHC 975 (Admin), w której zwrócono się do Wysokiego Trybunału o rozstrzygnięcie w kwestii udostępniania danych między policją a partnerstwem na rzecz ograniczenia przestępczości wymierzonej w przedsiębiorstwa (Business Crime Reduction Partnership – BCRP), organizacją upoważnioną do zarządzania programami zawiadomień o wykluczeniu, zabraniającymi osobom wstępu do lokali handlowych jej członków. Trybunał zbadał udostępnianie danych, które odbywało się na podstawie umowy mającej na celu ochronę społeczeństwa i zapobieganie przestępczości, i ostatecznie stwierdził, że większość aspektów udostępniania danych była zgodna z prawem, z wyjątkiem pewnych informacji szczególnie chronionych udostępnianych między policją a BCRP. Innym przykładem jest sprawa Cooper przeciwko NCA [2019] EWCA Civ 16, w której Sąd Apelacyjny potwierdził zgodność z prawem udostępniania danych między policją a Agencją ds. Poważnej Przestępczości Zorganizowanej (Serious Organised Crime Agency, SOCA), organem ścigania będącym obecnie częścią Krajowej Agencji ds. Zwalczania Przestępczości (NCA).

([209]) Art. 36 ust. 4 DPA 2018.

([210]) Ustawa o zwalczaniu terroryzmu z 2008 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) Ustawa o służbach wywiadowczych z 1994 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) Ustawa o Służbie Bezpieczeństwa z 1989 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) Art. 2 ust. 2 ustawy o służbach wywiadowczych z 1994 r. stanowi, że „Dyrektor służby wywiadowczej jest odpowiedzialny za skuteczne działanie tej służby i jego obowiązkiem jest zapewnienie, aby: a) wprowadzono rozwiązania służące zagwarantowaniu, aby służba wywiadowcza nie uzyskiwała żadnych informacji z wyjątkiem koniecznych do właściwego wykonywania jej funkcji oraz aby nie ujawniano żadnych informacji, o ile nie jest to niezbędne – (i) do tego celu; (ii) w interesie bezpieczeństwa narodowego; (iii) do celów zapobiegania poważnym przestępstwom lub ich wykrywania lub (iv) do celów jakichkolwiek postępowań karnych oraz b) służba wywiadowcza nie podejmowała żadnych działań na rzecz interesów jakiejkolwiek partii politycznej Zjednoczonego Królestwa"; natomiast art. 2 ust. 2 ustawy o Służbie Bezpieczeństwa z 1989 r. stanowi, że „Dyrektor generalny jest odpowiedzialny za skuteczne działanie Służby i jego obowiązkiem jest zapewnienie, aby: a) wprowadzono rozwiązania służące zagwarantowaniu, aby Służba nie uzyskiwała żadnych informacji z wyjątkiem koniecznych do właściwego wykonywania jej funkcji oraz aby nie ujawniano żadnych informacji, o ile nie jest to niezbędne do tego celu lub do celów zapobiegania poważnej przestępczości lub wykrywania jej lub do celów jakichkolwiek postępowań karnych; oraz b) Służba nie podejmowała żadnych działań na rzecz interesów jakiejkolwiek partii politycznej i c) wprowadzono rozwiązania, uzgodnione z Dyrektorem Generalnym Krajowej Agencji ds. Zwalczania Przestępczości, mające na celu koordynację działań Służby prowadzonych na podstawie art. 1 ust. 4 ustawy z działaniami sił policyjnych, Krajowej Agencji ds. Zwalczania Przestępczości i innych organów ścigania".

(150) Gdy właściwy organ zamierza udostępnić dane osobowe przetwarzane na podstawie części 3 DPA 2018 organom ścigania państwa trzeciego, zastosowanie mają szczególne wymagania ([214]). Mianowicie takie przekazywanie może mieć miejsce, gdy odbywa się na podstawie rozporządzeń stwierdzających odpowiedni stopień ochrony wydanych przez Sekretarza Stanu lub, w przypadku braku takich rozporządzeń, pod warunkiem zapewnienia odpowiednich zabezpieczeń. Art. 75 DPA 2018 stanowi, że odpowiednie zabezpieczenia istnieją, gdy ustanowiono je aktem prawnym, który jest wiążący dla zamierzonego odbiorcy, lub gdy administrator, po dokonaniu oceny wszystkich okoliczności związanych z przekazywaniem tego rodzaju danych osobowych do państwa trzeciego lub organizacji międzynarodowej, stwierdza, że istnieją odpowiednie zabezpieczenia służące ochronie danych.

(151) Jeżeli przekazanie nie opiera się na rozporządzeniu stwierdzającym odpowiedni stopień ochrony ani na odpowiednich zabezpieczeniach, może nastąpić wyłącznie w niektórych, określonych okolicznościach, zwanych „szczególnymi okolicznościami" ([215]). Dotyczy to sytuacji, w których przekazanie jest niezbędne: a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby; b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą; c) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego; d) w indywidualnym przypadku do celów ścigania przestępstw; lub e) w indywidualnym przypadku do celów prawnych (np. w związku z postępowaniem sądowym lub w celu uzyskania porady prawnej). Należy zauważyć, że lit. d) i e) nie mają zastosowania, jeżeli podstawowe prawa i wolności osoby, której dane dotyczą, są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem. Ten zbiór okoliczności odpowiada szczególnym sytuacjom i warunkom kwalifikującym się jako „wyjątki" na podstawie art. 38 dyrektywy (UE) 2016/680.

(152) Ponadto w IPA 2016 nałożono dodatkowe zabezpieczenia w sytuacji, w której materiały uzyskane przez organy ścigania na podstawie nakazu upoważniającego do przechwytywania lub ingerencji w urządzenia elektroniczne są przekazywane do państwa trzeciego. W szczególności takie ujawnienie, określone jako „ujawnienie za granicą", jest dozwolone tylko wtedy, gdy organ wydający stwierdzi, że istnieją specjalne odpowiednie rozwiązania ograniczające liczbę osób, którym ujawnia się dane, oraz zakres ujawniania, udostępniania lub kopiowania wszelkich materiałów i liczbę wykonanych kopii. Ponadto organ wydający może stwierdzić, że konieczne są odpowiednie rozwiązania służące zapewnieniu, aby wszelkie kopie jakichkolwiek części tych materiałów zostały zniszczone, gdy tylko przestaną istnieć uzasadnione powody do ich zachowania (o ile nie zostaną zniszczone wcześniej) ([216]).

(153) Ponadto szczególne formy dalszego przekazywania danych ze Zjednoczonego Królestwa do Stanów Zjednoczonych mogą w przyszłości odbywać się na podstawie „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" („umowa między Zjednoczonym Królestwem a USA" lub „umowa") ([217]) zawartej w październiku 2019 r. ([218]) Chociaż umowa między Zjednoczonym Królestwem a USA nie weszła jeszcze w życie w momencie przyjmowania niniejszej decyzji, jej spodziewane wejście w życie może mieć wpływ na dalsze przekazywanie do USA danych przekazanych wcześniej do Zjednoczonego Królestwa na podstawie decyzji. Dokładniej rzecz ujmując, dane przekazywane z UE do dostawców usług w Zjednoczonym Królestwie mogą podlegać nakazom wydania elektronicznego materiału dowodowego wydanym przez właściwe organy ścigania USA i stosowanym w Zjednoczonym Królestwie na podstawie wspomnianej umowy po jej wejściu w życie. W związku z tym ocena warunków i zabezpieczeń, na jakich takie nakazy mogą być wydawane i wykonywane, jest istotna dla niniejszej decyzji.

([214]) Zob. część 3 rozdział 5 DPA 2018.

([215]) Art. 76 DPA 2018.

([216]) Art. 54 i 130 IPA 2016. Organy wydające muszą rozważyć potrzebę nałożenia szczególnych zabezpieczeń w odniesieniu do materiałów przekazywanych organom zagranicznym, aby zapewnić poddanie danych zabezpieczeniom w zakresie ich zatrzymywania, niszczenia i ujawniania podobnym do zabezpieczeń nałożonych w art. 53 i 129 IPA 2016.

([217]) 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_Countering_Serious_Crime.pdf.

([218]) Jest to pierwsza umowa zawarta na podstawie amerykańskiej ustawy CLOUD (określającej legalne wykorzystanie danych za granicą). Ustawa CLOUD to ustawa federalna USA, którą przyjęto w dniu 23 marca 2018 r. i w której określono, w drodze zmiany ustawy z 1986 r. o przechowywanych danych przekazywanych za pomocą łączności elektronicznej, że amerykańscy dostawcy usług mają obowiązek przestrzegania amerykańskich nakazów ujawnienia danych dotyczących treści i danych niedotyczących treści niezależnie od miejsca przechowywania takich danych. Ustawa CLOUD umożliwia również zawieranie porozumień władzy wykonawczej (*executive agreements*) z rządami zagranicznymi, na podstawie których amerykańscy dostawcy usług mogą dostarczać dane dotyczące treści bezpośrednio do tych rządów zagranicznych (tekst ustawy CLOUD jest dostępny pod adresem: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) W tym zakresie należy zauważyć, że, po pierwsze, jeśli chodzi o zakres przedmiotowy umowy, ma ona zastosowanie wyłącznie do przestępstw, które podlegają karze pozbawienia wolności o maksymalnym wymiarze co najmniej trzech lat (określanych jako „poważne przestępstwa") ([219]), w tym „działalności terrorystycznej". Po drugie, dane przetwarzane w jurysdykcji drugiej strony można uzyskać na podstawie tej umowy wyłącznie w następstwie „nakazu [...] podlegającego kontroli lub nadzorowi na mocy prawa krajowego strony wydającej przez sąd, sędziego lub inny niezależny organ przed postępowaniem lub w trakcie postępowania dotyczącego wykonania nakazu" ([220]). Po trzecie, wszelkie nakazy muszą „spełniać wymogi dotyczące racjonalnego uzasadnienia opartego na jasnych i wiarygodnych faktach, szczegółowości, zgodności z prawem i powagi działań będących przedmiotem postępowania przygotowawczego" ([221]) oraz „dotyczyć określonych kont, jak również wskazywać określoną osobę, konto, adres, urządzenie osobiste lub jakikolwiek inny określony identyfikator" ([222]). Po czwarte, dane uzyskane na podstawie tej umowy są objęte ochroną równoważną względem szczególnych zabezpieczeń przewidzianych w tzw. „umowie ramowej między UE a USA" ([223]) – kompleksowej umowie o ochronie danych zawartej w grudniu 2016 r. przez UE i USA, w której określono zabezpieczenia i prawa mające zastosowanie do przekazywania danych w ramach współpracy dotyczącej ścigania przestępstw – i które w całości włączono do przedmiotowej umowy przez odniesienie na zasadzie *mutatis mutandis*, przede wszystkim aby uwzględnić szczególny charakter przekazywania danych (tj. przekazywanie danych od operatorów prywatnych do organów ścigania, a nie przekazywanie danych między organami ścigania) ([224]). Umowa między Zjednoczonym Królestwem a USA wyraźnie stanowi, że ochrona równoważna ochronie zapewnianej przez umowę ramową między UE a USA będzie miała zastosowanie „do wszystkich danych osobowych wydanych w trakcie wykonywania nakazów podlegających umowie w celu zapewnienia równoważnej ochrony" ([225]).

(155) Dane przekazywane organom USA na podstawie umowy między Zjednoczonym Królestwem a USA powinny zatem być objęte ochroną zapewnianą instrumentem prawa Unii, zawierającym niezbędne dostosowania odzwierciedlające charakter takiego przekazywania. Władze Zjednoczonego Królestwa potwierdziły ponadto, że ochrona przewidziana w umowie ramowej będzie miała zastosowanie do wszystkich danych osobowych wydawanych lub przechowywanych na podstawie umowy, niezależnie od charakteru lub rodzaju organu występującego z wnioskiem (np. zarówno federalne, jak i stanowe amerykańskie organy ścigania), tak więc równoważną ochronę należy zapewnić we wszystkich przypadkach. Władze Zjednoczonego Królestwa wyjaśniły jednak również, że nadal trwają rozmowy między Zjednoczonym Królestwem a USA w sprawie szczegółowych ustaleń dotyczących konkretnego wdrożenia zabezpieczeń służących ochronie danych. W kontekście rozmów ze służbami Komisji Europejskiej na temat niniejszej decyzji władze Zjednoczonego Królestwa potwierdziły, że dopuszczą do wejścia umowy w życie dopiero wtedy, gdy będą miały pewność, że zostanie wdrożona zgodnie z przewidzianymi w niej zobowiązaniami prawnymi, w tym w kwestii jasności co do zgodności z normami ochrony danych w przypadku wszelkich danych, o które wystąpiono na podstawie wspomnianej umowy. Ponieważ ewentualne wejście w życie umowy może mieć wpływ na stopień ochrony oceniany w niniejszej decyzji, Zjednoczone Królestwo powinno przekazywać Komisji Europejskiej wszelkie informacje i przyszłe wyjaśnienia na temat sposobu, w jaki USA będzie wypełniać swoje zobowiązania wynikające z umowy, gdy tylko staną się dostępne, a w każdym razie przed wejściem w życie umowy, aby zapewnić właściwe monitorowanie niniejszej decyzji zgodnie z art. 45 ust. 4 rozporządzenia (UE) 2016/679. Szczególna uwaga zostanie poświęcona stosowaniu i dostosowaniu zabezpieczeń umowy ramowej do szczególnego rodzaju przekazywania danych objętego umową między Zjednoczonym Królestwem a USA.

(156) Mówiąc bardziej ogólnie, wszelkie istotne zmiany dotyczące wejścia w życie i stosowania umowy zostaną należycie uwzględnione w kontekście stałego monitorowania niniejszej decyzji, w tym w odniesieniu do niezbędnych konsekwencji, które będzie należało wyciągnąć w przypadku jakichkolwiek przesłanek wskazujących, że zasadniczo odpowiadający stopień ochrony nie jest już zapewniany.

3.2.3. *Nadzór*

(157) W zależności od uprawnień wykonywanych przez właściwe organy przy przetwarzaniu danych osobowych do celów ścigania przestępstw (czy to na mocy DPA 2018, czy IPA 2016) nadzór nad wykonaniem tych uprawnień zapewniają różne organy. Gdy przetwarzanie danych osobowych wchodzi w zakres części 3 DPA 2018, nadzoruje

([219]) Art. 1 ust. 14 umowy.
([220]) Art. 5 ust. 2 umowy.
([221]) Art. 5 ust. 1 umowy.
([222]) Art. 4 ust. 5 umowy. W przypadku przechwytywania w czasie rzeczywistym obowiązuje dodatkowy i bardziej rygorystyczny standard: nakazy muszą być wydawane na czas określony, który nie może być dłuższy niż czas z racjonalnego punktu widzenia konieczny do osiągnięcia celów nakazu, i muszą być wydawane wyłącznie w przypadku, gdy tych samych informacji nie można w racjonalny sposób uzyskać za pomocą mniej inwazyjnej metody (art. 5 ust. 3 umowy).
([223]) Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych, Dz.U. L 336 z 10.12.2016, s. 3, dostępna pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.
([224]) Art. 9 ust. 1 umowy.
([225]) Art. 9 ust. 1 umowy.

je Komisarz ds. Informacji ([226]). Niezależny i sądowy nadzór nad korzystaniem z uprawnień dochodzeniowo-śledczych na podstawie IPA 2016 zapewnia biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych ([227]) (do tej kwestii odniesiono się w motywach 250–255). Ponadto dodatkowy nadzór gwarantuje parlament oraz inne organy.

3.2.3.1. Nadzór na podstawie części 3 DPA 2018

(158) Ogólne funkcje Komisarza ds. Informacji – którego niezależność i organizację omówiono w motywie 87 – w odniesieniu do przetwarzania danych osobowych wchodzącego w zakres części 3 DPA 2018 określono w załączniku 13 do DPA 2018. Głównym zadaniem Komisarza ds. Informacji jest monitorowanie i egzekwowanie części 3 DPA 2018, jak również zwiększanie świadomości społecznej, doradzanie parlamentowi, rządowi oraz innym instytucjom i organom. Aby utrzymać niezależność sądów, Komisarz ds. Informacji nie jest uprawniony do wykonywania swoich funkcji w odniesieniu do przetwarzania danych osobowych przez osobę fizyczną sprawującą wymiar sprawiedliwości bądź sąd lub trybunał sprawujący wymiar sprawiedliwości. W takich okolicznościach funkcje nadzorcze wykonują inne organy, jak wyjaśniono w motywach 99–103.

(159) Komisarz posiada ogólne uprawnienia dochodzeniowo-śledcze, uprawnienia w zakresie korekt, upoważnień i uprawnienia doradcze w odniesieniu do przetwarzania danych osobowych, do których zastosowanie ma część 3. W szczególności Komisarz posiada uprawnienia do zawiadomienia administratora lub podmiotu przetwarzającego o domniemanym naruszeniu przepisów części 3 DPA 2018, do udzielania ostrzeżeń lub upomnień administratorowi lub podmiotowi przetwarzającemu, który naruszył przepisy części 3 ustawy, a także do wydawania z własnej inicjatywy lub na wniosek opinii dla parlamentu, rządu lub innych instytucji i organów, a także obywateli w sprawie dowolnej kwestii związanej z ochroną danych osobowych ([228]).

(160) Ponadto Komisarz posiada uprawnienia do wydawania zawiadomień informacyjnych ([229]), zawiadomień oceniających ([230]) i zawiadomień egzekucyjnych ([231]), a także uprawnienia do uzyskania dostępu do dokumentów administratorów i podmiotów przetwarzających, dostępu do ich pomieszczeń ([232]) oraz nakładania administracyjnych kar pieniężnych w formie zawiadomień w sprawie sankcji ([233]). W polityce działań regulacyjnych Komisarza ds. Informacji określono okoliczności, w których wydaje on, odpowiednio, zawiadomienia informacyjne, oceniające, egzekucyjne i zawiadomienia w sprawie sankcji ([234]) (zob. również motyw 93 oraz motywy 101–102 decyzji stwierdzającej odpowiedni stopień ochrony na podstawie dyrektywy (UE) 2016/680.

(161) Zgodnie z ostatnimi sprawozdaniami rocznymi (2018–2019 ([235]), 2019–2020 ([236])) Komisarz ds. Informacji przeprowadził szereg postępowań i zastosował środki egzekucyjne w odniesieniu do przetwarzania danych przez organy ścigania. Na przykład w październiku 2019 r. Komisarz przeprowadził postępowanie i wydał opinię w sprawie wykorzystywania przez organy ścigania technologii rozpoznawania twarzy w miejscach publicznych. W postępowaniu skupiono się w szczególności na wykorzystywaniu przez policję południowej Walii i Metropolitalną Służbę Policyjną możliwości w zakresie rozpoznawania twarzy na żywo. Komisarz ds. Informacji zbadał również stosowaną przez Metropolitalną Służbę Policyjną „matrycę gangów" ([237]) i stwierdził szereg poważnych naruszeń przepisów o ochronie danych, które mogły podważyć zaufanie publiczne w kwestii stosowania matrycy i sposobu wykorzystywania danych. W listopadzie 2018 r. Komisarz ds. Informacji wydał zawiadomienie egzekucyjne, w następstwie którego Metropolitalna Służba Policyjna podjęła kroki wymagane do zwiększenia bezpieczeństwa i rozliczalności oraz zapewnienia wykorzystywania danych w sposób proporcjonalny. Innym przykładem działań egzekucyjnych w tym obszarze jest grzywna w wysokości

([226]) Art. 116 DPA 2018.
([227]) Zob. IPA 2016, a w szczególności część 8 rozdział 1.
([228]) Pkt 2 załącznika 13 do DPA 2018.
([229]) Nakazanie administratorowi i podmiotowi przetwarzającemu (a w określonych okolicznościach każdej innej osobie) dostarczenia niezbędnych informacji (art. 142 DPA 2018).
([230]) Umożliwienie prowadzenia postępowań przygotowawczych i audytu, na mocy którego administrator lub podmiot przetwarzający może być zobowiązany do zezwolenia Komisarzowi na wejście do określonych pomieszczeń, przeprowadzenie inspekcji lub analizy dokumentów lub sprzętu, przesłuchanie osób przetwarzających dane osobowe w imieniu administratora (art. 146 DPA 2018).
([231]) Umożliwiające wykonanie uprawnień naprawczych, które wymagają od administratorów/podmiotów przetwarzających podjęcia lub powstrzymania się od podjęcia określonych kroków (art. 149 DPA 2018).
([232]) Art. 154 DPA 2018.
([233]) Art. 155 DPA 2018.
([234]) Polityka działań regulacyjnych, zob. przypis 96.
([235]) Sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2018–2019, zob. przypis 101.
([236]) Sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2019–2020, zob. przypis 82.
([237]) Baza danych, w której zapisywano dane wywiadowcze dotyczące domniemanych członków gangów i poszkodowanych w przestępstwach związanych z gangami.

325 000 GBP, którą Komisarz nałożył w maju 2018 r. na prokuraturę za utracenie niezaszyfrowanych płyt DVD zawierających nagrania z przesłuchań policyjnych. Komisarz ds. Informacji prowadził również postępowania dotyczące szerszych zagadnień, na przykład w pierwszej połowie 2020 r. w sprawie wydobywania danych z telefonów komórkowych do celów policyjnych oraz przetwarzania przez policję danych osób poszkodowanych. Ponadto Komisarz bada obecnie sprawę, która dotyczy dostępu organów ścigania do danych będących w posiadaniu podmiotu sektora prywatnego, Clearview AI Inc. ([238])

(162) Oprócz wymienionych w motywach 160 i 161 uprawnień Komisarza ds. Informacji do egzekwowania przestrzegania przepisów niektóre naruszenia ustawodawstwa w dziedzinie ochrony danych stanowią przestępstwo i mogą tym samym podlegać sankcjom karnym (art. 196 DPA 2018). Dotyczy to na przykład uzyskania, ujawnienia lub zatrzymania danych osobowych bez zgody administratora oraz doprowadzenia do ujawnienia danych osobowych innej osobie bez zgody administratora ([239]); deanonimizacji informacji będących zanonimizowanymi danymi osobowymi bez zgody administratora odpowiedzialnego za anonimizację danych osobowych ([240]); umyślnego utrudniania Komisarzowi wykonywania jego uprawnień w zakresie kontroli danych osobowych zgodnie z zobowiązaniami międzynarodowymi ([241]), składania fałszywych oświadczeń w odpowiedzi na zawiadomienie informacyjne lub niszczenia informacji w związku z zawiadomieniem informacyjnym i oceniającym ([242]).

3.2.3.2. Inne organy nadzoru w obszarze ścigania przestępstw

(163) Oprócz Komisarza ds. Informacji istnieje szereg organów nadzorczych w obszarze ścigania przestępstw, które posiadają szczególne uprawnienia związane z kwestiami dotyczącymi ochrony danych. Są to m.in. Komisarz ds. Zatrzymywania i Wykorzystywania Materiału Biometrycznego (Komisarz ds. Biometrii) ([243]) oraz Komisarz ds. Kamer Nadzorujących ([244]).

3.2.3.3. Nadzór parlamentarny w obszarze ścigania przestępstw

(164) Komisja Specjalna do Spraw Wewnętrznych (Home Affairs Select Committee, HASC) zapewnia nadzór parlamentarny w obszarze ścigania przestępstw. Komisja składa się z 11 członków parlamentu wybranych z trzech największych partii politycznych. Zadaniem komisji jest badanie wydatków, administracji i polityki Home Office oraz powiązanych z nim organów publicznych, tj. m.in. policji i Krajowej Agencji ds. Zwalczania Przestępczości, których pracę komisja może kontrolować w szczególności ([245]).

([238]) Zob. oświadczenie Komisarza ds. Informacji, dostępne pod adresem: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

([239]) Art. 170 DPA 2018.

([240]) Art. 171 DPA 2018.

([241]) Art. 119 ust. 6 DPA 2018.

([242]) W roku budżetowym obejmującym okres od dnia 1 kwietnia 2019 r. do dnia 31 marca 2020 r. dochodzenia Komisarza ds. Informacji zakończyły się czterema ostrzeżeniami i ośmioma oskarżeniami. Sprawy te wszczęto na podstawie art. 55 ustawy o ochronie danych z 1998 r., art. 77 ustawy o swobodnym dostępie do informacji z 2000 r. oraz art. 170 ustawy o ochronie danych z 2018 r. W 75 % przypadków oskarżeni przyznali się do winy, dzięki czemu nie było potrzeby prowadzenia długotrwałych procesów sądowych i ponoszenia związanych z nimi kosztów. (Sprawozdanie roczne i sprawozdanie finansowe Komisarza ds. Informacji za okres 2019–2020, zob. przypis 87, s. 40).

([243]) Urząd Komisarza ds. Biometrii powołano na podstawie ustawy o ochronie wolności z 2012 r. (PoFA) (zob.: https://www.legislation.gov.uk/ukpga/2012/9/contents). Komisarz ds. Biometrii decyduje między innymi o tym, czy policja może zatrzymywać zapisy profili DNA i odcisków palców pozyskanych od osób aresztowanych, ale nie oskarżonych o popełnienie przestępstwa kwalifikowanego (art. 63G ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.). Ponadto Komisarz ds. Biometrii ma ogólny obowiązek dokonywania przeglądu zatrzymywania i wykorzystywania DNA i odcisków palców oraz zatrzymywania danych ze względów bezpieczeństwa narodowego (art. 20 ust. 2 ustawy o ochronie wolności z 2012 r.). Komisarz ds. Biometrii jest powoływany zgodnie z kodeksem w zakresie nominacji publicznych (kodeks jest dostępny pod następującym adresem: https://www.gov.uk/government/publications/governance-code-for-public-appointments), a w warunkach jego powołania jasno wskazano, że może on zostać odwołany ze stanowiska przez Home Secretary (ministra spraw wewnętrznych) jedynie w ściśle określonych okolicznościach; obejmują one niewypełnianie obowiązków przez okres trzech miesięcy, skazanie za przestępstwo lub nieprzestrzeganie warunków powołania.

([244]) Urząd Komisarza ds. Kamer Nadzorujących powołano na podstawie ustawy o ochronie wolności z 2012 r. i jego rola polega na zachęcaniu do działania zgodnie z kodeksem postępowania dotyczącego kamer nadzorujących; sprawdzaniu funkcjonowania tego kodeksu oraz doradzaniu ministrom w sprawie ewentualnych zmian kodeksu. Komisarza powołuje się zgodnie z tymi samymi zasadami co komisarzy ds. biometrii i przysługują mu podobne uprawnienia, zasoby i ochrona przed odwołaniem.

([245]) Zob. https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/.

(165) Komisja może, w granicach swoich kompetencji, wybrać własny przedmiot dochodzenia, w tym konkretne przypadki, o ile dana sprawa nie jest rozpatrywana przez sąd. Komisja może również zwracać się do szerokiego grona odpowiednich grup i osób fizycznych o przedstawienie dowodów w formie pisemnej i ustnej. Komisja sporządza sprawozdania w sprawie swoich ustaleń i wydaje zalecenia dla rządu ([246]). Rząd powinien odpowiedzieć na każde z zaleceń zawartych w sprawozdaniu i musi odpowiedzieć w ciągu 60 dni ([247]).

(166) Jeżeli chodzi o niejawny nadzór, Komisja sporządziła również sprawozdanie dotyczące ustawy regulującej uprawnienia dochodzeniowo-śledcze z 2000 r. (RIPA 2000) ([248]), w którym stwierdzono, że RIPA 2000 jest nieadekwatna. Sprawozdanie to uwzględniono podczas zastępowania istotnych części ustawy RIPA 2000 ustawą IPA 2016. Pełna lista dochodzeń znajduje się na stronie internetowej komisji ([249]).

(167) Zadania Komisji Specjalnej do Spraw Wewnętrznych są wykonywane w Szkocji przez Podkomisję Sprawiedliwości ds. Działań Policyjnych (Justice Subcommittee on Policing), a w Irlandii Północnej przez Komisję Sprawiedliwości (Committee for Justice) ([250]).

3.2.4. *Środki zaskarżenia*

(168) Jeśli chodzi o przetwarzanie danych przez organy ścigania, mechanizmy regulujące środki zaskarżenia określono w części 3 DPA 2018 oraz w IPA 2016, a także w ustawie o prawach człowieka z 1998 r.

(169) Ten zbiór mechanizmów zapewnia osobom, których dane dotyczą, skuteczne administracyjne i sądowe środki zaskarżenia, dzięki czemu mogą dochodzić swoich praw, w tym prawa do uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania lub usunięcia takich danych.

(170) Po pierwsze, zgodnie z art. 165 DPA 2018 osoba, której dane dotyczą, ma prawo do wniesienia skargi do Komisarza ds. Informacji, jeżeli uważa, że doszło do naruszenia części 3 DPA 2018 w odniesieniu do danych osobowych, które jej dotyczą ([251]). Komisarz ds. Informacji jest uprawniony do oceny przestrzegania DPA 2018 przez administratora i podmiot przetwarzający, wezwania ich do poczynienia koniecznych kroków w przypadku nieprzestrzegania przepisów oraz nakładania grzywien.

([246]) Komisje specjalne, w tym Komisja Specjalna do Spraw Wewnętrznych, podlegają regulaminowi Izby Gmin. Regulamin to uzgodnione przez Izbę Gmin zasady regulujące funkcjonowanie parlamentu. Zakres kompetencji komisji specjalnych jest szeroki, a pkt 152 ppkt 1 regulaminu stanowi, że „Komisje specjalne są powoływane w celu zbadania wydatków, administracji i polityki głównych departamentów rządowych określonych w ppkt 2 niniejszego punktu oraz związanych z nimi organów publicznych". Dzięki temu Komisja Specjalna do Spraw Wewnętrznych może zbadać każdą politykę, za którą odpowiada Home Office, co obejmuje politykę (i związane z nią prawodawstwo) w zakresie uprawnień dochodzeniowo-śledczych. Ponadto w pkt 152 ppkt 4 regulaminu wyraźnie stwierdzono, że komisje mają różne uprawnienia, w tym możliwość wzywania osób do przedstawienia dowodów lub dokumentów w danej sprawie oraz sporządzania sprawozdań. Bieżące i poprzednie zapytania komisji są dostępne pod adresem https://committees.parliament.uk/committee/83/home-affairs-committee/

([247]) Uprawnienia Komisji Specjalnej do Spraw Wewnętrznych Anglii i Walii są określone w regulaminie Izby Gmin, dostępnym pod adresem: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Dostępna pod adresem: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Dostępna pod adresem: https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Zasady działania szkockiej Podkomisji Sprawiedliwości ds. Działań Policyjnych są dostępne pod adresem https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, a zasady dotyczące Komisji Sprawiedliwości Irlandii Północnej przedstawiono pod adresem: http://www.niassembly.gov.uk/assembly-business/standing-orders/].

([251]) Najnowsze sprawozdanie roczne Komisarza ds. Informacji zawiera zestawienie otrzymanych i zamkniętych skarg w podziale na ich charakter. Liczba otrzymanych skarg dotyczących „czynności policyjnych i rejestrów karnych" wynosi 6 % całkowitej liczby otrzymanych skarg (przy wzroście o 1 % w porównaniu z poprzednim rokiem budżetowym). Ze sprawozdania rocznego wynika również, że skargi dotyczące wniosków o dostęp od osób, których dane dotyczą, stanowią największą liczbę (46 % w stosunku do całkowitej liczby skarg, przy wzroście o 8 % w porównaniu z poprzednim rokiem budżetowym) (sprawozdanie roczne Komisarza ds. Informacji 2019–2020, s. 55; zob. przypis 88).

(171) Po drugie DPA 2018 przewiduje prawo do środka ochrony prawnej przeciwko Komisarzowi ds. Informacji, jeżeli nie rozpatrzy on odpowiednio skargi złożonej przez osobę, której dane dotyczą. Mówiąc ściślej, jeżeli Komisarz nie „poczyni postępów" ([252]) w rozpatrywaniu skargi złożonej przez osobę, której dane dotyczą, skarżący ma dostęp do środka ochrony prawnej przed sądem – może zwrócić się do trybunału pierwszej instancji ([253]) o nakazanie Komisarzowi podjęcia odpowiednich kroków w celu udzielenia odpowiedzi na skargę lub poinformowania skarżącego o postępach w rozpatrywaniu skargi ([254]). Ponadto każda osoba, wobec której Komisarz wydał którekolwiek ze wspomnianych zawiadomień (zawiadomienie informacyjne, oceniające, egzekucyjne lub w sprawie sankcji), może odwołać się do Trybunału Pierwszej Instancji (First Tier Tribunal). Jeżeli Trybunał uzna, że decyzja Komisarza ds. Informacji nie jest zgodna z prawem lub że Komisarz powinien był skorzystać z przysługującej mu swobody uznania w inny sposób, Trybunał uwzględnia odwołanie lub zastępuje zawiadomienie lub decyzję innym zawiadomieniem lub decyzją, które Komisarz mógł wydać ([255]).

(172) Po trzecie osoby fizyczne mogą wnieść środki zaskarżenia przeciwko administratorom i podmiotom przetwarzającym bezpośrednio do sądu. W szczególności, zgodnie z art. 167 DPA 2018, osoba, której dane dotyczą, może złożyć wniosek do sądu w sprawie naruszenia jej prawa wynikającego z ustawodawstwa w dziedzinie ochrony danych, a sąd może w drodze nakazu zażądać od administratora podjęcia (lub powstrzymania się od podjęcia) wszelkich kroków w odniesieniu do przetwarzania w celu zapewnienia zgodności z DPA 2018. Ponadto, zgodnie z art. 169 DPA 2018, każda osoba, która poniosła szkodę z powodu naruszenia wymogu określonego w ustawodawstwie w dziedzinie ochrony danych (w tym w części 3 DPA 2018), innym niż RODO UK, jest uprawniona do odszkodowania z tytułu tej szkody od administratora lub podmiotu przetwarzającego, z wyjątkiem sytuacji, gdy administrator lub podmiot przetwarzający udowodni, że nie jest w żaden sposób odpowiedzialny za zdarzenie powodujące szkodę. Szkoda obejmuje zarówno stratę finansową, jak i szkodę niezwiązaną ze stratą finansową, taką jak cierpienie.

(173) Każda osoba, która uważa, że jej prawa, w tym prawa do prywatności i ochrony danych, zostały naruszone przez dowolne organy publiczne, może wreszcie dochodzić roszczeń przed sądami Zjednoczonego Królestwa na podstawie ustawy o prawach człowieka z 1998 r. ([256]), a po wyczerpaniu krajowych środków ochrony prawnej osobie fizycznej, organizacji pozarządowej i grupie osób przysługuje środek zaskarżenia przed Europejskim Trybunałem Praw Człowieka z tytułu naruszeń praw gwarantowanych w Konwencji o ochronie praw człowieka i podstawowych wolności ([257]) (zob. motyw 111).

#### 3.2.4.1. Mechanizmy zaskarżenia dostępne na mocy IPA 2016

(174) Osobom fizycznym przysługują środki zaskarżenia z tytułu naruszenia IPA 2016 przed Trybunałem ds. Uprawnień Dochodzeniowo-Śledczych (Investigatory Powers Tribunal). Możliwe środki zaskarżenia dostępne na podstawie IPA 2016 opisano w motywach 263–269 poniżej.

---

([252]) Art. 166 DPA 2018 odnosi się w szczególności do następujących sytuacji: a) gdy Komisarz nie podejmie odpowiednich kroków w celu udzielenia odpowiedzi na skargę; b) gdy Komisarz nie przekaże skarżącemu informacji o postępach w rozpatrywaniu skargi lub o skutkach rozpatrzenia skargi w terminie trzech miesięcy od chwili otrzymania skargi przez Komisarza; lub c) jeżeli, w przypadku niezakończenia rozpatrywania skargi w tym okresie, Komisarz nie poinformuje o tym skarżącego w okresie kolejnych trzech miesięcy.

([253]) Trybunał Pierwszej Instancji jest sądem właściwym do rozpatrywania odwołań od decyzji wydanych przez rządowe organy regulacyjne. W przypadku decyzji Komisarza ds. Informacji właściwą izbą jest „Izba ds. Regulatorów", która jest właściwa dla całego Zjednoczonego Królestwa.

([254]) Art. 166 DPA 2018. Przykłady skutecznych postępowań przeciwko Komisarzowi ds. Informacji przed trybunałem obejmują sprawę, w której Komisarz potwierdził otrzymanie skargi od osoby, której dane dotyczą, ale nie wskazał, jakie działania zamierza podjąć, w związku z czym trybunał nakazał mu potwierdzenie w ciągu 21 dni kalendarzowych, czy zamierza przeprowadzić dochodzenie w sprawie skargi, a jeżeli tak, informowanie skarżącego o postępach w dochodzeniu nie rzadziej niż co 21 dni kalendarzowych (wyrok nie został jeszcze opublikowany), oraz sprawę, w której trybunał pierwszej instancji uznał, że nie jest jasne, czy odpowiedź Komisarza na skargę stanowi należyty „wynik" skargi (zob. Susan Milne przeciwko The Information Commissioner [2020], wyrok dostępny pod adresem: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Art. 162 i 163 DPA 2018.

([256]) Zob. np. sprawa Brown przeciwko Commissioner of Police of the Metropolis i in. [2019] EWCA Civ 1724, w której na podstawie DPA 1998 i ustawy o prawach człowieka z 1998 r. Trybunał przyznał odszkodowanie w wysokości 9 000 GBP za bezprawne uzyskanie i wykorzystanie danych osobowych niezgodnie z przeznaczeniem, oraz sprawa Korona (z powództwa Bridges) przeciwko Chief Constable of South Wales [2020] EWCA Civ 1058, w której Sąd Apelacyjny uznał za niezgodne z prawem wdrożenie systemu rozpoznawania twarzy przez walijską policję, ponieważ naruszało to art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności i ocena skutków dla ochrony danych przeprowadzona przez administratora nie była zgodna z DPA 2018.

([257]) Art. 34 Konwencji o ochronie praw człowieka i podstawowych wolności stanowi, że „Trybunał może przyjmować skargi każdej osoby, organizacji pozarządowej lub grupy jednostek, która uważa, że stała się ofiarą naruszenia przez jedną z Wysokich Układających się Stron praw zawartych w Konwencji lub jej protokołach. Wysokie Układające się Strony zobowiązują się nie przeszkadzać w żaden sposób skutecznemu wykonywaniu tego prawa".

### 3.3. **Dostęp organów publicznych Zjednoczonego Królestwa do danych w celach związanych z bezpieczeństwem narodowym i wykorzystywanie przez nie danych w tych celach**

(175) W porządku prawnym Zjednoczonego Królestwa służbami wywiadowczymi uprawnionymi do gromadzenia informacji elektronicznych będących w posiadaniu administratorów lub podmiotów przetwarzających ze względów bezpieczeństwa narodowego, w sytuacjach istotnych dla scenariusza odpowiedniości, są: Służba Bezpieczeństwa ([258]) (Security Service, MI5), ([259]) Tajna Służba Wywiadowcza (Secret Intelligence Service, SIS) oraz Centrala Łączności Rządowej ([260]) (Government Communications Headquarters, GCHQ) ([261]).

#### 3.3.1. *Podstawy prawne, ograniczenia i zabezpieczenia*

(176) W Zjednoczonym Królestwie uprawnienia agencji wywiadowczych określono w IPA 2016 i RIPA 2000, które wraz z DPA 2018 określają zakres przedmiotowy i podmiotowy tych uprawnień i przewidują ograniczenia i zabezpieczenia w zakresie ich wykonywania. W dalszych sekcjach szczegółowo oceniono powyższe uprawnienia, jak również ograniczenia i zabezpieczenia mające do nich zastosowanie.

##### 3.3.1.1. Uprawnienia dochodzeniowo-śledcze wykonywane w kontekście bezpieczeństwa narodowego

(177) W IPA 2016 przewidziano ramy prawne dla korzystania z uprawnień dochodzeniowo-śledczych, tj. uprawnień do przechwytywania i dostępu do danych pochodzących z łączności oraz dokonywania ingerencji w urządzenia elektroniczne. W IPA 2016 wprowadzono ogólny zakaz i uznano za czyn zabroniony stosowanie technik umożliwiających dostęp do treści komunikacji, dostęp do danych pochodzących z łączności lub ingerencję w urządzenia elektroniczne bez zgodnego z prawem upoważnienia ([262]). Znajduje to odzwierciedlenie w fakcie, że korzystanie z tych uprawnień dochodzeniowo-śledczych jest zgodne z prawem tylko wtedy, gdy odbywa się na podstawie nakazu lub upoważnienia ([263]).

(178) W IPA 2016 określono szczegółowe zasady regulujące zakres i stosowanie poszczególnych uprawnień dochodzeniowych, a także szczególne ograniczenia i zabezpieczenia ich dotyczące. Stosuje się różne zasady w zależności od rodzaju uprawnień dochodzeniowo-śledczych (przechwytywanie komunikacji, pozyskiwanie i zatrzy-

([258]) MI5 podlega Home Secretary (ministrowi spraw wewnętrznych). W ustawie o Służbie Bezpieczeństwa z 1989 r. określono funkcje MI5: ochrona bezpieczeństwa narodowego (w tym ochrona przed zagrożeniami w postaci szpiegostwa, terroryzmu i sabotażu, przed działaniami agentów zagranicznych sił oraz przed działaniami mającymi na celu obalenie lub podważenie demokracji parlamentarnej środkami politycznymi, przemysłowymi lub przemocą), ochrona dobrobytu gospodarczego Zjednoczonego Królestwa przed zagrożeniami zewnętrznymi oraz wspieranie działań sił policyjnych i innych organów ścigania w zakresie zapobiegania i wykrywania poważnej przestępczości.

([259]) SIS podlega Foreign Secretary (ministrowi spraw zagranicznych), a jej funkcje określono w ustawie o służbach wywiadowczych z 1994 r. Jej funkcje polegają na pozyskiwaniu i dostarczaniu informacji dotyczących działań lub zamiarów osób spoza Wysp Brytyjskich oraz wykonywaniu innych zadań związanych z działaniami lub zamiarami takich osób. Funkcje te mogą być pełnione wyłącznie w interesie bezpieczeństwa narodowego, w interesie dobrobytu gospodarczego Zjednoczonego Królestwa lub w celu wspierania zapobiegania poważnym przestępstwom lub ich wykrywania.

([260]) GCHQ podlega Foreign Secretary (ministrowi spraw zagranicznych), a jej funkcje określono w ustawie o służbach wywiadowczych z 1994 r. Są to: a) monitorowanie, wykorzystywanie lub zakłócanie emisji elektromagnetycznych i innych oraz urządzeń wytwarzających takie emisje, pozyskiwanie i dostarczanie informacji pochodzących z takich emisji lub urządzeń oraz z zaszyfrowanych materiałów lub z nimi związanych; b) udzielanie porad i pomocy w zakresie języków, w tym terminologii stosowanej w sprawach technicznych i kryptografii, oraz w innych kwestiach związanych z ochroną informacji siłom zbrojnym, rządowi lub innym organizacjom bądź osobom, w przypadku których uznano to za stosowne. Funkcje te mogą być pełnione wyłącznie w interesie bezpieczeństwa narodowego, w interesie dobrobytu gospodarczego Zjednoczonego Królestwa w odniesieniu do działań lub zamiarów osób spoza Wysp Brytyjskich lub w celu wspierania zapobiegania poważnym przestępstwom lub ich wykrywania.

([261]) Inne podmioty publiczne pełniące funkcje istotne dla bezpieczeństwa narodowego to Defence Intelligence (DI – służba wywiadu wojskowego), National Security Council and Secretariat (Rada Bezpieczeństwa Narodowego i Sekretariat), Joint Intelligence Organisation (JIO – Wspólna Organizacja Wywiadowcza) oraz Joint Intelligence Committee (JIC – Wspólny Komitet Wywiadowczy). Jednak ani JIC, ani JIO nie mogą korzystać z uprawnień dochodzeniowo-śledczych na mocy IPA 2016, natomiast DI ma ograniczony zakres korzystania ze swoich uprawnień.

([262]) Zakaz ten dotyczy zarówno publicznych, jak i prywatnych sieci komunikacyjnych, a także publicznych usług pocztowych, jeżeli przechwytywanie odbywa się w Zjednoczonym Królestwie. Zakaz ten nie dotyczy administratora sieci prywatnej, jeżeli udzielił on wyraźnej lub dorozumianej zgody na przeprowadzenie przechwycenia (art. 3 IPA 2016).

([263]) W szczególnych, ograniczonych przypadkach możliwe jest zgodne z prawem przechwytywanie bez nakazu, tj. w przypadku przechwytywania za zgodą nadawcy lub odbiorcy (art. 44 IPA 2016), w przypadku ograniczonych celów administracyjnych lub egzekucyjnych (art. 45–48 ustawy o uprawnieniach dochodzeniowo-śledczych), w niektórych instytucjach specjalnych (art. 49–51 ustawy o uprawnieniach śledczych z 2016 r.) oraz zgodnie z wnioskami zagranicznymi (art. 52 IPA 2016).

mywanie danych pochodzących z łączności oraz ingerencja w urządzenia elektroniczne) ([264]), a także od tego, czy uprawnienia te wykonuje się w odniesieniu do konkretnego celu, czy też masowo. Szczegółowe informacje na temat zakresu, zabezpieczeń i ograniczeń określonych w IPA 2016 w odniesieniu do poszczególnych środków przedstawiono w sekcji poniżej.

(179) Ponadto uzupełnieniem IPA 2016 jest szereg ustawowych kodeksów postępowania, wydanych przez Sekretarza Stanu, zatwierdzonych przez obie izby parlamentu ([265]) i obowiązujących w całym państwie, zawierających dalsze wytyczne dotyczące korzystania ze wspomnianych uprawnień ([266]). Jakkolwiek osoby, których dane dotyczą, mogą przy wykonywaniu swoich praw powoływać się bezpośrednio na przepisy określone w IPA 2016, w załączniku 7 ust. 5 do IPA 2016 określono, że kodeksy postępowania są dopuszczalne jako dowód w postępowaniu cywilnym i karnym, a sąd, trybunał lub organ nadzorczy może wziąć pod uwagę wszelkie niezgodności z kodeksami przy ustalaniu istotnej kwestii w postępowaniu sądowym ([267]). W kontekście oceny wcześniejszych przepisów Zjednoczonego Królestwa w dziedzinie nadzoru – RIPA 2000 – pod kątem jakości prawa wielka izba Europejskiego Trybunału Praw Człowieka wyraźnie uznała znaczenie brytyjskich kodeksów postępowania i przyznała, że ich przepisy mogą być brane pod uwagę przy ocenie przewidywalności przepisów umożliwiających nadzór ([268]).

(180) Należy zatem zauważyć, że ukierunkowane uprawnienia (ukierunkowane przechwytywanie ([269]), pozyskiwanie danych pochodzących z łączności ([270]), zatrzymywanie danych pochodzących z łączności ([271]) i ukierunkowana ingerencja w urządzenia elektroniczne ([272])) są dostępne dla agencji bezpieczeństwa narodowego i niektórych organów ścigania ([273]), podczas gdy wyłącznie służby wywiadowcze mogą korzystać z uprawnień do masowego pozyskiwania danych (tj. masowego przechwytywania ([274]), masowego pozyskiwania danych pochodzących z łączności ([275]), masowej ingerencji w urządzenia elektroniczne ([276]) i masowych zbiorów danych osobowych ([277])).

(181) Podejmując decyzję, z którego uprawnienia dochodzeniowo-śledczego należy skorzystać, agencja wywiadowcza musi przestrzegać „ogólnych obowiązków w odniesieniu do prywatności" wymienionych w art. 2 ust. 2 lit. a) IPA 2016, które obejmują analizę niezbędności i proporcjonalności. Ściślej rzecz ujmując, zgodnie z tym przepisem organ publiczny mający zamiar skorzystać z uprawnienia dochodzeniowo-śledczego musi rozważyć (i) czy skutek, który ma zostać osiągnięty za pomocą nakazu, upoważnienia lub zawiadomienia, można by osiągnąć w sposób racjonalny za pomocą innych środków związanych z mniejszą ingerencją w prywatność; (ii) czy stopień ochrony,

([264]) Jeżeli chodzi na przykład o zakres takich środków, zgodnie z częścią 3 i 4 (zatrzymywanie i pozyskiwanie danych komunikacyjnych) zakres środka jest ściśle powiązany z definicją „operatorów telekomunikacyjnych", których dane użytkowników są objęte danym środkiem. Inny przykład można podać w odniesieniu do korzystania z uprawnień do masowego pozyskiwania danych. W tym przypadku ich zakres jest ograniczony do „komunikacji wysyłanych lub otrzymywanych przez osoby fizyczne poza Wyspami Brytyjskimi".

([265]) W załączniku 7 do IPA 2016 określono zakres kodeksów, tryb postępowania przy ich wydawaniu, zasady ich zmiany oraz skutki kodeksów.

([266]) Kodeksy postępowania na podstawie IPA 2016 są dostępne pod adresem: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Sądy i Trybunały korzystają z kodeksów postępowania, aby ocenić zgodność z prawem postępowania władz. Zob. np.: sprawa Dias przeciwko Cleveland Police [2017] UKIPTrib15_586-CH, w której Trybunał ds. Uprawnień Dochodzeniowo-Śledczych odniósł się do określonych fragmentów kodeksu postępowania w zakresie danych pochodzących z łączności, aby zrozumieć definicję podstawy „zapobiegania przestępstwom lub ich wykrywania albo zapobiegania zakłóceniom porządku" używanej do wnoszenia o pozyskanie danych pochodzących z łączności. Kodeks włączono do uzasadnienia w celu ustalenia, czy podstawę tę zastosowano nieprawidłowo. Sąd stwierdził następnie, że zakwestionowane działania były niezgodne z prawem. Sądy dokonały również oceny poziomu zabezpieczeń dostępnych w kodeksach, zob. np. Just for Kids Law przeciwko Secretary of State for the Home Department [2019] EWHC 1772 (Admin), kiedy to Wysoki Trybunał uznał, że przepisy ustawodawcze i wykonawcze wraz z wewnętrznymi wytycznymi zapewniały wystarczające zabezpieczenia; lub sprawa Korona (National Council for Civil Liberties) przeciwko Secretary of State for the Home Department i in. [2019] EWHC 2057 (Admin), w której stwierdzono, że zarówno IPA 2016, jak i kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne zawierały wystarczające przepisy co do potrzeby szczegółowości nakazów.

([268]) W sprawie Big Brother Watch wielka izba Europejskiego Trybunału Praw Człowieka zauważyła, że „kodeks IC jest dokumentem publicznym zatwierdzonym przez obie izby parlamentu, opublikowanym przez rząd w internecie i w wersji drukowanej, który musi być brany pod uwagę zarówno przez osoby wykonujące obowiązki w zakresie przechwytywania, jak i przez sądy (zob. pkt 93-94 powyżej). W konsekwencji Trybunał uznał, że przepisy kodeksu mogą być brane pod uwagę przy ocenie przewidywalności RIPA (zob. ww. wyrok w sprawie Kennedy, § 157). W związku z tym Trybunał uznałby, że prawo krajowe było odpowiednio „dostępne" (zob. wyrok Europejskiego Trybunału Praw Człowieka (wielka izba), Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu, skargi nr 58170/13, 62322/14 i 24960/15 z dnia 25 maja 2021 r., pkt 366).

([269]) Część 2 IPA 2016.

([270]) Część 3 IPA 2016.

([271]) Część 4 IPA 2016.

([272]) Część 5 IPA 2016.

([273]) Wykaz właściwych organów ścigania, które mogą stosować ukierunkowane uprawnienia dochodzeniowe na podstawie IPA 2016 – zob. przypis 139.

([274]) Art. 136 IPA 2016.

([275]) Art. 158 IPA 2016.

([276]) Art. 176 IPA 2016.

([277]) Art. 199 IPA 2016.

jaki należy zastosować w odniesieniu do każdego przypadku pozyskiwania informacji na podstawie nakazu, upoważnienia lub zawiadomienia, jest wyższy ze względu na szczególną wrażliwość tych informacji; (iii) interes publiczny w zakresie integralności i bezpieczeństwa systemów telekomunikacyjnych i usług pocztowych oraz (iv) wszelkie inne aspekty interesu publicznego w zakresie ochrony prywatności ([278]).

(182) Sposób, w jaki należy stosować te kryteria – oraz sposób, w jaki ocenia się ich zgodność w ramach zatwierdzania korzystania z takich uprawnień przez Sekretarza Stanu i niezależnych komisarzy sądowych – określono dokładniej w odpowiednich kodeksach postępowania. W szczególności korzystanie z któregokolwiek ze wspomnianych uprawnień dochodzeniowych musi być zawsze „proporcjonalne do skutku, który ma zostać osiągnięty[, co] obejmuje zrównoważenie wagi ingerencji w prywatność (i innych względów określonych w art. 2 ust. 2) w stosunku do potrzeby prowadzenia działań pod względem dochodzeniowym, operacyjnym lub w zakresie zdolności". Oznacza to przede wszystkim, że „powinno ono dawać realistyczną perspektywę uzyskania oczekiwanej korzyści i nie powinno być nieproporcjonalne ani arbitralne" oraz, że „[n]ie należy uznawać ingerencji w prywatność za proporcjonalną, jeżeli poszukiwaną informację można by pozyskać za pomocą innych środków związanych z mniejszą ingerencją w prywatność ([279]). Ściślej rzecz ujmując, zgodność z zasadą proporcjonalności należy oceniać z uwzględnieniem następujących kryteriów: „(i) zakres proponowanej ingerencji w prywatność w stosunku do skutku, który ma zostać osiągnięty; (ii) to, w jaki sposób i dlaczego metody, które mają zostać przyjęte, spowodują najmniejszą możliwą ingerencję w prywatność danej osoby i innych osób; (iii) to, czy działanie stanowi właściwe wykorzystanie ustawy oraz zasadny sposób osiągnięcia zamierzonego skutku, po rozważeniu wszystkich zasadnych alternatyw; (iv) to, jakich innych metod, w stosownych przypadkach, nie wdrożono lub jakie zastosowano, ale oceniono jako niewystarczające do osiągnięcia celów operacyjnych bez wykorzystania proponowanych uprawnień dochodzeniowo-śledczych" ([280]).

(183) W praktyce, jak wyjaśniły władze Zjednoczonego Królestwa, gwarantuje to, że agencja wywiadowcza po pierwsze określa cel operacyjny (wyznaczając w ten sposób granice gromadzenia, np. międzynarodowy cel walki z terroryzmem na określonym obszarze geograficznym), a po drugie, na podstawie tego celu operacyjnego, będzie ona musiała rozważyć, która opcja techniczna (np. ukierunkowane lub masowe przechwytywanie, ukierunkowana lub masowa ingerencja w urządzenia elektroniczne, ukierunkowane lub masowe pozyskiwanie danych pochodzących z łączności) jest najbardziej proporcjonalna (tj. najmniej naruszająca prywatność, por. art. 2 ust. 2 ustawy o uprawnieniach dochodzeniowo-śledczych) do zamierzonego celu i dlatego może zostać zatwierdzona na podstawie jednej z dostępnych ustawowych podstaw prawnych.

(184) Warto zauważyć, że to oparcie się na standardach niezbędności i proporcjonalności zauważył także i przyjął z zadowoleniem specjalny sprawozdawca ONZ ds. prawa do prywatności, Joseph Cannataci, który w odniesieniu do systemu ustanowionego na podstawie IPA 2016 stwierdził, że „[t]e procedury obowiązujące zarówno w ramach służb wywiadowczych, jak i w ramach organów ścigania wydają się systematycznie wymagać rozważenia niezbędności i proporcjonalności środka lub operacji nadzoru przed zaleceniem jego zatwierdzenia, jak również jego przeglądu na tych samych podstawach" ([281]). Ponadto zauważył on, że na spotkaniu z przedstawicielami organów ścigania i agencji bezpieczeństwa narodowego „dotarł [do niego] zgodny pogląd, że prawo do prywatności musi być głównym czynnikiem przy podejmowaniu jakichkolwiek decyzji dotyczących środków nadzoru. Wszyscy rozumieli i doceniali niezbędność i proporcjonalność jako kardynalne zasady, które należy brać pod uwagę".

([278]) W kodeksie postępowania w zakresie przechwytywania komunikacji (Code of Practice on Interception of Communications) określono, że inne elementy analizy proporcjonalności obejmują: „(i) zakres proponowanej ingerencji w prywatność w stosunku do skutku, który ma zostać osiągnięty; (ii) to, w jaki sposób i dlaczego metody, które mają zostać przyjęte, spowodują najmniejszą możliwą ingerencję w prywatność danej osoby i innych osób; (iii) to, czy działanie stanowi właściwe wykorzystanie ustawy oraz zasadny sposób osiągnięcia zamierzonego skutku, po rozważeniu wszystkich zasadnych alternatyw; (iv) to, jakich innych metod, w stosownych przypadkach, nie wdrożono lub jakie zastosowano, ale oceniono jako niewystarczające do osiągnięcia celów operacyjnych bez wykorzystania proponowanych uprawnień dochodzeniowo-śledczych". Kodeks postępowania w zakresie przechwytywania komunikacji, pkt 4.16, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Zob. kodeks postępowania w zakresie przechwytywania komunikacji, pkt 4.12 i 4.15, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Zob. kodeks postępowania w zakresie przechwytywania komunikacji, pkt 4.16.

([281]) Oświadczenie specjalnego sprawozdawcy ds. prawa do prywatności na zakończenie jego misji w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej, dostępne pod adresem: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, ust. 1 lit. a).

(185) Szczegółowe kryteria wydawania poszczególnych nakazów, a także ograniczenia i zabezpieczenia ustanowione w IPA 2016 w odniesieniu do poszczególnych uprawnień dochodzeniowych opisano szczegółowo w motywach 186–243.

3.3.1.1.1. Ukierunkowane przechwytywanie i badanie

(186) Istnieją trzy rodzaje nakazów ukierunkowanego przechwytywania: nakaz ukierunkowanego przechwytywania ([282]), nakaz ukierunkowanego zbadania oraz nakaz wzajemnej pomocy ([283]). Warunki ich uzyskania takich nakazów oraz dotyczące ich zabezpieczenia określono w części 2 rozdział 1 IPA 2016

(187) Nakaz ukierunkowanego przechwytywania upoważnia do przechwytywania komunikacji opisanej w nakazie w trakcie jej przekazywania oraz do pozyskiwania innych danych istotnych dla tej komunikacji ([284]), w tym danych wtórnych ([285]). Nakaz ukierunkowanego badania upoważnia osobę do dokonania wyboru w celu zbadania przechwyconych treści pozyskanych na podstawie nakazu masowego przechwytywania ([286]).

(188) Każdy nakaz na podstawie części 2 IPA 2016 może zostać wydany przez Sekretarza Stanu ([287]) i zatwierdzony przez komisarza sądowego ([288]). We wszystkich przypadkach okres obowiązywania każdego rodzaju ukierunkowanego nakazu jest ograniczony do 6 miesięcy ([289]), a zastosowanie mają przepisy szczegółowe dotyczące jego zmiany ([290]) i przedłużania ([291]).

(189) Przed wydaniem nakazu Sekretarz Stanu przeprowadza ocenę niezbędności i proporcjonalności ([292]). W szczególności w przypadku nakazu ukierunkowanego przechwytywania i nakazu ukierunkowanego badania Sekretarz Stanu powinien sprawdzić, czy środek jest niezbędny z jednego z następujących powodów: interesu bezpieczeństwa narodowego; zapobiegania poważnym przestępstwom lub ich wykrywania lub interesu dobrobytu gospodarczego Zjednoczonego Królestwa ([293]) w zakresie, w jakim interesy te są również istotne dla interesów bezpieczeństwa narodowego ([294]). Z drugiej strony nakaz w ramach wzajemnej pomocy (zob. motyw 139 powyżej) może zostać wydany tylko wtedy, gdy Sekretarz Stanu uzna, że istnieją okoliczności równoważne z tymi, w których wydałby nakaz w celu zapobieżenia poważnemu przestępstwu lub jego wykrycia ([295]).

(190) Ponadto Sekretarz Stanu powinien ocenić, czy środek jest proporcjonalny do skutku, który ma zostać osiągnięty ([296]). Ocena proporcjonalności wnioskowanych środków musi uwzględniać ogólne obowiązki w odniesieniu do prywatności określone w art. 2 ust. 2 IPA 2016, w szczególności potrzebę oceny, czy skutek, który ma zostać osiągnięty za pomocą nakazu, upoważnienia lub zawiadomienia, można by w zasadny sposób osiągnąć za pomocą

([282]) Art. 15 ust. 2 IPA 2016.
([283]) Art. 15 ust. 4 IPA 2016.
([284]) Art. 15 ust. 2 IPA 2016.
([285]) Dane wtórne to dane towarzyszące przechwyconej komunikacji lub logicznie powiązane z nią, które można logicznie od niej oddzielić i które, w przypadku takiego oddzielenia, nie ujawniłyby niczego z treści, którą można by racjonalnie uznać za (ewentualne) znaczenie komunikacji. Niektóre przykłady danych wtórnych obejmują konfiguracje routerów lub zapór sieciowych albo okres, przez jaki router był aktywny w sieci, jeżeli dane takie są częścią przechwyconej komunikacji, towarzyszą jej lub są z nią logicznie powiązane. Więcej szczegółów można znaleźć w definicji w art. 16 IPA 2016 i kodeksie postępowania w zakresie przechwytywania komunikacji, pkt 2.19, zob. przypis 278.
([286]) Badanie to przeprowadza się na zasadzie wyjątku od art. 152 ust. 4 IPA 2016, która przewiduje zakaz dążenia do identyfikacji komunikacji osób fizycznych, które znajdują się na Wyspach Brytyjskich. Zob. motyw 229.
([287]) Szkocki minister zatwierdza nakaz, gdy dotyczy on poważnej działalności przestępczej w Szkocji (zob. art. 21 i 22 IPA 2016), natomiast Sekretarz Stanu może wyznaczyć urzędnika wyższego szczebla do wydania nakazu w ramach wzajemnej pomocy, gdy wydaje się, że przechwytywanie będzie dotyczyło osoby lub obiektu znajdujących się poza Zjednoczonym Królestwem (art. 40 IPA 2016).
([288]) Art. 19 i 23 IPA 2016.
([289]) Art. 32 IPA 2016.
([290]) Art. 39 IPA 2016. Osoby uprawnione mogą dokonywać ograniczonych zmian w nakazach na warunkach określonych w IPA 2016 Osoba, która wydała nakaz, może go w każdej chwili odwołać. Musi to zrobić, jeżeli nakaz nie jest już niezbędny z jakichkolwiek istotnych powodów lub postępowanie, na które zezwala nakaz, nie jest już proporcjonalne do wyznaczonego celu.
([291]) Art. 33 IPA 2016. Decyzję o przedłużeniu nakazu musi zatwierdzić komisarz sądowy.
([292]) Art. 19 IPA 2016.
([293]) Co się tyczy pojęcia „interesów dobrobytu gospodarczego Zjednoczonego Królestwa, o ile interesy te mają również znaczenie dla bezpieczeństwa narodowego", wielka izba Europejskiego Trybunału Praw Człowieka w wyroku w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (zob. przypis 268 powyżej), pkt 371, stwierdziła, że pojęcie to w wystarczającym stopniu koncentruje się na bezpieczeństwie narodowym. Chociaż ustalenie Trybunału w tej sprawie było związane z zastosowaniem tego pojęcia w RIPA 2000, to samo pojęcie zostało użyte w IPA 2016.
([294]) Art. 20 ust. 2 IPA 2016.
([295]) Art. 20 ust. 3 IPA 2016.
([296]) Art. 19 ust. 1 lit. b), art. 19 ust. 2 lit. b) oraz art. 19 ust. 3 lit. b) IPA 2016.

innych środków związanych z mniejszą ingerencją w prywatność oraz czy stopień ochrony, który ma być stosowany w odniesieniu do wszelkiego pozyskiwania informacji na podstawie nakazu, jest wyższy ze względu na szczególną wrażliwość tych informacji (zob. motyw 181 powyżej).

(191) W tym celu Sekretarz Stanu musi wziąć pod uwagę wszystkie elementy wniosku przedstawione przez organ składający wniosek, w szczególności te związane z osobami, których ma dotyczyć przechwycenie, oraz ze znaczeniem środka dla dochodzenia. Elementy te wyszczególniono w kodeksie postępowania w zakresie przechwytywania komunikacji i należy je opisać z określonym stopniem szczegółowości ([297]). Ponadto w art. 17 IPA 2016 wymaga się, aby w każdym nakazie wydanym na podstawie jej rozdziału 2 wskazano lub opisano konkretną osobę lub grupę osób, organizację lub obiekt, których ma dotyczyć przechwycenie („cel"). W przypadku nakazu ukierunkowanego przechwytywania lub nakazu ukierunkowanego badania mogą one również odnosić się do grupy osób, więcej niż jednej osoby lub organizacji, lub więcej niż jednego zespołu obiektów (zwane również „nakazem tematycznym") ([298]). W takich przypadkach w nakazie należy opisać wspólny cel lub wspólną działalność grupy osób lub operację/dochodzenia oraz wymienić lub opisać jak największą liczbę tych osób/organizacji lub zespół lokali, o ile jest to wykonalne w zasadny sposób ([299]). Ponadto we wszystkich nakazach wydanych na podstawie części 2 IPA 2016 należy określić adresy, numery, aparaturę, czynniki lub kombinację czynników, które mają być wykorzystane do identyfikacji komunikacji ([300]). W tym zakresie w kodeksie postępowania w zakresie przechwytywania komunikacji określono, że w przypadku nakazu ukierunkowanego przechwytywania i nakazu ukierunkowanego badania „w nakazie należy określić (lub opisać) czynniki lub kombinację czynników, które mają być wykorzystane do identyfikacji komunikacji. Jeżeli komunikacja ma być identyfikowana poprzez (przykładowo) odniesienie do numeru telefonu, numer ten należy określić poprzez podanie go w całości. Jeżeli jednak do identyfikacji komunikacji mają być użyte bardzo złożone lub stale zmieniające się selektory internetowe, selektory te należy opisać w możliwie najszerszym zakresie" ([301]).

(192) Ważnym zabezpieczeniem w tym kontekście jest to, że ocena przeprowadzona przez Sekretarza Stanu w celu wydania nakazu wymaga zatwierdzenia przez niezależnego komisarza sądowego ([302]), który w szczególności sprawdzi, czy decyzja o wydaniu nakazu jest zgodna z zasadami niezbędności i proporcjonalności ([303]) (informacje o statusie i roli komisarzy sądowych – zob. motywy 251–256 poniżej). W IPA 2016 doprecyzowano również, że przeprowadzając taką kontrolę, komisarz sądowy musi stosować te same zasady, które zastosowałby sąd w przypadku wniosku o kontrolę sądową ([304]). Gwarantuje to, że w każdym przypadku i przed uzyskaniem dostępu do danych niezależny organ systematycznie kontroluje zgodność z zasadą niezbędności i proporcjonalności.

(193) W IPA 2016 przewidziano nieliczne konkretne i wąsko sformułowane wyjątki dotyczące przeprowadzania ukierunkowanego przechwytywania bez nakazu. Ograniczone przypadki są szczegółowo określone w prawie ([305]) i – z wyjątkiem przypadków opartych na zgodzie nadawcy lub odbiorcy – są prowadzone przez podmioty (prywatne lub publiczne) inne niż krajowe agencje bezpieczeństwa. Ponadto tego rodzaju przechwytywanie odbywa się w celach innych niż gromadzenie informacji wywiadowczych ([306]), a w przypadku niektórych z nich bardzo mało prawdopodobne jest, aby gromadzenie danych mogło odbywać się w ramach scenariusza przekazywania danych (np. w przypadku przechwytywania dokonywanego w szpitalu psychiatrycznym lub w więzieniu). Biorąc pod uwagę charakter organu, do którego mają zastosowanie te szczególne przypadki (innego niż krajowe agencje bezpieczeństwa), zastosowanie będą miały wszystkie zabezpieczenia przewidziane w części 2 DPA 2018 i w RODO UK,

([297]) Wymagane informacje obejmują szczegóły dotyczące kontekstu (opis osób/organizacji/zespołu obiektów, komunikacji, której ma dotyczyć przechwycenie) oraz tego, w jaki sposób uzyskanie tych informacji będzie korzystne dla dochodzenia, jak również opis postępowania, na które ma zostać udzielone zezwolenie. W przypadku gdy nie jest możliwe opisanie osób/organizacji/obiektów, należy podać wyjaśnienie, dlaczego nie było to możliwe lub dlaczego przedstawiono wyłącznie ogólny opis (kodeks postępowania w zakresie przechwytywania komunikacji, pkt 5.32 i 5.34, zob. przypis 278).

([298]) Art. 17 ust. 2 IPA 2016. Zob. również kodeks postępowania w zakresie przechwytywania komunikacji, pkt 5.11 i nast., zob. przypis 278.

([299]) Art. 31 ust. 4 i 5 IPA 2016.

([300]) Art. 31 ust. 8 IPA 2016.

([301]) Kodeks postępowania w zakresie przechwytywania komunikacji, pkt 5.37 i 5.38, zob. przypis 278.

([302]) Zatwierdzenie przez komisarza sądowego nie jest wymagane, jeżeli Sekretarz Stanu uzna, że istnieje pilna potrzeba wydania nakazu (art. 19 ust. 1 ustawy o uprawnieniach dochodzeniowo-śledczych). Należy jednak w krótkim czasie poinformować komisarza sądowego, który podejmuje decyzję o zatwierdzeniu lub niezatwierdzeniu nakazu. Jeżeli tego nie zrobi, nakaz traci moc (art. 24 i 25 IPA 2016).

([303]) Art. 23 ust. 1 IPA 2016.

([304]) Art. 23 ust. 2 IPA 2016.

([305]) Zob. art. 44-51 IPA 2016 i art. 12 kodeksu postępowania w zakresie przechwytywania komunikacji (zob. przypis 278).

([306]) Dotyczy to np. sytuacji, gdy przechwytywanie jest konieczne w więzieniu lub w szpitalu psychiatrycznym (w celu sprawdzenia zachowania osadzonego lub pacjenta) lub przez operatora pocztowego lub telekomunikacyjnego, na przykład w celu wykrycia treści stanowiących nadużycie.

w tym nadzór Komisarza ds. Informacji i dostępne mechanizmy dochodzenia roszczeń. Ponadto oprócz zabezpieczeń przewidzianych w DPA 2018 w niektórych przypadkach IPA 2016 przewiduje również nadzór *ex post* Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych ([307]).

(194) W sytuacji przechwytywania mają zastosowanie dodatkowe ograniczenia i zabezpieczenia związane ze szczególnym statusem osoby lub osób, których dotyczy przechwytywanie ([308]). Przykładowo przechwytywanie materiałów objętych prawniczą tajemnicą zawodową jest dozwolone wyłącznie w wyjątkowych i uzasadnionych okolicznościach; osoba wydająca nakaz musi uwzględnić interes publiczny w zachowaniu poufności materiałów objętych prawniczą tajemnicą zawodową oraz to, że istnieją szczególne wymogi dotyczące postępowania z takimi materiałami, ich zatrzymywania i ujawniania ([309]).

(195) Ponadto IPA 2016 przewiduje szczególne zabezpieczenia związane z bezpieczeństwem, zatrzymywaniem i ujawnianiem, które Sekretarz Stanu powinien wziąć pod uwagę przed wydaniem ukierunkowanego nakazu ([310]). W szczególności w art. 53 ust. 5 IPA 2016 wymaga się, aby każdą kopię wszelkich materiałów zebranych na podstawie nakazu przechowywano w bezpieczny sposób i niszczono, gdy tylko nie ma już istotnych podstaw do jej zatrzymywania, natomiast w art. 53 ust. 2 IPA 2016 wymaga się, aby liczbę osób, którym ujawnia się materiał, oraz zakres, w jakim wszelkie materiały są ujawniane, udostępniane lub kopiowane, ograniczono do minimum niezbędnego do realizacji celów ustawowych.

(196) Ponadto gdy materiał przechwycony na podstawie nakazu ukierunkowanego przechwytywania albo na podstawie nakazu w ramach wzajemnej pomocy ma zostać przekazany do państwa trzeciego („ujawnienia za granicą"), IPA 2016 przewiduje, że Sekretarz Stanu musi zapewnić, aby istniały odpowiednie ustalenia w celu zapewnienia istnienia podobnych zabezpieczeń dotyczących bezpieczeństwa, zatrzymywania i ujawniania w danym państwie trzecim ([311]). Ponadto art. 109 ust. 2 DPA 2018 stanowi, że służby wywiadowcze mogą przekazywać dane osobowe poza terytorium Zjednoczonego Królestwa jedynie wówczas, gdy przekazanie jest niezbędne i proporcjonalne do celów wykonywania ustawowych funkcji administratora lub do innych celów przewidzianych w art. 2 ust. 2 lit. a) ustawy o Służbie Bezpieczeństwa z 1989 r. lub art. 2 ust. 2 lit. a) i art. 4 ust. 2 lit. a) ustawy o służbach wywiadowczych z 1994 r. ([312]). Co ważne, wymogi te mają również zastosowanie w przypadkach, w których powołano się na wyłączenie ze względów bezpieczeństwa narodowego zgodnie z art. 110 DPA 2018, ponieważ w art. 110 DPA 2018 nie wymieniono art. 109 DPA 2018 jako jednego z przepisów, od których można odstąpić, jeżeli do celów ochrony bezpieczeństwa narodowego wymagane jest wyłączenie niektórych przepisów.

3.3.1.1.2. Ukierunkowane pozyskiwanie i zatrzymywanie danych pochodzących z łączności

(197) 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.

([307]) Zob. kontrprzykład w art. 229 ust. 4 IPA.

([308]) W art. 26–29 IPA 2016 wprowadzono ograniczenia w zakresie uzyskiwania nakazów ukierunkowanego przechwytywania i badania w odniesieniu do przechwytywania komunikacji wysyłanej przez osobę będącą członkiem parlamentu (dowolnego parlamentu Zjednoczonego Królestwa) lub przeznaczonych dla tej osoby, przechwytywania materiałów objętych prawniczą tajemnicą zawodową, przechwytywania komunikacji, co do której organ przechwytujący uważa, że będzie zawierała poufne materiały dziennikarskie, oraz gdy celem nakazu jest identyfikacja lub potwierdzenie źródła informacji dziennikarskich.

([309]) Art. 26 IPA 2016.

([310]) Art. 19 ust. 1 IPA 2016.

([311]) Art. 54 IPA 2016. Zabezpieczenia dotyczące ujawniania materiałów organom zagranicznym są bardziej szczegółowo określone w kodeksie postępowania: zob. w szczególności pkt 9.26 i nast. oraz 9.87 Kodeksu postępowania w zakresie przechwytywania komunikacji oraz pkt 9.33 i nast. oraz 9.41 kodeksu postępowania w zakresie ingerencji w urządzenia elektroniczne (zob. przypis 278).

([312]) Cele te są następujące: w przypadku Służby Bezpieczeństwa – zapobieganie poważnym przestępstwom lub ich wykrywanie lub wszelkie postępowania karne (art. 2 ust. 2 lit. a) ustawy o Służbie Bezpieczeństwa z 1989 r.), w przypadku Służby Wywiadu – interesy bezpieczeństwa narodowego, zapobieganie poważnym przestępstwom lub ich wykrywanie lub wszelkie postępowania karne (art. 2 ust. 2 lit. a) ustawy o służbach wywiadowczych z 1994 r.), natomiast w przypadku GCHQ – wszelkie postępowania karne (art. 4 ust. 2 lit. a) ustawy o służbach wywiadowczych z 1994 r.). Zob. również noty wyjaśniające do DPA 2018, dostępne pod adresem: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Termin „dane pochodzące z łączności" 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. W odróżnieniu od przechwytywania, pozyskiwanie i zatrzymywanie danych pochodzących z łączności nie ma na celu uzyskania treści wiadomości, ale pozyskanie informacji np. o abonencie usługi telefonicznej lub o szczegółowym rachunku. Mogą one dotyczyć czasu i okresu trwania komunikacji, numeru lub adresu e-mail nadawcy i odbiorcy, a czasami lokalizacji urządzeń, z których dokonano połączenia ([313]).

(199) Należy zauważyć, że zatrzymywanie i pozyskiwanie danych pochodzących z łączności zazwyczaj nie będzie dotyczyć danych osobowych osób z UE, przekazywanych na podstawie niniejszej decyzji do Zjednoczonego Królestwa. Obowiązek zatrzymania lub ujawnienia danych pochodzących z łączności zgodnie z częściami 3 i 4 IPA 2016 obejmuje dane, które operatorzy telekomunikacyjni w Zjednoczonym Królestwie gromadzą bezpośrednio od użytkowników usługi telekomunikacyjnej ([314]). Ten rodzaj przetwarzania „widoczny dla klienta" zazwyczaj nie wiąże się z przekazywaniem na podstawie niniejszej decyzji, tj. przekazywaniem od administratora lub podmiotu przetwarzającego w UE do administratora lub podmiotu przetwarzającego w Zjednoczonym Królestwie.

(200) Niemniej dla pełnego obrazu sytuacji w poniższych motywach opisano warunki i zabezpieczenia regulujące te systemy pozyskiwania i zatrzymywania danych.

(201) Jako założenie należy zauważyć, że zatrzymywanie i ukierunkowane pozyskiwanie danych pochodzących z łączności przysługuje zarówno krajowym agencjom bezpieczeństwa, jak i niektórym organom ścigania ([315]). Warunki wymagające zatrzymywania lub pozyskiwania danych pochodzących z łączności mogą różnić się w zależności od podstawy złożenia wniosku o zastosowanie środka, a mianowicie bezpieczeństwa narodowego lub celu związanego z egzekwowaniem prawa.

(202) W szczególności, chociaż w nowym systemie wprowadzono ogólny wymóg uprzedniego uzyskania zezwolenia niezależnego organu, mający zastosowanie we wszystkich przypadkach zatrzymywania lub pozyskiwania danych pochodzących z łączności (do celów egzekwowania prawa lub do celów związanych z bezpieczeństwem narodowym), w następstwie wyroku Europejskiego Trybunału Sprawiedliwości w sprawie Tele2/Watson ([316]) wprowadzono szczególne zabezpieczenia w przypadku wystąpienia o zastosowanie środka do celów ochrony porządku publicznego. W szczególności w przypadku gdy wniosek o zatrzymywanie lub pozyskiwanie danych pochodzących z łączności jest wymagany do celów egzekwowania prawa, zawsze wymagane jest uprzednie zezwolenie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych. Nie zawsze ma to miejsce w przypadku wniosku o zastosowanie środka ze względów bezpieczeństwa narodowego, ponieważ, jak opisano poniżej, w niektórych przypadkach taki rodzaj środków może zostać zatwierdzony przez inną osobę zatwierdzającą. Ponadto w nowym systemie próg, w przypadku którego można zezwolić na zatrzymywanie i pozyskiwanie danych pochodzących z łączności, podniesiono do poziomu „poważnych przestępstw" ([317]).

---

([313]) Dane pochodzące z łączności zdefiniowano w art. 261 ust. 5 IPA 2016 Dane pochodzące z łączności dzielą się na „dane o zdarzeniach" (wszelkie dane umożliwiające identyfikację zdarzenia lub je opisujące, niezależnie od tego, czy odnoszą się do jego lokalizacji, w systemie telekomunikacyjnym lub za jego pomocą, w przypadku gdy zdarzenie polega na wykonywaniu przez jeden lub więcej podmiotów określonej czynności w określonym czasie) oraz „dane o podmiotach" (wszelkie dane, które a) dotyczą (i) podmiotu, (ii) związku między usługą telekomunikacyjną a podmiotem, lub (iii) związku między jakąkolwiek częścią systemu telekomunikacyjnego a podmiotem, b) składają się z danych lub zawierają dane umożliwiające identyfikację podmiotu lub go opisujące (bez względu na to, czy odnoszą się do lokalizacji podmiotu), oraz c) nie są danymi o zdarzeniach).

([314]) Wynika to z definicji terminu „dane pochodzące z łączności" zawartej w art. 261 ust. 5 IPA 2016, zgodnie z którą dane pochodzące z łączności są przechowywane lub uzyskiwane przez operatora telekomunikacyjnego i dotyczą użytkownika usługi telekomunikacyjnej oraz są związane ze świadczeniem tej usługi albo są elementem komunikacji, są jej częścią, towarzyszą jej lub są z nią powiązane pod względem logicznym (zob. również kodeks postępowania w zakresie danych pochodzących z łączności [Code of Practice on Communications Data], dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, pkt 2.22–2.33). Ponadto zgodnie z definicją terminu „operator telekomunikacyjny" zawartą w art. 261 ust. 10 IPA 2016 wymaga się, aby operatorem telekomunikacyjnym była osoba, która oferuje lub świadczy usługi telekomunikacyjne osobom w Zjednoczonym Królestwie lub która kontroluje lub zapewnia system telekomunikacyjny, który znajduje się (w całości lub częściowo) w Zjednoczonym Królestwie lub jest kontrolowany ze Zjednoczonego Królestwa. Definicje te jasno wskazują, że obowiązki wynikające z IPA 2016 nie mogą być nakładane na operatorów telekomunikacyjnych, których urządzenia nie znajdują się w Zjednoczonym Królestwie ani nie są kontrolowane z terytorium tego państwa i którzy nie oferują ani nie świadczą usług osobom fizycznym w Zjednoczonym Królestwie (zob. również kodeks postępowania w zakresie danych pochodzących z łączności, pkt 2.1). W przypadku abonentów z UE (czy to znajdujących się w UE, czy w Zjednoczonym Królestwie) korzystających z usług w Zjednoczonym Królestwie wszelkie informacje związane ze świadczeniem tych usług byłyby gromadzone bezpośrednio przez dostawcę usług w Zjednoczonym Królestwie, nie byłyby natomiast przekazywane z UE.

([315]) Odpowiednie organy wymieniono w załączniku 4 do IPA 2016 i obejmują one siły policyjne, służby wywiadowcze, niektóre ministerstwa i departamenty rządowe, Krajową Agencję ds. Zwalczania Przestępczości (NCA), Urząd Podatkowy i Celny Jej Królewskiej Mości (HMRC), Urząd ds. Konkurencji i Rynków (Competition and Markets Authority), Komisarza ds. Informacji, pogotowie ratunkowe, straż pożarną i służby ratownicze oraz organy np. w dziedzinie zdrowia i bezpieczeństwa żywności.

([316]) Sprawy połączone C-203/15 i C-698/15, Tele2/Watson, ECLI:EU:C:2016:970.

([317]) Zob. art. 61.7 lit. b) dotyczący pozyskiwania danych pochodzących z łączności oraz art. 87.10A dotyczący zatrzymywania danych pochodzących z łączności .

(i) *Zezwolenie na pozyskiwanie danych pochodzących z łączności*

(203) Zgodnie z częścią 3 IPA 2016 właściwe organy publiczne są upoważnione do pozyskiwania danych pochodzących z łączności od operatora telekomunikacyjnego lub dowolnej osoby zdolnej do pozyskania i ujawnienia takich danych. Zezwolenie nie może obejmować przechwytywanie treści komunikacji ([318]) i traci moc po upływie jednego miesiąca ([319]) z możliwością przedłużenia pod warunkiem uzyskania dodatkowego zezwolenia ([320]). Pozyskanie danych pochodzących z łączności wymaga zezwolenia Komisarza ds. Uprawnień Dochodzeniowo-Śledczych (Investigatory Powers Commissioner) ([321]) (więcej informacji o jego statusie i uprawnieniach w motywach 250–251 poniżej). Dotyczy to wszystkich przypadków, w których o uzyskanie danych pochodzących z łączności wnioskuje właściwy organ ścigania Art. 61 IPA 2016 stanowi jednak, że gdy dane pozyskuje się w interesie bezpieczeństwa narodowego lub dobrobytu gospodarczego Zjednoczonego Królestwa, o ile są one istotne dla bezpieczeństwa narodowego, lub gdy wniosek złożył członek agencji wywiadowczej na podstawie art. 61 ust. 7 lit. b) ([322]), zezwolenie na pozyskanie może wydać ([323]) Komisarz ds. Uprawnień Dochodzeniowo-Śledczych lub wyznaczony urzędnik wyższego szczebla ([324]). Wyznaczony urzędnik nie może mieć związku z danym postępowaniem przygotowawczym ani z daną operacją i musi posiadać praktyczną wiedzę na temat zasad i przepisów w obszarze praw człowieka, w szczególności na temat zasad niezbędności i proporcjonalności ([325]). Decyzja podjęta przez wyznaczonego urzędnika podlega nadzorowi *ex post* prowadzonemu przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych (zob. bardziej szczegółowe informacje na temat funkcji nadzorczych *ex post* Komisarza ds. Uprawnień Dochodzeniowo-Śledczych w motywie 254 poniżej).

(204) Zezwolenie na uzyskanie danych pochodzących z łączności wydaje się na podstawie oceny niezbędności i proporcjonalności środka. W szczególności niezbędność środka ocenia się w świetle przesłanek wymienionych w ustawodawstwie ([326]). Mając na uwadze ukierunkowany charakter tego środka, musi on być niezbędny również w przypadku konkretnego postępowania przygotowawczego lub konkretnej operacji ([327]). Dalsze wymogi dotyczące oceny niezbędności środka określono w kodeksie postępowania w zakresie danych pochodzących z łączności ([328]). W szczególności w kodeksie określono, że w celu uzasadnienia takiego żądania we wniosku złożonym przez organ wnioskujący należy wskazać następujące trzy minimalne wymagane elementy: (i) zdarzenie będące przedmiotem postępowania przygotowawczego, takie jak przestępstwo lub zlokalizowanie szczególnie narażonej osoby zaginionej; (ii) osobę, której żądane dane dotyczą – taką osobą może być podejrzany, świadek lub osoba zaginiona; należy przy tym określić, w jaki sposób taka osoba jest związana z danym zdarzeniem; (iii) żądane dane pochodzące z łączności, takie jak numer telefonu lub adres IP; należy przy tym określić, w jaki sposób takie dane wiążą się z daną osobą lub z danym zdarzeniem ([329]).

(205) Ponadto pozyskiwanie danych pochodzących z łączności musi być proporcjonalne do celu, któremu służy ([330]). W kodeksie postępowania w zakresie danych pochodzących z łączności wyjaśniono, że w ramach takiej oceny osoba zatwierdzająca powinna wyważyć, czy „stopień ingerencji w prawa i wolności danej osoby fizycznej jest pro-

([318]) Art. 60A ust. 6 IPA 2016.

([319]) Okres ten ulega skróceniu do trzech dni, gdy zezwolenie wydaje się ze względu na pilny charakter sprawy (art. 65 ust. 3A IPA 2016).

([320]) Zgodnie z art. 65 IPA 2016 przedłużone zezwolenie obowiązuje przez okres jednego miesiąca od daty wygaśnięcia poprzedniego zezwolenia. Osoba, która udzieliła zezwolenia, może je w dowolnej chwili unieważnić, jeżeli uzna, że wymagania nie są już spełniane.

([321]) Art. 60A ust. 1 IPA 2016. Urząd ds. Upoważnień Dotyczących Danych Pochodzących z Łączności (Office for Communications Data Authorisations, OCDA) pełni tę funkcję w imieniu Komisarza ds. Uprawnień Dochodzeniowo-Śledczych (zob. kodeksy praktyk w zakresie danych pochodzących z łączności, pkt 5.6)

([322]) Wniosek na podstawie art. 61 ust. 7 lit. b) IPA 2016 składa się z uwagi na „właściwy cel związany z przestępczością", co oznacza, zgodnie z art. 61 ust. 7A IPA 2016: „jeżeli dane pochodzące z łączności są w całości lub częściowo danymi o zdarzeniach, celem jest zapobieganie poważnym przestępstwom lub ich wykrywanie; w każdym innym przypadku celem jest zapobieganie przestępstwom lub ich wykrywanie, lub zapobieganie zakłóceniom porządku".

([323]) Kodeks postępowania w zakresie danych pochodzących z łączności stanowi, że „[j]eżeli wniosek związany z bezpieczeństwem narodowym można złożyć na podstawie art. 60A albo art. 61, decyzję w sprawie najodpowiedniejszego trybu uzyskania zezwolenia w danym przypadku podejmują poszczególne organy publiczne. Organy publiczne, które chcą zastosować wariant wydania zezwolenia przez wyznaczonego urzędnika wyższego szczebla, muszą kierować się wyraźnymi wytycznymi dotyczącymi sytuacji, w których taki tryb uzyskania zezwolenia jest odpowiedni" (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 5. 19, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf ).

([324]) Art. 70 ust. 3 IPA 2016 zawiera definicję terminu „wyznaczony urzędnik", przy czym w poszczególnych odpowiednich organach publicznych jest to inny urzędnik (jak określono w załączniku 4 do tej ustawy).

([325]) Dalsze szczegóły dotyczące niezależności wyznaczonego wyższego rangą urzędnika znajdują się w kodeksie postępowania w zakresie danych pochodzących z łączności (pkt 4.12-4.17, zob. przypis 323).

([326]) Przesłanki te obejmują: (i) względy bezpieczeństwa narodowego; (ii) zapobieganie przestępstwom lub ich wykrywanie, lub zapobieganie zakłóceniom porządku (w przypadku „danych o zdarzeniach" – dotyczy to wyłącznie poważnej przestępczości); (iii) interesy dobrobytu gospodarczego Zjednoczonego Królestwa w zakresie, w jakim interesy te są również istotne dla interesów bezpieczeństwa narodowego; (iv) względy bezpieczeństwa publicznego; (v) zapobieganie utracie życia lub obrażeniom ciała lub innym uszczerbkom na zdrowiu fizycznym lub psychicznym osób, lub ograniczenie wszelkich obrażeń ciała lub uszczerbków na zdrowiu fizycznym lub psychicznym osób; (vi) pomoc w postępowaniach przygotowawczych dotyczących domniemanych pomyłek sądowych lub (vii) identyfikacja osoby zmarłej lub osoby, która nie jest w stanie sama podać swojej tożsamości ze względu na konkretny stan (art. 61 ust. 7 IPA 2016).

([327]) Art. 60A ust. 1 lit. b) IPA 2016.

([328]) Kodeks postępowania w zakresie danych pochodzących z łączności, pkt 3.3 i kolejne, zob. przypis 323.

([329]) Kodeks postępowania w zakresie danych pochodzących z łączności, pkt 3.13, zob. przypis 323.

([330]) Art. 60A ust. 1 lit. c) IPA 2016.

porcjonalny do wynikającej z tej interwencji korzyści dla postępowania przygotowawczego lub operacji prowadzonych przez odpowiedni organ publiczny w interesie publicznym", a ponadto w kodeksie wyjaśniono, że biorąc pod uwagę wszystkie okoliczności danej sprawy „ingerencja w prawa i wolności danej osoby fizycznej nadal może być nieuzasadniona ze względu na nadmierny negatywny wpływ na prawa innej osoby fizycznej lub grupy osób fizycznych". Ponadto na potrzeby szczegółowej oceny proporcjonalności tego środka w kodeksie wymieniono szereg elementów, które należy uwzględnić we wniosku przedstawianym przez organ wnioskujący ([331]). Co więcej, szczególną uwagę należy zwracać na rodzaj pozyskiwanych danych pochodzących z łączności („dane o podmiotach" lub „dane o zdarzeniach" ([332])), a w pierwszej kolejności należy stosować mniej inwazyjną kategorię danych ([333]). Kodeks postępowania w zakresie danych pochodzących z łączności zawiera również konkretne wytyczne dotyczące wydawania zezwoleń w przypadku danych pochodzących z łączności dotyczących osób wykonujących określone zawody (w tym lekarzy, prawników, dziennikarzy, parlamentarzystów lub duchownych) ([334]), w odniesieniu do których zastosowanie mają dodatkowe zabezpieczenia ([335]).

(ii) *Nakaz zatrzymywania danych pochodzących z łączności*

(206) Część 4 IPA 2016 zawiera przepisy dotyczące zatrzymywania danych pochodzących z łączności, w szczególności kryteria, które muszą być spełnione, aby Sekretarz Stanu mógł wydać nakaz zatrzymywania danych ([336]). Zabezpieczenia wprowadzone w IPA są takie same niezależnie od tego, czy dane zatrzymuje się do celów związanych ze ściganiem przestępstwa, czy w interesie bezpieczeństwa narodowego.

(207) Takie nakazy zatrzymywania danych 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 ([337]). 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 i omówionego w motywach 203–205.

(208) Wykonanie uprawnienia do nakazania zatrzymania określonych danych podlega szeregowi ograniczeń i zabezpieczeń. Sekretarz Stanu może wydać operatorowi lub operatorom nakaz zatrzymywania danych ([338]) wyłącznie wówczas, gdy uważa, że wymóg zatrzymywania danych jest niezbędny w jednym z ustawowych celów ([339]) oraz jest proporcjonalny do celu, któremu służy ([340]). Jak wyjaśniono w tekście

([331]) Wymagane informacje muszą obejmować: (i) wskazanie, w jaki sposób uzyskanie tych danych będzie korzystne dla postępowania przygotowawczego lub operacji; (ii) wyjaśnienie znaczenia okresów określonych we wniosku, w tym wyjaśnienie, w jaki sposób okresy te są proporcjonalne do zdarzenia będącego przedmiotem postępowania przygotowawczego; (iii) wyjaśnienie, w jaki sposób poziom ingerencji jest uzasadniony w świetle korzystnego wpływu pozyskanych danych na postępowanie przygotowawcze (w takim uzasadnieniu należy rozważyć kwestię, czy ten sam cel można by osiągnąć, prowadząc postępowania przygotowawcze o mniejszym stopniu inwazyjności); (iv) omówienie praw (szczególnie prawa do prywatności i w stosownych przypadkach wolności wypowiedzi) osób fizycznych oraz wyważenie tych praw w stosunku do korzyści dla postępowania przygotowawczego; (v) informacje na temat charakteru ewentualnej ingerencji w prywatność osób trzecich oraz sposobu, w jaki okresy objęte wnioskiem wpływają na taką ewentualną ingerencję (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 3.22–3.26, zob. przypis 323).

([332]) Zob. przypis 313.

([333]) Jeżeli wniosek dotyczący danych pochodzących z łączności ma służyć pozyskaniu danych o większym stopniu inwazyjności (tj. danych o zdarzeniach), w kodeksie określono, że właściwszym rozwiązaniem jest pozyskanie w pierwszej kolejności danych o podmiotach lub pozyskanie bezpośrednio danych o zdarzeniach w ograniczonych pilnych przypadkach (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 6.10–6.14, zob. przypis 323).

([334]) Kodeks postępowania w zakresie danych pochodzących z łączności, pkt 8.8–8.44, zob. przypis 323.

([335]) Kodeks postępowania stanowi, że „osoba zatwierdzająca musi zachować szczególną ostrożność, rozpatrując takie wnioski, m.in. musi dodatkowo rozważyć kwestię, czy takie wnioski mogą wywoływać niezamierzone konsekwencje i czy służą one w najlepszy sposób interesowi publicznemu" (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 8.8). Ponadto należy zachowywać dokumentację dotycząca tego rodzaju wniosków, a wnioski należy przedstawić Komisarzowi ds. Uprawnień Dochodzeniowo-Śledczych w czasie kolejnej kontroli (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 8.10, zob. przypis 323).

([336]) Art. 87–89 IPA 2016.

([337]) Zgodnie z art. 90 IPA 2016 operator telekomunikacyjny, który otrzyma nakaz zatrzymywania danych, może zwrócić się do Sekretarza Stanu, który wydał taki nakaz, o jego kontrolę.

([338]) Zgodnie z sekcją 87 ust. 2 lit. a) IPA 2016 decyzja o zatrzymaniu może dotyczyć „określonego operatora bądź operatorów określonych w jakikolwiek sposób".

([339]) Cele te obejmują: (i) względy bezpieczeństwa narodowego; (ii) właściwy cel związany z przestępczością (zdefiniowany w art. 87 ust. 10A IPA 2016); (iii) interesy dobrobytu gospodarczego Zjednoczonego Królestwa w zakresie, w jakim interesy te są również istotne dla interesów bezpieczeństwa narodowego; (iv) względy bezpieczeństwa publicznego; (v) zapobiegania utracie życia lub obrażeniom ciała lub innym uszczerbkom na zdrowiu fizycznym lub psychicznym osób, lub ograniczenie wszelkich obrażeń ciała lub uszczerbków na zdrowiu fizycznym lub psychicznym osób; lub (vi) pomoc w postępowaniach przygotowawczych dotyczących domniemanych pomyłek sądowych (art. 87 IPA).

([340]) Art. 87 IPA 2016. Ponadto zgodnie z odpowiednim kodeksem postępowania do celów oceny proporcjonalności nakazu zatrzymywania danych stosuje się kryteria przewidziane w art. 2 ust. 2 IPA 2016, w szczególności wymóg oceny kwestii, czy cel, któremu służy nakaz, można osiągnąć za pomocą mniej inwazyjnych środków. Podobnie jak w przypadku oceny proporcjonalności pozyskiwania danych pochodzących z łączności w kodeksie postępowania w zakresie danych pochodzących z łączności wyjaśniono, że taka ocena obejmuje ustalenie, czy stopień ingerencji w prawa danej osoby fizycznej do poszanowania jej życia prywatnego jest proporcjonalny do wynikającej z niej korzyści dla danego postępowania przygotowawczego (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 16.3, zob. przypis 323).

samej IPA 2016 ([341]), przed wydaniem nakazu zatrzymywania danych Sekretarz Stanu musi rozważyć: prawdopodobne korzyści wynikające z takiego nakazu ([342]); opis danych usług telekomunikacyjnych; kwestię, czy należy ograniczyć zatrzymywane dane poprzez odniesienie do lokalizacji lub opisów osób, na których rzecz świadczone są dane usługi telekomunikacyjne ([343]); prawdopodobną liczbę użytkowników (jeżeli jest znana) każdej usługi telekomunikacyjnej, do której odnosi się dany nakaz ([344]); kwestię, czy nakaz jest wykonalny z technicznego punktu widzenia; prawdopodobny koszt wykonania nakazu oraz wszelki inny wpływ nakazu na operatora telekomunikacyjnego (lub opis operatorów), którego dotyczy nakaz ([345]). Zgodnie z dalszymi przepisami zawartymi w rozdziale 17 kodeksu postępowania w zakresie danych pochodzących z łączności we wszystkich nakazach zatrzymywania danych należy określić każdy rodzaj zatrzymywanych danych oraz wyjaśnić, dlatego zatrzymywanie danego rodzaju danych jest niezbędne.

(209) We wszystkich przypadkach (zarówno do celów bezpieczeństwa narodowego, jak i do celów egzekwowania prawa) decyzja Sekretarza Stanu o wydaniu nakazu zatrzymania musi zostać zatwierdzona w ramach tzw. procedury dwustopniowej autoryzacji nakazów przez niezależnego komisarza sądowego, który musi w szczególności sprawdzić, czy powiadomienie o zatrzymaniu odpowiednich danych pochodzących z łączności jest konieczne i proporcjonalne do określonego celu ustawowego lub celów ustawowych ([346]).

3.3.1.1.3. Ingerencja w urządzenia elektroniczne

(210) Ingerencja w urządzenia elektroniczne oznacza szereg technik stosowanych w celu uzyskania różnego rodzaju danych z urządzeń ([347]), w tym z komputerów, tabletów i smartfonów, a także kabli, przewodów i urządzeń pamięciowych ([348]). Ingerencja w urządzenia elektroniczne umożliwia uzyskanie zarówno treści komunikacji, jak i danych o urządzeniach ([349]).

(211) Zgodnie z art. 13 ust. 1 IPA 2016, aby służby wywiadowcze mogły ingerować w urządzenia elektroniczne, muszą one uzyskać zezwolenie w postaci nakazu wydanego w procedurze dwustopniowej autoryzacji nakazów ustanowionej w tejże ustawie, a także musi występować „związek z Wyspami Brytyjskimi" ([350]). Zgodnie z wyjaśnieniami przedstawionymi przez władze Zjednoczonego Królestwa – w sytuacjach, w których dane przekazuje się z Unii

([341]) Zob. art. 88 IPA 2016.

([342]) Może chodzić o istniejące już lub przewidywane korzyści, które muszą być zgodne z ustawowymi celami umożliwiającymi zatrzymywanie danych (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 17.17, zob. przypis 323).

([343]) Dotyczy to ustalenia, czy pełen zasięg geograficzny nakazu zatrzymywania danych jest niezbędny i proporcjonalny, oraz czy niezbędne i proporcjonalne jest uwzględnienie lub wykluczenie konkretnych opisów osób (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 17.17, zob. przypis 323).

([344]) W ten sposób Sekretarzowi Stanu łatwiej jest ocenić zarówno poziom ingerencji w prywatność konsumentów, jak i prawdopodobne korzyści wynikające z zatrzymywania danych (kodeks postępowania w zakresie danych pochodzących z łączności, pkt 17.17, zob. przypis 323).

([345]) Art. 88 IPA 2016.

([346]) Art. 89 IPA 2016.

([347]) Zgodnie z art. 135 ust. 1 i art. 198 ust. 1 IPA 2016 „urządzenia" oznaczają urządzenia generujące fale elektromagnetyczne, fale dźwiękowe lub inne emisje oraz każdy sprzęt, który można wykorzystać w połączeniu z takimi urządzeniami.

([348]) Kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, pkt 2.2.

([349]) Dane o urządzeniach zdefiniowano w art. 100 IPA 2016 jako dane systemowe i dane, które a) są zawarte lub uwzględnione w komunikacji (niekoniecznie ze strony nadawcy) lub dowolnej innej informacji, dołączone do takiej komunikacji lub informacji, lub też w sposób logiczny z nią powiązaney; b) można logicznie oddzielić od pozostałej części komunikacji lub informacji oraz c) w przypadku takiego oddzielenia nie ujawniłyby niczego z treści, którą można by racjonalnie uznać za (ewentualne) znaczenie komunikacji lub informacji.

([350]) Zgodnie z art. 13 ust. 1 IPA 2016, aby spełnienie wymogu posiadania nakazu było konieczne, postępowanie służb wywiadowczych musi nosić znamiona co najmniej jednego czynu zabronionego na mocy art. 1–3A ustawy z 1990 r. o niewłaściwym użyciu komputerów, który to wymóg byłby spełniony w zdecydowanej większości przypadków; zob. kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, pkt 3.32 i 3.6–3.9). Zgodnie z art. 13 ust. 2 IPA 2016 „związek z Wyspami Brytyjskimi" zachodzi, jeżeli a) jakiekolwiek działanie miałoby miejsce na terytorium Wysp Brytyjskich (niezależnie od lokalizacji urządzeń, które stanowiłyby lub mogłyby stanowić przedmiot ingerencji), b) służby wywiadowcze uważają, że którekolwiek z urządzeń, które stanowiłyby lub mogłyby stanowić przedmiot ingerencji, znajdowałyby się lub mogłyby się znajdować na terytorium Wysp Brytyjskich w którymkolwiek momencie w czasie trwania ingerencji, lub c) celem ingerencji jest przechwycenie (i) komunikacji przesłanej przez osobę lub do osoby, która faktycznie lub zdaniem służb wywiadowczych przebywa w danym czasie na terytorium Wysp Brytyjskich, (ii) prywatnych informacji dotyczących osoby fizycznej, która faktycznie lub zdaniem służb wywiadowczych przebywa w danym czasie na terytorium Wysp Brytyjskich, lub (iii) danych o urządzeniu, które stanowią element komunikacji lub prywatnej informacji, o których mowa w ppkt (i) lub (ii), lub które są związane z taką komunikacją lub prywatną informacją.

Europejskiej do Zjednoczonego Królestwa w zakresie stosowania niniejszej decyzji, zawsze będzie występował „związek z Wyspami Brytyjskimi", a zatem każda ingerencja w urządzenia elektroniczne obejmująca takie dane będzie podlegać wymogowi wydania obowiązkowego nakazu określonemu w art. 13 ust. 1 IPA 2016 ([351]).

(212) Przepisy dotyczące nakazów ukierunkowanej ingerencji w urządzenia elektroniczne określono w części 5 IPA 2016. Podobnie jak ukierunkowane przechwytywanie, ukierunkowana ingerencja w urządzenia elektroniczne musi dotyczyć określonego „celu", który należy wskazać w nakazie ([352]). Wymagane informacje identyfikujące „cel" zależą od przedmiotu sprawy i rodzaju urządzeń podlegających ingerencji. W szczególności w art. 115 ust. 3 IPA określono elementy, które należy uwzględnić w nakazie (np. imię i nazwisko osoby lub nazwę organizacji, opis lokalizacji), w zależności na przykład od tego, czy ingerencja dotyczy urządzenia, które należy do konkretnej osoby, organizacji lub grupy osób, jest w jej posiadaniu lub jest przez nią wykorzystywane, lub też znajduje się w określonej lokalizacji itp. ([353]) Przesłanki wydania nakazów ukierunkowanej ingerencji w urządzenia elektroniczne zależą od organu publicznego, który kieruje wniosek o wydanie takiego nakazu ([354]).

(213) Podobnie jak w przypadku ukierunkowanego przechwytywania organ wydający nakaz musi rozważyć kwestię, czy taki środek jest niezbędny i proporcjonalny do skutku, który ma zostać osiągnięty ([355]). Ponadto taki organ powinien również rozważyć, czy istnieją zabezpieczenia dotyczące ochrony, zatrzymywania i ujawniania danych, a także „ujawnienia za granicą" ([356]) (zob. motyw 196).

(214) Nakaz musi zatwierdzić komisarz sądowy, z wyjątkiem pilnych przypadków ([357]). W pilnych przypadkach komisarz sądowy musi zostać poinformowany o wydaniu nakazu i musi zatwierdzić taki nakaz w terminie trzech dni roboczych. Jeżeli komisarz sądowy odmówi zatwierdzenia nakazu, nakaz traci moc i nie może zostać przedłużony ([358]). Ponadto komisarz sądowy jest uprawniony do żądania usunięcia wszelkich danych uzyskanych na podstawie nakazu ([359]). Fakt, że nakaz został wydany w trybie pilnym, nie ma wpływu na nadzór *ex post* (zob. motywy 244–255) ani na możliwości dochodzenia roszczeń przez osoby fizyczne (zob. motywy 260–270). Osoby fizyczne mogą w zwykłym trybie złożyć skargę do Komisarza ds. Informacji lub wnieść skargę dotyczącą niewłaściwego postępowania do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych. We wszystkich przypadkach kryterium stosowanym przez komisarza sądowego przy decyzji o zatwierdzeniu nakazu jest kryterium niezbędności i proporcjonalności stosowane w przypadku analizy wniosków o ukierunkowane przechwytywanie ([360]) (zob. motyw 192 powyżej).

---

([351]) Tytułem uzupełnienia należy zauważyć, że nawet w sytuacjach, w których nie zachodzi „związek z Wyspami Brytyjskimi" i tym samym ingerencja w urządzenia elektroniczne nie podlega obowiązkowemu wymogowi posiadania nakazu przewidzianemu w art. 13 ust. 1 IPA 2016, służba wywiadowcza planująca działanie, w odniesieniu do którego może uzyskać nakaz zezwalający na masową ingerencję w urządzenia elektroniczne, powinna uzyskiwać taki nakaz w ramach obowiązującej polityki (zob. kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, pkt 3.24). Nawet jeżeli nakaz zezwalający na ingerencję w urządzenia elektroniczne przewidziany w IPA 2016 nie jest prawnie wymagany ani nie jest uzyskiwany w ramach obowiązującej polityki, działania służb wywiadowczych podlegają szeregowi warunków i ograniczeń przewidzianych w art. 7 ustawy o służbach wywiadowczych z 1994 r. W szczególności takim warunkiem jest wymóg uzyskania zezwolenia Sekretarza Stanu, który musi mieć pewność, że żadne działanie nie wykracza poza to, co jest niezbędne dla odpowiedniego sprawowania funkcji służb wywiadowczych.

([352]) W art. 115 IPA 2016 uregulowano treść nakazu, wskazując, że musi on zawierać imię i nazwisko/nazwę lub opis osób, organizacji, miejsca lub grupy osób, które stanowią „cel", opis charakteru postępowania przygotowawczego oraz opis czynności, do których wykorzystuje się dane urządzenie. W nakazie należy także opisać rodzaj urządzenia oraz czynności, do jakich jest uprawniona osoba, która uzyskała taki nakaz.

([353]) Zob. również kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, pkt 5.7, zob. przypis 348.

([354]) Agencje bezpieczeństwa narodowego mogą ubiegać się o wydanie nakazu ingerencji w urządzenia elektroniczne, jeżeli jest to niezbędne ze względu na bezpieczeństwo narodowe, do celów wykrycia poważnego przestępstwa lub ze względu na interesy dobrobytu gospodarczego Zjednoczonego Królestwa w zakresie, w jakim interesy te są również istotne dla interesów bezpieczeństwa narodowego (art. 102–103 IPA 2016). W zależności od agencji wniosek o wydanie nakazu ingerencji w urządzenia elektroniczne można złożyć do celów ścigania przestępstw, jeżeli jest on niezbędny do wykrycia poważnego przestępstwa lub zapobieżenia mu lub do zapobieżenia utracie życia lub obrażeniom ciała lub innemu uszczerbkowi na zdrowiu fizycznym lub psychicznym osób, lub do ograniczenia wszelkich obrażeń ciała lub uszczerbku na zdrowiu fizycznym lub psychicznym osób (zob. art. 106 ust. 1 i 3 IPA 2016).

([355]) Art. 102 ust. 1 lit. IPA 2016.

([356]) Art. 129–131 IPA 2016.

([357]) Art. 109 IPA 2016.

([358]) Art. 109 ust. 4 IPA 2016.

([359]) Art. 110 ust. 3 lit. b) IPA 2016. Zgodnie z pkt 5.67 kodeksu postępowania w sprawie ingerencji w urządzenia elektroniczne pilny charakter sprawy ocenia się poprzez ustalenie, czy rozsądnie wykonalne byłoby ubieganie się o zgodę komisarza sądowego na wydanie nakazu w terminie umożliwiającym zaspokojenie potrzeb operacyjnych lub dochodzeniowych. Pilne nakazy powinny zaliczać się do jednej lub obu następujących kategorii: (i) bezpośrednie zagrożenie życia lub poważna szkoda – np. jeżeli osoba została uprowadzona i ocenia się, że jej życie jest bezpośrednio zagrożone lub (ii) ograniczona czasowo możliwość gromadzenia danych wywiadowczych lub prowadzenia dochodzenia – np. do Zjednoczonego Królestwa niebawem dotrze transport narkotyków klasy A, a organy ścigania chcą uzyskać dane sprawców poważnych przestępstw w celu dokonania aresztowań. Zob. przypis 348.

([360]) Art. 108 IPA 2016.

(215) Ponadto szczególne zabezpieczenia stosowane wobec ukierunkowanego przechwytywania mają zastosowanie również w przypadku ingerencji w urządzenia elektroniczne, jeżeli chodzi o okres obowiązywania, przedłużanie i zmianę nakazu, a także w przypadku przechwytywania komunikacji parlamentarzystów, elementów objętych prawniczą tajemnicą zawodową oraz materiałów dziennikarskich (zob. więcej informacji w motywie 193).

3.3.1.1.4. Wykonywanie uprawnień do masowego pozyskiwania danych

(216) Uprawnienia do masowego pozyskiwania danych są uregulowane w części 6 IPA 2016. Ponadto kodeksy postępowania zawierają więcej szczegółowych informacji na temat wykonywania uprawnień do masowego pozyskiwania danych. Chociaż w prawie Zjednoczonego Królestwa nie określono definicji terminu „uprawnienia do masowego pozyskiwania danych", w kontekście IPA 2016 uprawnienia te opisano jako gromadzenie i zatrzymywanie dużych ilości danych pozyskanych przez rząd różnymi środkami (tj. uprawnienia do masowego przechwytywania, masowego pozyskiwania danych, masowej ingerencji w urządzenia elektroniczne i tworzenia masowych zbiorów danych osobowych), do których to danych później organy mają dostęp. Opis ten wyjaśniono, wskazując, czym uprawnienia do masowego pozyskiwania danych nie są: uprawnienia te nie są równoważne z „masową inwigilacją", która nie podlega ograniczeniom ani zabezpieczeniom. Wręcz przeciwnie, jak wyjaśniono poniżej, uprawnienia te podlegają ograniczeniom i zabezpieczeniom mającym na celu zapewnienie, aby nie udzielano powszechnego lub nieuzasadnionego dostępu do danych ([361]). W szczególności uprawnienia do masowego pozyskiwania danych można wykonywać wyłącznie w przypadku ustalenia związku między środkiem technicznym, który krajowa agencja wywiadowcza planuje zastosować, a celem operacyjnym, w odniesieniu do którego wystąpiono o zastosowania takiego środka.

(217) Ponadto uprawnienia do masowego pozyskiwania danych przysługują wyłącznie agencjom wywiadowczym i zawsze muszą stanowić przedmiot nakazu wydanego przez Sekretarza Stanu i zatwierdzonego przez komisarza sądowego. Dokonując wyboru środka gromadzenia danych wywiadowczych, należy rozważyć kwestię, czy dany cel można osiągnąć za pomocą „mniej inwazyjnych środków" ([362]). Takie podejście wynika z ram legislacyjnych, u których podstaw leży zasada proporcjonalności i w których tym samym przewiduje się pierwszeństwo gromadzenia ukierunkowanego nad masowym.

3.3.1.1.4.1. Masowe przechwytywanie i masowa ingerencja w urządzenia elektroniczne

(218) System masowego przechwytywania przewidziano w części 6 rozdział 1 IPA 2016, natomiast w tej samej części w rozdziale 3 uregulowano kwestię masowej ingerencji w urządzenia elektroniczne. Systemy te są zasadniczo takie same, w związku z czym warunki i dodatkowe zabezpieczenia stosowane wobec takich nakazów analizuje się łącznie.

(i) *Warunki i kryteria wydania nakazu*

(219) Zakres stosowania nakazu masowego przechwytywania komunikacji ogranicza się do przechwytywania w trakcie jej przekazywania lub odbierania przez osoby fizyczne znajdujące się poza terytorium Wysp Brytyjskich ([363]), tj. „komunikacji zagranicznej" ([364]), a także do innych istotnych danych i późniejszego wyboru do

([361]) Zgodnie ze sprawozdaniem dotyczącym uprawnień do masowego pozyskiwania danych przedstawionym przez lorda Davida Andersona, który dokonał niezależnego przeglądu przepisów dotyczących terroryzmu przed zatwierdzeniem IPA 2016, „nie może być wątpliwości, że masowe gromadzenie i zatrzymywanie danych nie stanowi tak zwanej masowej inwigilacji. *Każdy system prawny godny tego miana będzie obejmował ograniczenia i zabezpieczenia mające konkretnie na celu zapewnienie, aby nie udzielano powszechnego lub nieuzasadnionego dostępu do zbiorów danych wrażliwych (...)*. Takie ograniczenia i zabezpieczenia bez wątpienia zapewniono w przedmiotowym projekcie ustawy". Lord David Anderson, sprawozdanie z przeglądu uprawnień do masowego pozyskiwania danych, sierpień 2016 r., pkt 1.9 (dodano podkreślenie), dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) Art. 2 ust. 2 IPA 2016. Zob. na przykład kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, pkt 4.11, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) Na „Wyspy Brytyjskie" składają się: Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej, Wyspy Normandzkie i Wyspa Man, zgodnie z definicją zawartą w załączniku 1 do ustawy interpretacyjnej z 1978 r. – dokument dostępny pod adresem https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Zgodnie z art. 136 IPA 2016 „komunikacja zagraniczna" oznacza: (i) komunikację wysyłaną przez osoby fizyczne znajdujące się poza terytorium Wysp Brytyjskich lub (ii) komunikację odbieraną przez osoby fizyczne znajdujące się poza terytorium Wysp Brytyjskich. Jak potwierdziły władze Zjednoczonego Królestwa, system ten obejmuje również komunikację między dwiema osobami, z których obie znajdują się poza terytorium Wysp Brytyjskich. W sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (zob. przypis 279 powyżej), pkt 376, wielka izba Europejskiego Trybunału Praw Człowieka stwierdziła w odniesieniu do podobnego (odnoszącego się do „komunikacji zewnętrznej") ograniczenia przekazów, które mogą być przedmiotem masowego przechwytywania na podstawie RIPA 2000, że było ono wystarczająco ograniczone i przewidywalne.

celów analizy przechwyconego materiału ([365]). Adresat nakazu masowej ingerencji w urządzenia elektroniczne ([366]) jest uprawniony do ingerencji w dowolne urządzenie do celów pozyskania komunikacji zagranicznej (w tym wszelkich komunikatów słownych, muzycznych, dźwiękowych, obrazów lub wszelkich danych) oraz do pozyskania danych o urządzeniach (dane, które umożliwiają lub ułatwiają funkcjonowania usług pocztowych, systemu telekomunikacyjnego, usług telekomunikacyjnych) lub wszystkich innych informacji ([367]).

(220) Sekretarz Stanu może wydać nakaz masowego pozyskania danych wyłącznie na wniosek szefa służby wywiadowczej ([368]). Nakaz zatwierdzający masowe przechwytywanie lub masową ingerencję w urządzenia elektroniczne może być wydawany wyłącznie w sytuacjach, gdy jest to niezbędne dla bezpieczeństwa narodowego i do celów zapobieżenia poważnemu przestępstwu lub jego wykrycia, lub ze względu na interesy dobrobytu gospodarczego Zjednoczonego Królestwa istotne dla interesów bezpieczeństwa narodowego ([369]). Ponadto art. 142 ust. 7 IPA 2016 stanowi, że w nakazie masowego przechwytywania należy podać bardziej szczegółowe informacje, nieograniczające się wyłącznie do stwierdzenia, że służy on „interesom bezpieczeństwa narodowego", „interesom dobrobytu gospodarczego Zjednoczonego Królestwa" i „zapobieżeniu poważnemu przestępstwu i jego zwalczeniu", i należy ustalić związek między środkiem, którego dotyczy wniosek, a celem lub celami operacyjnymi, które należy wskazać w nakazie.

(221) Cel operacyjny wybiera się w drodze wielopoziomowego procesu. W art. 142 ust. 4 wskazano, że cele operacyjne wskazane w nakazie muszą być tożsame z celami, które w wykazie prowadzonym przez szefów służb wywiadowczych zostały przez nich określone jako cele operacyjne, na potrzeby których przechwycone treści lub dane wtórne uzyskane na podstawie nakazów masowego przechwytywania mogą zostać wybrane do zbadania. Wykaz celów operacyjnych musi zostać zatwierdzony przez Sekretarza Stanu. Sekretarz Stanu może dokonać takiego zatwierdzenia wyłącznie wówczas, gdy ma pewność, że w opisie celu operacyjnego podano więcej szczegółów nieograniczających się do wskazania ogólnych podstaw do zatwierdzenia nakazu (którymi są: bezpieczeństwo narodowe lub bezpieczeństwo narodowe i dobrobyt gospodarczy lub zapobieżenie poważnemu przestępstwu) ([370]). Na koniec każdego odpowiedniego trzymiesięcznego okresu Sekretarz Stanu musi przekazać egzemplarz wykazu celów operacyjnych parlamentarnej Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa. Ponadto premier musi dokonać przeglądu wykazu celów operacyjnych przynajmniej raz w roku ([371]). Jak odnotował Wysoki Trybunał, „[n]ie należy traktować tych zabezpieczeń jako mało ważne, gdyż łącznie tworzą one złożony zestaw trybów odpowiedzialności obejmujących parlament i członków rządu na najwyższych szczeblach" ([372]).

(222) W ramach takich celów operacyjnych ogranicza się również wybór przechwyconego materiału, który ma zostać zbadany. To, które spośród wszelkich materiałów zgromadzonych na podstawie nakazu masowego pozyskania danych zostaną wybrane do zbadania, musi być uzasadnione celami operacyjnymi. Jak wyjaśniły władze Zjednoczonego Królestwa, oznacza to, że praktyczne ustalenia dotyczące badania muszą zostać ocenione przez Sekretarza Stanu już na etapie wydania nakazu, przy czym należy zapewnić poziom szczegółowości wystarczający do spełnienia obowiązków ustawowych określonych w art. 152 i 193 IPA 2016 ([373]). Szczegółowe informacje udzielone Sekretarzowi Stanu w odniesieniu do tych ustaleń muszą obejmować na przykład (w stosownych przypadkach) informacje na temat stopnia, w jakim ustalenia dotyczące filtrowania mogą się różnić w czasie obowiązywania nakazu ([374]). Aby uzyskać więcej informacji na temat tego procesu i zabezpieczeń stosowanych na etapie filtrowania i badania, zob. motyw 229 poniżej.

---

([365]) Art. 136 ust. 4 IPA 2016. Z wyjaśnień otrzymanych od rządu Zjednoczonego Królestwa wynika, że masowe przechwytywanie można stosować na przykład w celu identyfikacji wcześniej nieznanych zagrożeń dla bezpieczeństwa narodowego Zjednoczonego Królestwa poprzez filtrowanie i analizowanie przechwyconego materiału w celu identyfikacji komunikacji o znaczeniu wywiadowczym (ramy wyjaśniające Zjednoczonego Królestwa, sekcja H: Bezpieczeństwo narodowe, s. 27–28, zob. przypis 29). Zgodnie z wyjaśnieniami władz Zjednoczonego Królestwa takie instrumenty można wykorzystywać do ustalenia związku między znanymi osobami podejrzanymi, a także do poszukiwania śladów działalności osób fizycznych, które mogą jeszcze nie być znane, ale które mogą pojawić się w toku postępowania przygotowawczego, oraz do identyfikacji wzorców działalności, które mogą wskazywać na istnienie zagrożenia dla Zjednoczonego Królestwa.

([366]) Zgodnie z art. 13 ust. 1 IPA 2016, aby służby wywiadowcze mogły ingerować w urządzenia elektroniczne, muszą one uzyskać zezwolenie w postaci nakazu wydanego na podstawie IPA 2016, a także musi występować „związek z Wyspami Brytyjskimi" – zob. motyw 211.

([367]) Art. 176 IPA 2016. Na mocy nakazu masowej ingerencji w urządzenia elektroniczne nie można zezwolić na działania, które – o ile nie są prowadzone na podstawie zgodnego z prawem upoważnienia – stanowiłyby bezprawne przechwytywanie (nie dotyczy to komunikacji przechowywanej). Zgodnie z ramami wyjaśniającymi Zjednoczonego Królestwa pozyskane informacje mogą być niezbędne do identyfikacji osób podejrzewanych i zazwyczaj stanowiłyby odpowiednie operacje prowadzone na dużą skalę (ramy wyjaśniające Zjednoczonego Królestwa, sekcja H: Bezpieczeństwo narodowe, s. 28, zob. przypis 29).

([368]) Art. 138 ust. 1 i art. 178 ust. 1 IPA 2016.

([369]) Art. 138 ust. 2 i art. 178 ust. 2 IPA 2016.

([370]) Zgodnie z wyjaśnieniami przedstawionymi przez władze Zjednoczonego Królestwa przykładowo w ramach celu operacyjnego zastosowanie danego środka może ograniczać się do zagrożenia istniejącego na określonym obszarze geograficznym.

([371]) Art. 142 ust. 4–10 IPA 2016.

([372]) Wysoki Trybunał, Liberty, [2019] EWHC 2057 (Admin), pkt 167.

([373]) Zgodnie z wymogami art. 152 i 193 IPA 2016: a) wyboru materiału do zbadania dokonuje się wyłącznie do celów operacyjnych określonych w nakazie, b) materiał wybrany do zbadania jest niezbędny i proporcjonalny we wszystkich okolicznościach oraz c) wybierając materiał do zbadania, nie złamano zakazu wyboru materiałów i identyfikacji komunikatów przesłanych osobom fizycznym, co do których wiadomo, że w danym czasie przebywają na terytorium Wysp Brytyjskich, lub przeznaczonych dla takich osób.

([374]) Zob. kodeks postępowania w zakresie przechwytywania komunikacji, pkt 6.6, zob. przypis 278.

(223) Na wykonanie uprawnień do masowego pozyskiwania danych można zezwolić wyłącznie wówczas, gdy jest to proporcjonalne do celu, któremu służy ([375]). Jak określono w kodeksie postępowania w zakresie przechwytywania, każda ocena proporcjonalności musi obejmować „wyważenie stopnia ingerencji w prywatność (i innych względów określonych w art. 2 ust. 2) w stosunku do potrzeby prowadzenia działań pod względem dochodzeniowym, operacyjnym lub w zakresie zdolności. Czynności objęte zezwoleniem powinny dawać realistyczną perspektywę uzyskania oczekiwanej korzyści i nie powinny być nieproporcjonalne lub arbitralne" ([376]). Jak już stwierdzono, w praktyce oznacza to, że analiza proporcjonalności opiera się na wyważeniu skutku, który ma być osiągnięty („cele operacyjne"), dostępnych wariantów technicznych (np. ukierunkowane lub masowe przechwytywanie, ingerencja w urządzenia elektroniczne, pozyskiwanie danych pochodzących z łączności), przy czym preferencyjnie należy traktować środki najmniej inwazyjne (zob. motywy 181 i 182 powyżej). Jeżeli dany cel można osiągnąć za pomocą więcej niż jednego środka, należy wybrać środek mniej inwazyjny.

(224) W kontekście oceny proporcjonalności środka wskazanego we wniosku dodatkowym zabezpieczeniem jest fakt, że Sekretarz Stanu musi otrzymać istotne informacje potrzebne mu do właściwego przeprowadzenia oceny. W szczególności kodeks postępowania w zakresie przechwytywania komunikacji i kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne zawierają wymóg, aby we wniosku składanym przez odpowiedni organ przedstawić kontekst wniosku, opis przechwytywanej komunikacji oraz operatorów telekomunikacyjnych, którzy będą musieli udzielić pomocy, opis zatwierdzonych czynności, cele operacyjne i wyjaśnienie powodów, dla których dane działanie jest niezbędne i proporcjonalne ([377]).

(225) Istotny jest wreszcie fakt, że decyzję Sekretarza Stanu o wydaniu nakazu musi zatwierdzić niezależny komisarz sądowy, który poddaje ocenę niezbędności i proporcjonalności proponowanego środka własnej ocenie, kierując się tymi samymi zasadami, które zastosowałby sąd w toku kontroli sądowej ([378]). Ściślej mówiąc, komisarz sądowy dokona przeglądu wniosków Sekretarza Stanu w kwestii, czy nakaz jest niezbędny oraz czy działania są proporcjonalne w świetle zasad określonych w art. 2 ust. 2 IPA 2016 (ogólne obowiązki w związku z ochroną prywatności). Komisarz sądowy dokona przeglądu wniosków Sekretarza Stanu pod kątem tego, czy dla każdego z celów operacyjnych określonych w nakazie wybór określonego materiału jest lub może być niezbędny. Jeżeli komisarz sądowy odmówi zatwierdzenia decyzji o wydaniu nakazu, Sekretarz Stanu może: (i) przyjąć taką decyzję i tym samym zrezygnować z wydania nakazu; albo (ii) przekazać sprawę do rozstrzygnięcia przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych (chyba że pierwotną decyzję wydał Komisarz ds. Uprawnień Dochodzeniowo-Śledczych) ([379]).

(ii) *Dodatkowe zabezpieczenia*

(226) W IPA 2016 określono dalsze ograniczenia dotyczące okresu obowiązywania, przedłużania i zmiany nakazów masowego pozyskania danych. Okres obowiązywania nakazu nie może przekraczać sześciu miesięcy, a każda decyzja o jego przedłużeniu lub zmianie (z wyjątkiem nieznacznych zmian) również podlega obowiązkowi zatwierdzenia przez komisarza sądowego ([380]). W kodeksie postępowania w zakresie przechwytywania komunikacji i kodeksie postępowania w zakresie ingerencji w urządzenia elektroniczne stwierdzono, że zmianę celów operacyjnych określonych w nakazie uznaje się za istotną zmianę nakazu ([381]).

([375]) Art. 138 ust. 1 lit. b) i c) oraz art. 178 lit. b) i c) IPA 2016.

([376]) Kodeks postępowania w zakresie przechwytywania komunikacji, pkt 4.10, zob. przypis 278.

([377]) Kodeks postępowania w zakres przechwytywania komunikacji, pkt 6.20, zob. przypis 278, oraz kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, pkt 6.13, zob. przypis 348.

([378]) Art. 138 ust. 1 lit. g) i art. 178 ust. 1 lit. f) IPA 2016. Europejski Trybunał Praw Człowieka uznał w szczególności, że uprzednia zgoda niezależnego organu stanowi ważne zabezpieczenie przed nadużyciami w kontekście masowego przechwytywania. Europejski Trybunał Praw Człowieka (wielka izba), Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu, (zob. przypis 269 powyżej), pkt 351 i 352. Należy pamiętać, że wyrok ten dotyczył poprzednich ram prawnych (RIPA 2000), które nie przewidywały niektórych zabezpieczeń (w tym uprzedniej zgody niezależnego komisarza sądowego), wprowadzonych przez IPA 2016.

([379]) Art. 159 ust. 3 i 4 IPA 2016.

([380]) Art. 143–146 i 184–188 IPA 2016. W przypadku pilnej zmiany Sekretarz Stanu może dokonać takiej zmiany bez zatwierdzenia, ale musi powiadomić o niej komisarza, który z kolei musi podjąć decyzję o jej przyjęciu albo odrzuceniu (art. 147 IPA 2016). Nakaz należy unieważnić, jeżeli nie jest już niezbędny lub proporcjonalny, lub jeżeli badanie przechwyconych treści, metadanych lub innego rodzaju danych uzyskanych na podstawie danego nakazu nie jest już niezbędne do osiągnięcia celów operacyjnych określonych w tym nakazie (art. 148 i 189 IPA 2016).

([381]) Kodeks postępowania w zakres przechwytywania komunikacji, pkt 6.44–6.47, zob. przypis 278, oraz kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, pkt 6.48, zob. przypis 348.

(227) Podobnie jak w przypadku zasad dotyczących ukierunkowanego przechwytywania, w części 6 IPA 2016 określono, że Sekretarz Stanu musi zapewnić, aby obowiązywały ustalenia zapewniające zabezpieczenia w zakresie zatrzymywania i ujawniania materiałów uzyskanych na podstawie nakazu ([382]), a także w odniesieniu do ujawniania za granicą ([383]). W szczególności w art. 150 ust. 5 i art. 191 ust. 5 IPA 2016 wymaga się, aby każdą kopię wszelkich materiałów zebranych na podstawie nakazu przechowywano w bezpieczny sposób i niszczono, gdy tylko nie ma już istotnych podstaw do jej zatrzymywania, natomiast w art. 150 ust. 2 i art. 191 ust. 2 wymaga się, aby liczba osób, którym ujawnia się materiał, oraz zakres, w jakim dany materiał jest ujawniany, udostępniany lub kopiowany, były ograniczone do minimum niezbędnego do realizacji celów ustawowych ([384]).

(228) Ponadto gdy materiał, który przechwycono w ramach masowego przechwytywania albo masowej ingerencji w urządzenia elektroniczne, ma zostać przekazany do państwa trzeciego („ujawnienia za granicą"), w IPA 2016 przewiduje się, że Sekretarz Stanu musi zapewnić, aby istniały odpowiednie ustalenia w celu zapewnienia istnienia podobnych zabezpieczeń dotyczących bezpieczeństwa, zatrzymywania i ujawniania w danym państwie trzecim ([385]). Ponadto w art. 109 DPA 2018 określono szczegółowe wymogi dotyczące międzynarodowego przekazywania danych osobowych przez służby wywiadowcze do państw trzecich lub organizacji międzynarodowych. Zgodnie z tym przepisem dane nie mogą być przekazywane do państwa ani terytorium poza Zjednoczonym Królestwem ani do organizacji międzynarodowej, chyba że przekazanie jest niezbędne i proporcjonalne do celów wykonywania ustawowych funkcji administratora lub do innych celów przewidzianych w art. 2 ust. 2 lit. a) ustawy o Służbie Bezpieczeństwa z 1989 r. lub art. 2 ust. 2 lit. a) i art. 4 ust. 2 lit. a) ustawy o służbach wywiadowczych z 1994 r. ([386]). Co ważne, wymogi te mają również zastosowanie w przypadkach, w których powołano się na wyłączenie ze względów bezpieczeństwa narodowego zgodnie z art. 110 DPA 2018, ponieważ w art. 110 DPA 2018 nie wymieniono art. 109 DPA 2018 jako jednego z przepisów, od których można odstąpić, jeżeli do celów ochrony bezpieczeństwa narodowego wymagane jest wyłączenie niektórych przepisów.

(229) Po zatwierdzeniu nakazu i masowym zgromadzeniu danych dokonuje się wyboru danych do zbadania. Etap wyboru i badania podlega dalszej analizie proporcjonalności prowadzonej przez analityka, który definiuje kryteria wyboru na podstawie celów operacyjnych wskazanych w nakazie (i ewentualnych przyjętych ustaleń dotyczących filtrowania). Jak określono w art. 152 i 193 IPA, wydając nakaz, Sekretarz Stanu musi zapewnić obowiązywanie ustaleń gwarantujących, aby wyboru materiałów dokonywano wyłącznie w odniesieniu do określonych celów operacyjnych oraz aby wybrane materiały były niezbędne i proporcjonalne we wszystkich okolicznościach. W tym kontekście władze Zjednoczonego Królestwa wyjaśniły, że materiały podlegające masowemu przechwytywaniu wybiera się przede wszystkim za pomocą automatycznego filtrowania służącego odrzuceniu danych, co do których nie jest prawdopodobne, aby były one istotne dla bezpieczeństwa narodowego. Dobór filtrów może ulegać zmianie (wraz ze zmianą wzorców, rodzajów i protokołów ruchu internetowego) w zależności od technologii i kontekstu operacyjnego. Na tym etapie dane można wybrać do zbadania wyłącznie wówczas, gdy są one odpowiednie do celów operacyjnych wskazanych w nakazie ([387]). Zabezpieczenia przewidziane w IPA 2016 w odniesieniu do badania zebranych materiałów mają zastosowanie do wszelkiego rodzaju danych (zarówno przechwyconych treści, jak i danych wtórnych) ([388]). W art. 152 i 193 IPA 2016 przewidziano również ogólny zakaz wyboru do zbadania materiałów odnoszących się do rozmów, w przypadku których nadawcami lub zamierzonymi odbiorcami są osoby fizyczne znajdujące się na terytorium Wysp Brytyjskich. Jeżeli organy zamierzają zbadać takie materiały, składają wniosek o nakaz ukierunkowanego zbadania na podstawie części 2 i 4 IPA 2016 wydawany przez Sekretarza Stanu i zatwierdzany przez komisarza sądowego ([389]). Osoba, która celowo wybiera do zbadania przechwycone treści niezgodnie z wymogami określonymi w przepisach ([390]), dopuszcza się czynu zabronionego ([391]).

([382]) Art. 156 IPA 2016.
([383]) Art. 150 i 191 IPA 2016.
([384]) Wielka izba Europejskiego Trybunału Praw Człowieka w wyroku w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (zob. przypis 268 powyżej) utrzymała system dodatkowych zabezpieczeń dotyczących zatrzymywania informacji, dostępu do nich i ich ujawniania, przewidziany w RIPA 2000, zob. pkt 392–394 i 402–405. Ten sam system zabezpieczeń przewidziano w IPA 2016.
([385]) Art. 151 i 192 IPA 2016.
([386]) Więcej informacji na ten temat w przypisie 312.
([387]) W tym kontekście kodeks w zakresie przechwytywania komunikacji stanowi, że „[t]akie systemy przetwarzania obejmują przetwarzanie danych z połączeń lub sygnałów komunikacyjnych, które organ przechwytujący wybrał do przechwycenia. Następnie stosuje się pewien stopień filtrowania ruchu na tych połączeniach i sygnałach w celu wyboru rodzajów komunikacji, które potencjalnie są istotne do celów wywiadowczych, i odrzucenia rodzajów komunikacji, w przypadku których prawdopodobieństwo znaczenia wywiadowczego jest najmniejsze. W wyniku takiego filtrowania, które różni się w zależności od systemu przetwarzania, automatycznie odrzuca się znaczną część komunikacji na tych połączeniach i sygnałach. Następnie można prowadzić złożone operacje przeglądania danych, aby dokonać dalszej selekcji przekazów, które najprawdopodobniej mają największe znaczenie wywiadowcze w kontekście ustawowych funkcji danej agencji. Taki przekaz następnie wybiera się do zbadania pod kątem celu lub celów operacyjnych określonych w nakazie, pod warunkiem że spełnione są warunki niezbędności i proporcjonalności. Do zbadania przez upoważnione osoby można potencjalnie wybrać wyłącznie elementy, które nie zostały odrzucone w procesie filtrowania" (kodeks postępowania w zakresie przechwytywania komunikacji, pkt 6.6, zob. przypis 278).
([388]) Zob. art. 152 ust. 1 lit. a) i b) IPA 2016, zgodnie z którym badanie obu rodzajów danych (przechwyconych treści i danych wtórnych) musi być przeprowadzone wyłącznie w określonym celu oraz musi być konieczne i proporcjonalne we wszystkich okolicznościach.
([389]) Tego rodzaju nakaz nie jest wymagany, jeżeli dane dotyczące osób przebywających na terytorium Wysp Brytyjskich są „danymi wtórnymi" (zob. sekcja 152 ust. 1 lit. c) IPA 2016).
([390]) Art. 152 i 193 IPA 2016.
([391]) Art. 155 i 196 IPA 2016.

(230) Przeprowadzona przez analityka ocena wybranych materiałów podlega nadzorowi *ex post* sprawowanemu przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych, który ocenia zgodność z konkretnymi zabezpieczeniami określonymi w IPA 2016 w odniesieniu do etapu badania ([392]) (zob. również motyw 229). Komisarz ds. Uprawnień Dochodzeniowo-Śledczych musi kontrolować (w tym w drodze audytu, inspekcji i badania) wykonanie przez organy publiczne uprawnień dochodzeniowo-śledczych wymienionych w IPA 2016 ([393]). W tym kontekście w kodeksie postępowania w zakresie przechwytywania i kodeksie postępowania w zakresie ingerencji w urządzenia elektroniczne wyjaśniono, że dana agencja musi prowadzić dokumentację do celów badania i audytów na późniejszym etapie, a w takiej dokumentacji należy wskazać powody, dla których udostępnienie danych materiałów upoważnionym osobom jest niezbędne i proporcjonalne, oraz mające zastosowanie cele operacyjne ([394]). Na przykład w sprawozdaniu rocznym z 2018 r. Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych ([395]) ustaliło, że udokumentowane przez analityków powody uzasadniające zbadanie określonych materiałów gromadzonych masowo spełniały wymaganą normę proporcjonalności, gdyż przedstawiono wystarczająco szczegółowe uzasadnienie „zapytań" w stosunku do wyznaczonego celu ([396]). W swoim sprawozdaniu z 2019 r. Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych wyraźnie zaznaczyło w odniesieniu do uprawnień do masowego pozyskiwania danych swój zamiar kontynuowania kontroli przechwyceń masowych, w tym szczegółową analizę selektorów i kryteriów wyszukiwania ([397]). Biuro będzie również nadal uważnie analizować, indywidualnie dla każdego przypadku, wybór środków nadzoru (ukierunkowanych i masowych) zarówno w ramach rozpatrywania wniosków o wydanie nakazu w procedurze dwustopniowej autoryzacji, jak i w ramach kontroli ([398]). To dalsze monitorowanie zostanie należycie uwzględnione w kontekście monitorowania przez Komisję niniejszej decyzji, o którym mowa w motywach 281–284.

3.3.1.1.4.2. Masowe pozyskiwanie danych pochodzących z łączności

(231) W części 6 rozdział 2 IPA 2016 uregulowano nakazy masowego pozyskania danych, które to nakazy upoważniają adresata do żądania od operatora telekomunikacyjnego ujawnienia lub uzyskania wszelkich danych pochodzących z łączności będących w posiadaniu operatora. Nakazy te upoważniają również organ wnioskujący do wyboru danych do dalszego etapu badania. Podobnie jak w przypadku ukierunkowanego zatrzymywania i pozyskiwania danych pochodzących z łączności (zob. motyw 199), również masowe pozyskiwanie danych pochodzących z łączności nie dotyczy zazwyczaj danych osobowych osób z UE, które to dane są przekazywane na podstawie niniejszej decyzji do Zjednoczonego Królestwa. Obowiązek ujawnienia danych pochodzących z łączności zgodnie z częścią 6 rozdział 2 IPA 2016 obejmuje dane, które są zbierane przez operatorów telekomunikacyjnych w Zjednoczonym Królestwie bezpośrednio od użytkowników usługi telekomunikacyjnej ([399]). Ten rodzaj przetwarzania „widoczny dla klienta" zazwyczaj nie wiąże się z przekazywaniem na podstawie niniejszej decyzji, tj. przekazywaniem od administratora lub podmiotu przetwarzającego w UE do administratora lub podmiotu przetwarzającego w Zjednoczonym Królestwie.

(232) Niemniej dla pełnego obrazu sytuacji poniżej opisano warunki i zabezpieczenia regulujące pozyskiwanie masowych danych pochodzących z łączności.

([392]) Art. 152 i 193 IPA 2016.
([393]) Art. 229 IPA 2016.
([394]) Kodeks postępowania w zakres przechwytywania komunikacji, pkt 6.74, zob. przypis 278, oraz kodeks postępowania w zakresie ingerencji w urządzenia elektroniczne, pkt 6.78, zob. przypis 348.
([395]) Na podstawie art. 238 IPA 2016 Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych ma zapewniać Komisarzowi ds. Uprawnień Dochodzeniowo-Śledczych niezbędny personel, pomieszczenia, wyposażenie oraz inne urządzenia i usługi niezbędne do pełnienia jego funkcji (zob. motyw 251).
([396]) W sprawozdaniu rocznym Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2018 r. wskazano, że uzasadnienia udokumentowane przez analityków GCHQ „spełniały wymaganą normę, a analitycy wystarczająco szczegółowo udokumentowali proporcjonalność ich zapytań odnoszących się do danych masowych". Sprawozdanie roczne Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2018 r., pkt 6.22, zob. przypis 464.
([397]) Zob. sprawozdanie roczne Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r., pkt 7.6, zob. przypis 463.
([398]) Zob. sprawozdanie roczne Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r., pkt 10.22, zob. przypis 463.
([399]) Wynika to z definicji terminu „dane pochodzące z łączności" zawartej w art. 261 ust. 5 IPA 2016, zgodnie z którą dane pochodzące z łączności są przechowywane lub uzyskiwane przez operatora telekomunikacyjnego i dotyczą użytkownika usługi telekomunikacyjnej oraz są związane ze świadczeniem tej usługi albo są elementem komunikacji, są jej częścią, towarzyszą jej lub są z nią logicznie powiązane (zob. również kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf pkt 2.15–2.22). Ponadto zgodnie z definicją terminu „operator telekomunikacyjny" zawartą w art. 261 ust. 10 IPA 2016 wymaga się, aby operatorem telekomunikacyjnym była osoba, która oferuje lub świadczy usługi telekomunikacyjne osobom w Zjednoczonym Królestwie lub która kontroluje lub zapewnia system telekomunikacyjny, który znajduje się (w całości lub częściowo) w Zjednoczonym Królestwie lub jest kontrolowany ze Zjednoczonego Królestwa. Definicje te jasno wskazują, że obowiązki wynikające z IPA 2016 nie mogą być nakładane na operatorów telekomunikacyjnych, których urządzenia nie znajdują się w Zjednoczonym Królestwie ani nie są z kontrolowane z terytorium tego państwa i którzy nie oferują ani nie świadczą usług osobom fizycznym w Zjednoczonym Królestwie (zob. również kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, pkt 2.2). W przypadku abonentów z UE (czy to znajdujących się w UE, czy w Zjednoczonym Królestwie) korzystających z usług w Zjednoczonym Królestwie wszelkie informacje związane ze świadczeniem tych usług byłyby gromadzone bezpośrednio przez dostawcę usług w Zjednoczonym Królestwie, nie byłyby natomiast przekazywane z UE.

(233) IPA 2016 zastępuje przepisy dotyczące pozyskiwania masowych danych pochodzących z łączności, które były przedmiotem wyroku TSUE w sprawie Privacy International. Przepisy będące przedmiotem tej sprawy zostały uchylone, a nowy system przewiduje szczególne warunki i zabezpieczenia, na podstawie których można zatwierdzić taki środek.

(234) W szczególności, inaczej niż w poprzednim systemie, w ramach którego Sekretarz Stanu miał pełną swobodę uznania w zatwierdzaniu środka ([400]), IPA 2016 wymaga, aby Sekretarz Stanu wydał nakaz wyłącznie wtedy, gdy środek jest niezbędny i proporcjonalny. W praktyce oznacza to, że powinien istnieć związek między dostępem do danych a realizowanym celem ([401]). W szczególności Sekretarz Stanu musi ocenić istnienie związku między środkiem, którego dotyczy wniosek, a celem lub celami operacyjnymi wskazanymi w nakazie (zob. motyw 219) w odniesieniu do oceny proporcjonalności; właściwy kodeks postępowania stanowi, że: „Sekretarz Stanu musi wziąć pod uwagę to, czy cel, który ma zostać osiągnięty za pomocą nakazu, można osiągnąć za pomocą innych, mniej inwazyjnych środków (art. 2 ust. 2 lit. a) ustawy). Przykładem może być uzyskanie wymaganych informacji przy użyciu mniej inwazyjnych środków takich jak ukierunkowane pozyskiwanie danych pochodzących z łączności" ([402]).

(235) W celu przeprowadzenia takiej oceny Sekretarz Stanu opiera się na informacjach, które szefowie agencji wywiadowczych ([403]) zobowiązani są przedstawić w swoim wniosku, np. dotyczących powodów, dla których dany środek jest uważany za niezbędny ze względu na jedną z przesłanek ustawowych, oraz powodów, dla których zamierzonego celu nie można w racjonalny sposób osiągnąć za pomocą innych, mniej inwazyjnych środków ([404]). Ponadto cele operacyjne ograniczają zakres, w jakim dane uzyskane na podstawie nakazu można wybrać do zbadania ([405]). Jak określono we właściwym kodeksie postępowania, cele operacyjne muszą zawierać opis jasnego wymogu oraz wystarczającą liczbę informacji szczegółowych, aby upewnić Sekretarza Stanu, że uzyskane dane mogą zostać wybrane do zbadania wyłącznie ze szczególnych powodów ([406]). W praktyce przed wydaniem zezwolenia na wydanie nakazu Sekretarz Stanu będzie musiał upewnić się, że dokonano szczegółowych ustaleń w celu zagwarantowania, że do zbadania wybrane zostaną wyłącznie te materiały, które uznano za niezbędne do badania pod kątem celu operacyjnego i celu ustawowego, oraz że będą one proporcjonalne i niezbędne we wszystkich okolicznościach. Ten szczególny wymóg, odzwierciedlony w art. 158 i 172 ([407]) IPA 2016, dotyczący uprzedniej oceny niezbędności i proporcjonalności kryteriów stosowanych do celów wyboru, stanowi kolejną istotną nowość systemu wprowadzonego w IPA 2016 w porównaniu z systemem obowiązującym poprzednio.

(236) W IPA 2016 nałożono również na Sekretarza Stanu obowiązek zapewnienia, aby przed wydaniem nakazu masowego pozyskiwania danych pochodzących z łączności zostały wprowadzone określone ograniczenia w zakresie bezpieczeństwa, zatrzymywania i ujawniania zgromadzonych danych osobowych ([408]). W przypadku ujawnienia za granicą zabezpieczenia opisane w motywie 227, dotyczące masowego przechwytywania i masowej ingerencji w urządzenia elektroniczne, mają zastosowanie również w tym kontekście ([409]). Dalsze ograniczenia określono w przepisach dotyczących okresu obowiązywania ([410]), przedłużania ([411]) i zmiany nakazów masowego pozyskania danych ([412]).

(237) Co istotne, podobnie jak w przypadku pozostałych uprawnień do masowego pozyskiwania danych, przed wydaniem nakazu Sekretarz Stanu musi uzyskać zatwierdzenie przez komisarza sądowego ([413]). Jest to jedna z kluczowych cech systemu wprowadzonego na mocy IPA 2016.

([400]) Art. 94 ust. 1 ustawy o łączności z 1984 r. stanowił, że Sekretarz Stanu może wydawać „wskazówki o charakterze ogólnym, które Sekretarz Stanu uważa za wymagane lub wskazane dla interesu bezpieczeństwa narodowego (...)" (zob. przypis 451).
([401]) Zob. Privacy International, pkt 78.
([402]) Zob. kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, pkt 4.11 (zob. przypis 399414).
([403]) O nakaz masowego pozyskania danych mogą wystąpić wyłącznie szefowie służb wywiadowczych, którymi są: (i) Dyrektor Generalny Służby Bezpieczeństwa; (ii) Dyrektor Tajnej Służby Wywiadowczej lub (iii) Dyrektor GCHQ (zob. art. 158 i 263 IPA 2016).
([404]) Kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, pkt 4.5 (zob. przypis 399)
([405]) Zgodnie z art. 161 IPA 2016 cele operacyjne wskazane w nakazie muszą być tożsame z celami, które w wykazie prowadzonym przez szefów służb wywiadowczych („wykaz celów operacyjnych") zostały przez nich określone jako cele operacyjne, na potrzeby których dane pochodzące z łączności uzyskane na podstawie nakazów masowego pozyskania danych mogą zostać wybrane do zbadania.
([406]) Kodeks postępowania w zakresie masowego pozyskiwania danych pochodzących z łączności, pkt 6.6 (zob. przypis 399).
([407]) Art. 172 IPA 2016 wymaga wprowadzenia szczególnych zabezpieczeń na etapie filtrowania pozyskanych masowo danych pochodzących z łączności i ich wyboru do zbadania. Ponadto umyślne badanie z naruszeniem tych zabezpieczeń jest również przestępstwem (zob. art. 173 IPA 2016).
([408]) Art. 171 IPA 2016.
([409]) Art. 171 ust. 9 IPA 2016.
([410]) Art. 162 IPA 2016.
([411]) Art. 163 IPA 2016.
([412]) Art. 164–166 IPA 2016.
([413]) Art. 159 IPA 2016.

(238) Komisarz ds. Uprawnień Dochodzeniowo-Śledczych przeprowadza nadzór *ex post* procedury badania materiałów (danych pochodzących z łączności) uzyskanych masowo (zob. motyw 254 poniżej). W tym zakresie w IPA 2016 wprowadzono wymóg, aby przed wyborem danych do zbadania analityk wywiadu przeprowadzający badanie odnotował powód, dla którego proponowane badanie jest niezbędne i proporcjonalne dla określonego celu operacyjnego ([414]). W sprawozdaniu rocznym Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r. w odniesieniu do praktyki GCHQ i MI5 stwierdzono, że: „kluczowa rola masowych danych pochodzących z łączności dla szerokiego zakresu działań prowadzonych w GCHQ została dobrze wyartykułowana w skontrolowanych przez nas sprawach. Po przeanalizowaniu charakteru danych, o które wystąpiono, oraz wskazanych wymogów wywiadowczych na podstawie dokumentacji upewniliśmy się, że podejście GCHQ i MI5 było niezbędne i proporcjonalne ([415]). Odnotowane uzasadnienia MI5 były na dobrym poziomie i spełniały zasady niezbędności i proporcjonalności" ([416]).

3.3.1.1.4.3. Zatrzymywanie i badanie masowych zbiorów danych osobowych

(239) Nakazy dotyczące masowych zbiorów danych osobowych ([417]) upoważniają agencje wywiadowcze do zatrzymywania i badania zbiorów danych, które zawierają dane osobowe dotyczące większej liczby osób fizycznych. Zgodnie z wyjaśnieniami przedstawionymi przez władze Zjednoczonego Królestwa analiza takich zbiorów danych może być dla wspólnoty wywiadowczej Zjednoczonego Królestwa (UKIC) „jedynym sposobem na osiągnięcie postępów w dochodzeniach i identyfikację terrorystów na podstawie bardzo ograniczonych danych wywiadowczych lub w przypadku gdy komunikacja między nimi została celowo ukryta" ([418]). Istnieją dwa rodzaje nakazów: grupowe nakazy dotyczące masowych zbiorów danych osobowych (*class BPD warrants*) ([419]), które dotyczą określonej kategorii zbiorów danych, tj. zbiorów danych, które są podobne pod względem zawartości i proponowanego wykorzystania oraz wiążą się z podobnymi zagadnieniami dotyczącymi na przykład stopnia naruszenia prywatności i wrażliwości oraz proporcjonalności wykorzystania danych, co pozwala Sekretarzowi Stanu rozważyć niezbędność i proporcjonalność jednoczesnego pozyskania wszystkich danych w ramach danej kategorii. Na przykład grupowy nakaz dotyczący masowych zbiorów danych osobowych może obejmować zbiory danych o podróży, które odnoszą się do podobnych tras ([420]). Indywidualne nakazy dotyczące masowych zbiorów danych osobowych (*specific BPD warrants*) ([421]) dotyczą natomiast jednego określonego zbioru danych, takiego jak zbiór danych obejmujący nowy lub nietypowy rodzaj informacji, który nie wchodzi w zakres istniejącego grupowego nakazu dotyczącego masowych zbiorów danych osobowych, albo zbioru danych, który dotyczy określonych rodzajów danych osobowych ([422]) i w związku z tym wymaga dodatkowych zabezpieczeń ([423]). Przepisy IPA 2016 dotyczące masowych zbiorów danych osobowych pozwalają na badanie i zatrzymywanie takich zbiorów danych wyłącznie w przypadku, gdy jest to niezbędne i proporcjonalne ([424]), oraz zgodnie z ogólnymi zobowiązaniami dotyczącymi prywatności ([425]).

(240) Uprawnienia do wydawania nakazu dotyczącego masowego zbioru danych osobowych podlegają procedurze dwustopniowej autoryzacji: ocenę niezbędności i proporcjonalności środka przeprowadza najpierw Sekretarz Stanu, a następnie komisarz sądowy ([426]). Sekretarz Stanu jest zobowiązany rozważyć charakter i zakres rodzaju nakazu i kategorię danych, których dotyczy wniosek, oraz liczbę poszczególnych masowych zbiorów danych osobowych, które mogą zostać objęte danym rodzajem nakazu ([427]). Ponadto jak określono w kodeksie postępowania w zakresie zatrzymywania i wykorzystywania przez służby wywiadowcze masowych zbiorów danych osobowych, należy prowadzić szczegółową dokumentację, która podlega kontroli Komisarza ds. Uprawnień Dochodzeniowo-Śledczych ([428]). Zatrzymywanie i badanie masowych zbiorów danych osobowych wykraczające poza zakres określony w IPA 2016 jest przestępstwem ([429]).

([414]) Sprawozdanie roczne Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r., pkt 8.6, zob. przypis 463.
([415]) Sprawozdanie roczne Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r., pkt 10.4, zob. przypis 463.
([416]) Sprawozdanie roczne Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r., pkt 8.37, zob. przypis 463.
([417]) Art. 200 IPA 2016.
([418]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Bezpieczeństwo narodowe, s. 34, zob. przypis 29.
([419]) Art. 204 IPA 2016.
([420]) Kodeks postępowania w zakresie zatrzymywania i wykorzystywania przez służby wywiadowcze masowych zbiorów danych osobowych, pkt 4.7, dostępny pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) Art. 205 IPA 2016.
([422]) Takie jak na przykład wrażliwe dane osobowe, zob. art. 202 IPA 2016 oraz kodeks postępowania w zakresie zatrzymywania i wykorzystywania przez służby wywiadowcze masowych zbiorów danych osobowych, pkt 4.21 i 4.12, zob. przypis 469.
([423]) Wniosek o wydanie indywidualnego nakazu dotyczącego masowego zbioru danych osobowych musi być rozpatrywany indywidualnie przez Sekretarza Stanu, tj. w odniesieniu do jednego określonego zbioru danych. W art. 205 IPA wymaga się, aby we wniosku o wydanie indywidualnego nakazu dotyczącego masowego zbioru danych osobowych służba wywiadowcza udzieliła szczegółowych wyjaśnień dotyczących charakteru i zakresu przedmiotowego materiału oraz wykaz „celów operacyjnych", dla których odpowiednia służba wywiadowcza zamierza zbadać masowy zbiór danych osobowych (w przypadku gdy służba wywiadowcza ubiega się o nakaz dotyczący zatrzymywania i badania, a nie wyłącznie zatrzymywania). Przy wydawaniu grupowego nakazu dotyczącego masowych zbiorów danych osobowych Sekretarz rozpatruje natomiast całą kategorię zbiorów danych jednocześnie.
([424]) Art. 204 i 205 IPA 2016.
([425]) Art. 2 IPA 2016.
([426]) Art. 204 i 205 IPA 2016.
([427]) Kodeks postępowania w zakresie zatrzymywania i wykorzystywania przez służby wywiadowcze masowych zbiorów danych osobowych, pkt 5.2, zob. przypis 420.
([428]) Kodeks postępowania w zakresie zatrzymywania i wykorzystywania przez służby wywiadowcze masowych zbiorów danych osobowych, pkt 8.1–8.15, zob. przypis 420.
([429]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Bezpieczeństwo narodowe s. 34, zob. przypis 29.

3.3.2. *Dalsze wykorzystywanie zebranych informacji*

(241) Danych osobowych przetwarzanych na podstawie części 4 DPA 2018 nie można przetwarzać w sposób niezgodny z celem, dla którego zostały zebrane ([430]). DPA 2018 stanowi, że administrator może przetwarzać dane w celu innym niż ten, dla którego dane zostały zebrane, jeżeli jest on zgodny z celem pierwotnym i pod warunkiem że administrator jest upoważniony przez prawo do przetwarzania danych, a przetwarzanie jest niezbędne i proporcjonalne ([431]). Ponadto ustawa o Służbie Bezpieczeństwa z 1989 r. oraz ustawa o służbach wywiadowczych z 1994 r. stanowią, że szefowie agencji wywiadowczych mają obowiązek dopilnować, aby nie uzyskano ani nie ujawniono żadnych informacji, z wyjątkiem tych, które są niezbędne do właściwego wykonywania funkcji agencji lub do pozostałych ograniczonych i szczególnych celów wymienionych we właściwych przepisach ([432]).

(242) Ponadto w art. 109 DPA 2018 określono szczegółowe wymogi dotyczące międzynarodowego przekazywania danych osobowych przez służby wywiadowcze do państw trzecich lub organizacji międzynarodowych. Zgodnie z tym przepisem dane osobowe nie mogą być przekazywane do państwa ani terytorium poza Zjednoczonym Królestwem ani do organizacji międzynarodowej, chyba że przekazanie jest niezbędne i proporcjonalne do celów wykonywania ustawowych funkcji administratora lub do innych celów przewidzianych w art. 2 ust. 2 lit. a) ustawy o Służbie Bezpieczeństwa z 1989 r. lub art. 2 ust. 2 lit. a) i art. 4 ust. 2 lit. a) ustawy o służbach wywiadowczych z 1994 r. ([433]). Co ważne, wymogi te mają również zastosowanie w przypadkach, w których powołano się na wyłączenie ze względów bezpieczeństwa narodowego zgodnie z art. 110 DPA 2018, ponieważ w art. 110 DPA 2018 nie wymieniono art. 109 DPA 2018 jako jednego z przepisów, od których można odstąpić, jeżeli do celów ochrony bezpieczeństwa narodowego wymagane jest wyłączenie niektórych przepisów.

(243) Ponadto, jak podkreślił Komisarz ds. Informacji w swoich wytycznych dotyczących przetwarzania danych przez służby wywiadowcze, oprócz zabezpieczeń przewidzianych w części 4 DPA 2018 agencja wywiadowcza, udostępniając dane organowi wywiadowczemu państwa trzeciego, podlega również zabezpieczeniom przewidzianym w innych mających do niej zastosowanie środkach ustawodawczych w celu zapewnienia, aby dane osobowe były pozyskiwane, udostępniane i przetwarzane zgodnie z prawem i w sposób odpowiedzialny ([434]). Przykładowo w IPA 2016 określono dalsze zabezpieczenia w odniesieniu do przekazywania do państwa trzeciego materiałów zebranych w drodze ukierunkowanego przechwytywania ([435]), ukierunkowanej ingerencji w urządzenia elektroniczne ([436]), masowego przechwytywania ([437]), masowego pozyskiwania danych pochodzących z łączności ([438]) oraz masowej ingerencji w urządzenia elektroniczne ([439]) (tzw. „ujawnienia za granicą"). W szczególności organ wydający nakaz musi zapewnić, aby obowiązywały ustalenia mające na celu zagwarantowanie, że państwo trzecie otrzymujące dane ogranicza liczbę osób, które zapoznają się z materiałami, zakres ujawnienia oraz liczbę kopii wszelkich materiałów do minimum niezbędnego do osiągnięcia dozwolonych celów określonych w IPA 2016 ([440]).

3.3.3. *Nadzór*

(244) Dostęp rządowy do celów bezpieczeństwa narodowego nadzoruje szereg różnych organów. Komisarz ds. Informacji nadzoruje przetwarzanie danych osobowych w świetle DPA 2018 (więcej informacji na temat niezależności, roli związanej z powołaniem i uprawnień Komisarza znajduje się w motywach od 85 do 98), natomiast niezależny i sądowy nadzór nad korzystaniem z uprawnień dochodzeniowo-śledczych na mocy IPA 2016 sprawuje Komisarz

([430]) Art. 87 ust. 1 DPA 2018.

([431]) Art. 87 ust. 3 DPA 2018. Chociaż administratorzy mogą być wyłączeni z tej zasady na podstawie art. 110 DPA 2018 w zakresie, w jakim jest to wymagane do ochrony bezpieczeństwa narodowego, wyłączenie takie musi być oceniane w każdym przypadku z osobna i można się na nie powoływać wyłącznie w zakresie, w jakim zastosowanie określonego przepisu miałoby negatywne konsekwencje dla bezpieczeństwa narodowego (zob. motyw 132). Certyfikaty bezpieczeństwa narodowego dla służb wywiadowczych Zjednoczonego Królestwa (dostępne pod adresem: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) nie obejmują art. 87 ust. 3 DPA 2018. Ponadto, ponieważ każde przetwarzanie danych w innym celu musi być prawnie dozwolone, służby wywiadowcze muszą mieć jasną podstawę prawną do dalszego przetwarzania.

([432]) Więcej informacji na ten temat w przypisie 312.

([433]) Zob. przypis 312.

([434]) Wytyczne ICO dotyczące przetwarzania danych przez służby wywiadowcze (zob. przypis 161).

([435]) Art. 54 IPA 2016.

([436]) Art. 130 IPA 2016.

([437]) Art. 151 IPA 2016.

([438]) Art. 171 ust. 9 IPA 2016.

([439]) Art. 192 IPA 2016.

([440]) Ustalenia muszą obejmować środki zapewniające, aby każda kopia wykonana z tych materiałów była przechowywana (tak długo, jak długo jest zatrzymywana) w bezpieczny sposób. Materiały uzyskane na podstawie nakazu oraz każda wykonana z nich kopia muszą zostać zniszczone, gdy tylko przestaną istnieć uzasadnione powody do ich zachowania (zob. art. 150 ust. 2 i 5 oraz art. 151 ust. 2 IPA 2016). Warto zauważyć, że podobne gwarancje przewidziane w poprzednich ramach prawnych (RIPA 2000) zostały uznane za zgodne z wymogami określonymi przez Europejski Trybunał Praw Człowieka w odniesieniu do udostępniania obcym państwom lub organizacjom międzynarodowym materiałów uzyskanych w wyniku masowego przechwytywania [Europejski Trybunał Praw Człowieka (wielka izba), Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu, (zob. przypis 279 powyżej), pkt 362 i 399].

ds. Uprawnień Dochodzeniowo-Śledczych. Komisarz ds. Uprawnień Dochodzeniowo-Śledczych nadzoruje korzystanie z uprawnień dochodzeniowo-śledczych wynikających z IPA 2016 zarówno przez organy ścigania, jak i przez organy bezpieczeństwa narodowego. Nadzór polityczny jest gwarantowany przez parlamentarną Komisję ds. Służb Wywiadowczych (Intelligence Service Committee of the Parliament).

3.3.3.1. Nadzór na podstawie części 4 ustawy o ochronie danych

(245) Przetwarzanie danych osobowych prowadzone przez służby wywiadowcze na podstawie części 4 DPA 2018, nadzoruje Komisarz ds. Informacji ([441]).

(246) Ogólne funkcje Komisarza ds. Informacji w odniesieniu do przetwarzania danych osobowych przez służby wywiadowcze na podstawie części 4 DPA 2018 zostały określone w załączniku 13 do tej ustawy. Jego zadania obejmują m.in.: monitorowanie i egzekwowanie części 4 DPA 2018, zwiększanie świadomości społecznej, doradzanie parlamentowi, rządowi i innym instytucjom w zakresie środków legislacyjnych i administracyjnych, zwiększanie świadomości administratorów i podmiotów przetwarzających w zakresie ich obowiązków, udzielanie informacji osobie, której dane dotyczą, dotyczących wykonywania jej praw czy prowadzenie postepowań.

(247) Komisarz, podobnie jak określono w części 3 DPA 2018, jest uprawniony do powiadamiania administratorów o domniemanym naruszeniu oraz do wydawania ostrzeżeń, że przetwarzanie może naruszać przepisy, a także udziela upomnień, gdy naruszenie zostanie potwierdzone. Może również wydawać zawiadomienia egzekucyjne i zawiadomienia w sprawie sankcji za naruszenie określonych przepisów ustawy ([442]). W odróżnieniu jednak od uprawnień określonych w innych częściach DPA 2018 Komisarz nie może wydać zawiadomienia oceniającego organowi bezpieczeństwa narodowego ([443]).

(248) Ponadto w art. 110 DPA 2018 przewidziano wyjątek dotyczący korzystania przez Komisarza z niektórych uprawnień, gdy jest to wymagane do celów ochrony bezpieczeństwa narodowego. Wyjątek ten obejmuje uprawnienie Komisarza do wydawania (wszelkiego rodzaju) zawiadomień na podstawie ustawy o ochronie danych (zawiadomień informacyjnych, oceniających, egzekucyjnych i w sprawie sankcji), uprawnienie do przeprowadzania inspekcji zgodnie z zobowiązaniami międzynarodowymi, uprawnienia do wstępu i inspekcji oraz przepisy dotyczące przestępstw ([444]). Jak wyjaśniono w motywie 126, wyjątki te mają zastosowanie tylko wtedy, gdy jest to niezbędne i proporcjonalne, oraz po przeprowadzeniu oceny każdego przypadku z osobna.

(249) Komisarz ds. Informacji i służby wywiadowcze Zjednoczonego Królestwa podpisały protokół ustaleń ([445]), który ustanawia ramy współpracy w wielu kwestiach, w tym w zakresie powiadamiania o naruszeniu ochrony danych i rozpatrywania skarg osób, których dane dotyczą. W szczególności protokół ten stanowi, że po otrzymaniu skargi Komisarz ds. Informacji oceni prawidłowość zastosowania jakiegokolwiek wyłączenia dotyczącego bezpieczeństwa narodowego. Odpowiednia agencja wywiadowcza jest zobowiązana udzielić odpowiedzi na zapytania kierowane przez Komisarza ds. Informacji w kontekście rozpatrywania skarg indywidualnych w terminie 20 dni roboczych, korzystając z odpowiednich bezpiecznych kanałów, jeżeli zapytania dotyczą informacji niejawnych. Od kwietnia 2018 r. do chwili obecnej Komisarz ds. Informacji otrzymał od osób fizycznych 21 skarg, które dotyczyły służb wywiadowczych. Każda skarga została oceniona, a o rezultacie poinformowano osobę, której dane dotyczą ([446]).

([441]) Art. 116 DPA 2018.

([442]) Zgodnie z załącznikiem 13 ust. 2 do DPA 2018 wobec administratora lub podmiotu przetwarzającego mogą zostać wystawione zawiadomienia egzekucyjne i zawiadomienia w sprawie sankcji w związku z naruszeniem części 4 rozdział 2 DPA 2018 (zasady przetwarzania), przepisu części 4 DPA 2018 przyznającego prawa osobie, której dane dotyczą, wymogu poinformowania Komisarza o naruszeniu ochrony danych osobowych na mocy art. 108 DPA 2018 oraz zasad przekazywania danych osobowych do państw trzecich, państw nieobjętych konwencją i organizacji międzynarodowych, które to zasady ustanowiono w art. 109 DPA 2018 (więcej szczegółów na temat zawiadomień egzekucyjnych i w sprawie sankcji można znaleźć w motywie 92).

([443]) Zgodnie z art. 147 ust. 6 DPA 2018 Komisarz ds. Informacji nie może wydać zawiadomienia oceniającego organowi określonemu w art. 23 ust. 3 ustawy o swobodnym dostępie do informacji z 2000 r. Organem takim jest Służba Bezpieczeństwa (MI5), Tajna Służba Wywiadowcza (MI6) oraz Centrala Łączności Rządowej).

([444]) Zastosowanie wyjątku jest możliwe w przypadku następujących przepisów: art. 108 (informowanie Komisarza o naruszeniu ochrony danych osobowych), art. 119 (inspekcja zgodnie z zobowiązaniami międzynarodowymi); art. 142–154 i załącznik 15 (zawiadomienia wydawane przez Komisarza oraz uprawnienia do wstępu i inspekcji); oraz art. 170–173 (przestępstwa związane z danymi osobowymi). Ponadto – w odniesieniu do przetwarzania przez służby wywiadowcze – pkt 1 lit. a) i g) oraz pkt 2 w załączniku 13 (inne ogólne funkcje Komisarza).

([445]) Protokół ustaleń pomiędzy Biurem Komisarza ds. Informacji a wspólnotą wywiadowczą Zjednoczonego Królestwa, zob. przypis 165.

([446]) W siedmiu z tych spraw Komisarz ds. Informacji doradził skarżącemu, aby zgłosił problem administratorowi danych (dotyczy to sytuacji, gdy osoba fizyczna zgłosiła problem Komisarzowi ds. Informacji, ale powinna była najpierw zgłosić go administratorowi danych), w jednej z tych spraw Komisarz ds. Informacji udzielił administratorowi danych ogólnej porady (ma to miejsce, gdy czynności administratora danych wydają się nie naruszać przepisów, ale udoskonalenie praktyk mogło pozwolić na uniknięcie zgłoszenia problemu Komisarzowi ds. Informacji), a w pozostałych 13 przypadkach nie było wymagane żadne działanie ze strony administratora danych (dzieje się tak w sytuacjach, gdy mimo że problemy zgłoszone przez osobę fizyczną podlegają ustawie o ochronie danych z 2018 r., ponieważ dotyczą przetwarzania danych osobowych, to na podstawie dostarczonych informacji nie wydaje się, aby administrator naruszył przepisy).

3.3.3.2. Nadzór nad wykonywaniem uprawnień dochodzeniowo-śledczych na mocy IPA 2016

(250) Zgodnie z częścią 8 IPA 2016 nadzór nad korzystaniem z uprawnień dochodzeniowo-śledczych sprawuje Komisarz ds. Uprawnień Dochodzeniowo-Śledczych (IPC). Komisarzowi ds. Uprawnień Dochodzeniowo-Śledczych pomagają inni komisarze sądowi, których wspólnie określa się mianem komisarzy sądowych ([447]). W IPA 2016 określono gwarancje chroniące niezależność komisarzy sądowych. Od komisarzy sądowych wymaga się, aby zajmowali (obecnie lub w przeszłości) wysokie stanowiska sędziowskie (np. członkostwo w sądach najwyższego szczebla) ([448]) i, jak każdy pracownik wymiaru sprawiedliwości, korzystają oni ze statusu instytucji niezależnej od rządu ([449]). Zgodnie z art. 227 IPA 2016 to premier wyznacza Komisarza ds. Uprawnień Dochodzeniowo-Śledczych i tylu komisarzy sądowych, ilu uzna za niezbędne. Wszyscy komisarze, niezależnie od tego, czy są obecnymi, czy byłymi sędziami, mogą być mianowani wyłącznie na podstawie wspólnego zalecenia trzech głównych sędziów Anglii i Walii, Szkocji oraz Irlandii Północnej, a także Lorda Kanclerza ([450]). Sekretarz Stanu musi zapewnić Komisarzowi ds. Uprawnień Dochodzeniowo-Śledczych personel, pomieszczenia, wyposażenie oraz inne urządzenia i usługi ([451]). Kadencja komisarzy trwa trzy lata i mogą oni być mianowani ponownie ([452]). W ramach dodatkowego zabezpieczenia ich niezależności komisarze sądowi mogą zostać usunięci ze stanowiska wyłącznie w ściśle określonych okolicznościach nakładających wysoki próg: albo przez premiera w szczególnych okolicznościach wymienionych w sposób wyczerpujący w art. 228 ust. 5 IPA 2016 (takich jak upadłość lub kara pozbawienia wolności), albo jeśli uchwała zatwierdzająca usunięcie została przyjęta przez obie izby parlamentu ([453]).

(251) Komisarza ds. Uprawnień Dochodzeniowo-Śledczych i komisarzy sądowych wspiera w pełnieniu ich funkcji Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych. Personel Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych składa się z zespołu inspektorów, wewnętrznych ekspertów prawnych i technicznych oraz panelu doradczego ds. technologii, zapewniającego fachowe doradztwo. Podobnie jak w przypadku poszczególnych komisarzy sądowych, niezależność Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych jest chroniona. Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych jest „organem niezależnym" Home Office, tj. otrzymuje fundusze od Home Office, ale wykonuje swoje funkcje niezależnie ([454]).

(252) Główne funkcje komisarzy sądowych określono w art. 229 IPA 2016 ([455]). W szczególności komisarze sądowi mają szerokie uprawnienia w zakresie uprzedniej zgody, co stanowi część zabezpieczeń wprowadzonych do ram prawnych Zjednoczonego Królestwa wraz z IPA 2016. Komisarze sądowi muszą zatwierdzać nakazy w odniesieniu do ukierunkowanego przechwytywania, ingerencji w urządzenia elektroniczne, masowego zbioru danych osobowych, masowego pozyskiwania danych pochodzących z łączności, a także nakazy zatrzymywania danych pochodzących z łączności ([456]). Komisarz ds. Uprawnień Dochodzeniowo-Śledczych musi również zawsze wstępnie zatwierdzać pozyskiwanie danych pochodzących z łączności do celów ścigania przestępstw ([457]). Jeżeli komisarz odmówi zatwierdzenia nakazu, Sekretarz Stanu może odwołać się do Komisarza ds. Uprawnień Dochodzeniowo-Śledczych, którego decyzja jest ostateczna.

---

([447]) Zgodnie z art. 227 ust. 7 i 8 IPA 2016 Komisarz ds. Uprawnień Dochodzeniowo-Śledczych jest komisarzem sądowym, a wraz z pozostałymi komisarzami sądowymi jest objęty łącznym określeniem „komisarze sądowi". Obecnie jest 15 komisarzy sądowych.

([448]) Zgodnie z art. 60 ust. 2 części 3 ustawy o reformie konstytucyjnej z 2005 r. wysokie stanowisko sędziowskie oznacza stanowisko sędziego w którymkolwiek z następujących sądów: (i) Sąd Najwyższy (Supreme Court); (ii) Sąd Apelacyjny w Anglii i Walii (Court of Appeal in England and Wales); (iii) Wysoki Trybunał w Anglii i Walii (High Court in England and Wales); (iv) Najwyższy Sąd Cywilny (Court of Session); (v) Sąd Apelacyjny w Irlandii Północnej (Court of Appeal in Northern Ireland); (vi) Wysoki Trybunał w Irlandii Północnej (High Court in Northern Ireland) lub stanowisko sędziego Sądu Apelacyjnego w sądzie powszechnym (Lord of Appeal in Ordinary).

([449]) Niezależność sądów opiera się na konwencji i jest powszechnie uznawana od czasu ustawy o następstwie tronu z 1701 r.

([450]) Art. 227 ust. 3 IPA 2016. Komisarze sądowi muszą być rekomendowani również przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych zgodnie z art. 227 ust. 4 lit. e) IPA 2016.

([451]) Art. 238 IPA 2016.

([452]) Art. 227 ust. 2 IPA 2016.

([453]) Procedura usunięcia z urzędu jest identyczna jak w przypadku innych sędziów w Zjednoczonym Królestwie (zob. np. art. 11 ust. 3 ustawy w sprawie sądów wyższej instancji z 1981 r. oraz art. 33 ustawy o reformie konstytucyjnej z 2005 r., w których wymaga się również uchwały po zatwierdzeniu przez obie izby parlamentu). Do chwili obecnej żadnego komisarza sądowego nie usunięto z urzędu.

([454]) Organ niezależny to organizacja lub agencja, która otrzymuje środki finansowe od rządu, ale jest w stanie działać niezależnie (definicja i więcej informacji na temat organu niezależnego znajduje się w podręczniku Kancelarii Rządu (Cabinet Office) dotyczącym klasyfikacji organów publicznych, dostępnym pod adresem): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf i pierwsze sprawozdanie z sesji komisji specjalnej Izby Gmin ds. administracji publicznej w latach 2014–2015, dostępne pod adresem: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Zgodnie z sekcją 229 IPA 2016 komisarz sądowy posiada szerokie uprawnienia nadzorcze, które obejmują również nadzór nad zatrzymywaniem i ujawnianiem danych gromadzonych przez agencje wywiadowcze.

([456]) Decyzje o tym, czy zatwierdzić decyzję Sekretarza Stanu o wydaniu nakazu, należą do samych komisarzy sądowych. Jeżeli komisarz odmówi zatwierdzenia nakazu, Sekretarz Stanu może odwołać się do Komisarza ds. Uprawnień Dochodzeniowo-Śledczych, którego decyzja jest ostateczna.

([457]) Zezwolenie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych jest zawsze wymagane w przypadku pozyskiwania danych pochodzących z łączności do celów ścigania przestępstw (art. 60A IPA 2016). Jeżeli dane pochodzące z łączności pozyskuje się do celów bezpieczeństwa narodowego, zezwolenie może zostać wydane przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych lub, alternatywnie, przez wyznaczonego urzędnika wyższego szczebla odpowiedniego organu publicznego (zob. art. 61 i 61A IPA 2016 i motyw 203).

(253) Specjalny sprawozdawca ONZ ds. prawa do prywatności z dużym zadowoleniem przyjął powołanie komisarzy sądowych w ramach IPA 2016, ponieważ „wszystkie bardziej wrażliwe lub inwazyjne wnioski o prowadzenie nadzoru muszą być zatwierdzone zarówno przez ministra rządu, jak i przez Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych". W szczególności podkreślił, że „ten element kontroli sądowej [poprzez rolę Komisarza ds. Uprawnień Dochodzeniowo-Śledczych], przy wsparciu lepiej wyposażonego zespołu doświadczonych inspektorów i ekspertów ds. technologii, jest jednym z najważniejszych nowych zabezpieczeń wprowadzonych przez IPA" w miejsce wcześniejszego rozdrobnionego systemu organów nadzoru i jako uzupełnienie kompetencji Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa Parlamentu i Trybunału ds. Uprawnień Dochodzeniowo-Śledczych ([458]).

(254) Ponadto Komisarz ds. Uprawnień Dochodzeniowo-Śledczych ma uprawnienia do prowadzenia nadzoru *ex post* ([459]), w tym w drodze audytu, kontroli i dochodzeń, nad wykonywaniem uprawnień dochodzeniowo-śledczych na mocy IPA 2016 oraz niektórych innych uprawnień i funkcji przewidzianych w odpowiednich przepisach ([460]). Wyniki takiego nadzoru *ex post* są zawarte w sprawozdaniu, które Komisarz ds. Uprawnień Dochodzeniowo-Śledczych musi przygotowywać corocznie i przedstawiać premierowi ([461]) oraz które musi być publikowane i przedkładane Parlamentowi ([462]). Sprawozdanie zawiera odpowiednie dane statystyczne i informacje na temat korzystania z uprawnień dochodzeniowo-śledczych przez agencje wywiadowcze i organy ścigania, a także na temat stosowania zabezpieczeń w odniesieniu do elementów objętych prawniczą tajemnicą zawodową, poufnych materiałów dziennikarskich i źródeł informacji dziennikarskich, informacji na temat podjętych ustaleń i celów operacyjnych wykorzystywanych w kontekście nakazów masowego pozyskania danych. Ponadto w sprawozdaniu rocznym Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych określono, w jakim obszarze organom publicznym przekazano zalecenia i jak się do nich odniesiono ([463]).

(255) Zgodnie z art. 231 IPA 2016, jeżeli Komisarz ds. Uprawnień Dochodzeniowo-Śledczych dowie się o jakimkolwiek istotnym błędzie popełnionym przez organy publiczne przy korzystaniu z ich uprawnień dochodzeniowo-śledczych, musi poinformować daną osobę, jeżeli uzna, że błąd jest poważny i że poinformowanie tej osoby leży w interesie publicznym ([464]). W szczególności w art. 231 IPA 2016 określono, że informując osobę o błędzie, Komisarz ds. Uprawnień Dochodzeniowo-Śledczych musi przekazać informacje o prawie danej osoby do wystąpienia z wnioskiem do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych, a także przekazać szczegóły, które Komisarz uzna za niezbędne do korzystania z tych praw, a za ujawnieniem przemawia interes publiczny ([465]).

([458]) Oświadczenie specjalnego sprawozdawcy ds. prawa do prywatności na zakończenie jego misji w Zjednoczonym Królestwie Wielkiej Brytanii i Irlandii Północnej (zob. przypis 281).

([459]) Art. 229 IPA 2016. Uprawnienia dochodzeniowo-śledcze i informacyjne komisarza sądowego określono w art. 235 IPA 2016.

([460]) Obejmuje to środki nadzoru na mocy RIPA 2000, wykonywanie funkcji na mocy części 3 ustawy o policji z 1997 r. (zezwolenie na działania w odniesieniu do mienia) oraz wykonywanie przez Sekretarza Stanu funkcji na mocy art. 5–7 ustawy o służbach wywiadowczych z 1994 r. (nakazy ingerencji w radiotelegrafię, wstępu do pomieszczeń i ingerencji w mienie [art. 229 IPA 2016]).

([461]) Art. 230 IPA 2016. Komisarz ds. Uprawnień Dochodzeniowo-Śledczych może również z własnej inicjatywy składać premierowi sprawozdania w każdej sprawie związanej z jego funkcjami. Komisarz ds. Uprawnień Dochodzeniowo-Śledczych musi również składać sprawozdania premierowi na jego wniosek, a premier może nakazać Komisarzowi ds. Uprawnień Dochodzeniowo-Śledczych dokonanie przeglądu wszelkich funkcji służb wywiadowczych.

([462]) Niektóre części mogą zostać wyłączone, jeśli ich publikacja byłaby sprzeczna z bezpieczeństwem narodowym.

([463]) Np. w sprawozdaniu rocznym Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r. (pkt 6.38) wspomniano, że MI5 zalecono zmianę polityki zatrzymywania masowych zbiorów danych osobowych, ponieważ powinna ona była przyjąć podejście uwzględniające proporcjonalność zatrzymywania w odniesieniu do wszystkich pól w masowych zbiorach danych osobowych i w odniesieniu do każdego przechowywanego masowego zbioru danych osobowych. Pod koniec 2018 r. Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych nie miało pewności, że zalecenie to zostało wykonane, a w sprawozdaniu za 2019 r. wyjaśniło, że MI5 wprowadza obecnie nowy proces w celu spełnienia tego wymogu. W sprawozdaniu rocznym za 2019 r. (pkt 8.22) wspomniano również, że GHCQ otrzymał szereg zaleceń dotyczących ewidencjonowania proporcjonalności zapytań dotyczących danych masowych. W sprawozdaniu potwierdzono, że na koniec 2018 r. w tym obszarze nastąpiła poprawa. Sprawozdanie roczne Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., dostępne pod adresem: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Ponadto z każdej inspekcji organu publicznego przeprowadzanej przez Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych sporządza się sprawozdanie zawierające wszelkie zalecenia wynikające z tej kontroli, które przekazuje się temu organowi. Biuro Komisarza ds. Uprawnień Dochodzeniowo-Śledczych rozpoczyna następnie każdą kolejną inspekcję od przeglądu wszelkich uprzednich zaleceń; znajdują one odzwierciedlenie w nowym sprawozdaniu z inspekcji, niezależnie od tego, czy zostały zrealizowane, czy zostają utrzymane w mocy.

([464]) Błąd uznaje się za „poważny", gdy Komisarz uzna, że spowodował on znaczny uszczerbek lub szkodę dla danej osoby (art. 231 ust. 2 IPA 2016). W 2018 r. zgłoszono 22 błędy, z czego osiem uznano za poważne i skutkowały one poinformowaniem osoby zainteresowanej. Zob. sprawozdanie roczne Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2018 r., załącznik C (zob. https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). W 2019 r. 14 błędów uznano za poważne. Zob. sprawozdanie roczne Biura Komisarza ds. Uprawnień Dochodzeniowo-Śledczych za 2019 r., załącznik C, zob. przypis 463.

([465]) W art. 231 IPA 2016 określono, że informując osobę o błędzie, Komisarz ds. Uprawnień Dochodzeniowo-Śledczych musi przedstawić informacje, które uzna za niezbędne do korzystania z tych praw, uwzględniając w szczególności zakres, w jakim ujawnienie szczegółów byłoby sprzeczne z interesem publicznym lub szkodliwe dla zapobiegania poważnym przestępstwom i ich wykrywania, dla dobrobytu gospodarczego Zjednoczonego Królestwa lub dalszego wykonywania funkcji którejkolwiek ze służb wywiadowczych.

3.3.3.3. Nadzór parlamentarny nad służbami wywiadowczymi

(256) Podstawą ustawową regulującą nadzór parlamentarny sprawowany przez Komisję ds. Agencji Wywiadowczych i Bezpieczeństwa jest ustawa o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. ([466]). Na mocy tej ustawy powołano Komisję ds. Agencji Wywiadowczych i Bezpieczeństwa, która stanowi jedną z komisji parlamentu Zjednoczonego Królestwa. W 2013 r. zwiększono zakres uprawnień Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa i obecnie obejmuje on również nadzór nad działaniami operacyjnymi podejmowanymi przez służby bezpieczeństwa. Zgodnie z art. 2 ustawy o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa powierzono zadanie sprawowania nadzoru nad wydatkami agencji bezpieczeństwa narodowego, ich administracją, realizowaną przez nie polityką oraz podejmowanymi przez nie działaniami operacyjnymi. Zgodnie z ustawą o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa może prowadzić postępowania w kwestiach operacyjnych, jeżeli nie dotyczą one operacji będących w toku ([467]). W protokole ustaleń uzgodnionym między premierem a Komisją ds. Agencji Wywiadowczych i Bezpieczeństwa ([468]) wyszczególniono elementy, które należy wziąć pod uwagę przy ustalaniu, czy dana czynność jest częścią operacji będącej w toku, czy też nie ([469]). Premier może również zwrócić się do Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa o zbadanie operacji będących w toku; komisja może ponadto dokonać przeglądu informacji przekazanych dobrowolnie przez agencje.

(257) Zgodnie z załącznikiem 1 do ustawy o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa może wystąpić do kierownika każdej z trzech służb wywiadowczych o ujawnienie wszelkich informacji. Agencja jest zobowiązana udostępnić żądane informacje, chyba że Sekretarz Stanu się temu sprzeciwi ([470]). Zgodnie z wyjaśnieniami przedstawionymi przez władze Zjednoczonego Królestwa w praktyce przypadki odmowy udostępnienia Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa żądanych przez nią informacji zdarzają się niezwykle rzadko ([471]).

(258) W skład Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa wchodzą członkowie izb parlamentu powołani przez premiera po zasięgnięciu opinii lidera opozycji ([472]). Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa jest zobowiązana przedstawić parlamentowi sprawozdanie roczne ze swojej działalności, a w stosownych przypadkach również inne sprawozdania ([473]). Ponadto Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa jest uprawniona do otrzymywania co trzy miesiące wykazu celów operacyjnych, który wykorzystuje się do badania materiałów otrzymywanych masowo ([474]). Premier udostępnia Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa kopie dokumentów dotyczących postępowań, inspekcji lub audytów prowadzonych przez Komisarza ds. Uprawnień Dochodzeniowo-Śledczych, jeżeli przedmiot sprawozdań jest istotny dla ustawowych kompetencji Komisji ([475]). Ponadto Komisja może zwrócić się do Komisarza ds. Uprawnień Dochodzeniowo-Śledczych o przeprowadzenie postępowania, a Komisarz musi poinformować Komisję ds. Agencji Wywiadowczych i Bezpieczeństwa o decyzji dotyczącej przeprowadzenia takiego postępowania ([476]).

(259) Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa przedstawiła również swoje uwagi na temat projektu IPA 2016, co zaowocowało szeregiem poprawek, które zostały obecnie odzwierciedlone w IPA 2016 ([477]). W szczegól-

([466]) Zgodnie z wyjaśnieniami udzielonymi przez władze Zjednoczonego Królestwa w ustawie o wymiarze sprawiedliwości i bezpieczeństwie rozszerzono zakres uprawnień Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa, aby uwzględnić jej rolę w sprawowaniu nadzoru nad wspólnotą wywiadowczą, którego zakres wykracza poza trzy główne agencje, oraz aby zapewnić możliwość sprawowania nadzoru z mocą wsteczną nad działaniami operacyjnymi agencji w kwestiach mających istotne znaczenie z punktu widzenia interesu narodowego.

([467]) Art. 2 ustawy o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r.

([468]) Protokół ustaleń między premierem a Komisją ds. Agencji Wywiadowczych i Bezpieczeństwa dostępny pod adresem: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Protokół ustaleń między premierem a Komisją ds. Agencji Wywiadowczych i Bezpieczeństwa, pkt 14, zob. przypis 468.

([470]) Sekretarz Stanu może sprzeciwić się ujawnieniu informacji wyłącznie w dwóch przypadkach: gdy żądane informacje są szczególnie chronione i nie powinny zostać ujawnione Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa ze względów związanych z bezpieczeństwem narodowym lub są informacjami takiego rodzaju, że w przypadku gdyby Sekretarz Stanu został poproszony o ich przedstawienie przed departamentalną komisją specjalną Izby Gmin, musiałby uznać ich przedstawienie za niewłaściwe (ze względów innych niż względy związane z bezpieczeństwem narodowym) (pkt 4 ppkt 2 w załączniku 1 do ustawy o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r.).

([471]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Bezpieczeństwo narodowe, s. 43, zob. przypis 31.

([472]) Art. 1 ustawy o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. Ministrowie nie mogą być członkami komisji. Kadencja członków Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa odpowiada kadencji parlamentu, w trakcie której ich powołano. Członków może odwołać w drodze uchwały izba parlamentu, która ich powołała; ich kadencja wygasa również z chwilą zaprzestania pełnienia przez nich funkcji członka parlamentu lub powierzenia im funkcji ministra. Członek komisji może również samodzielnie zrezygnować z członkostwa.

([473]) Sprawozdania i opinie komisji są dostępne online pod adresem: https://isc.independent.gov.uk/publications/. W 2015 r. Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa opublikowała sprawozdanie pt. „Prywatność i bezpieczeństwo: nowoczesne i przejrzyste ramy prawne" (zob.: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), w którym przeprowadziła analizę ram prawnych regulujących kwestie związane ze stosowaniem technik nadzoru przez agencje wywiadowcze i wydała szereg zaleceń, które poddano następnie ocenie i włączono do projektu ustawy o uprawnieniach dochodzeniowo-śledczych, przekształconej na późniejszym etapie w IPA 2016. Odpowiedź rządu na sprawozdanie dotyczące prywatności i bezpieczeństwa jest dostępna pod adresem: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) Art. 142, 161 i 183 IPA 2016.

([475]) Art. 234 IPA 2016.

([476]) Art. 236 IPA 2016.

([477]) Sprawozdanie Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa Parlamentu w sprawie projektu ustawy o uprawnieniach dochodzeniowo-śledczych, dostępne pod adresem: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf.

ności Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa zaleciła wzmocnienie ochrony prywatności poprzez wprowadzenie zestawu środków ochrony prywatności mających zastosowanie do pełnego zakresu uprawnień dochodzeniowo-śledczych ([478]). Komisja zaproponowała również zmiany w zakresie proponowanych możliwości dotyczących ingerencji w urządzenia elektroniczne, masowego zbioru danych osobowych i danych pochodzących z łączności oraz zwróciła się o wprowadzenie innych szczegółowych zmian w celu wzmocnienia ograniczeń i zabezpieczeń w zakresie korzystania z uprawnień dochodzeniowo-śledczych ([479]).

3.3.4. *Środki zaskarżenia*

(260) W dziedzinie dostępu rządu do danych w celach bezpieczeństwa narodowego, osobom, których dane dotyczą, powinna przysługiwać możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania lub usunięcia takich danych ([480]). Taki organ sądowy musi w szczególności posiadać uprawnienia do przyjmowania wiążących decyzji w sprawie służby wywiadowczej ([481]). W Zjednoczonym Królestwie, jak wyjaśniono w motywach 261–271, szereg sądowych środków zaskarżenia zapewnia osobom, których dane dotyczą, możliwość ubiegania się o takie środki ochrony prawnej i skorzystania z nich.

3.3.4.1. Mechanizmy zaskarżenia dostępne w ramach części 4 ustawy o ochronie danych

(261) Zgodnie z art. 165 DPA 2018 osoba, której dane dotyczą, ma prawo do wniesienia skargi do Komisarza ds. Informacji, jeżeli uważa, że doszło do naruszenia części 4 DPA 2018 w odniesieniu do danych osobowych, które jej dotyczą. Komisarz ds. Informacji jest uprawniony do oceny przestrzegania DPA 2018 przez administratora i podmiot przetwarzający oraz wezwania ich do podjęcia koniecznych działań. Ponadto zgodnie z częścią 4 DPA 2018 osoby fizyczne są uprawnione do wystąpienia do Wysokiego Trybunału (lub do Court of Session w Szkocji) o wydanie nakazu zobowiązującego administratora do zapewnienia poszanowania prawa dostępu do danych ([482]), prawa do wyrażenia sprzeciwu wobec przetwarzania danych ([483]) lub prawa do sprostowania danych bądź ich usunięcia ([484]).

(262) Osoby fizyczne mogą również dochodzić odszkodowania z tytułu szkód, jakich doznały wskutek niespełnienia przez administratora lub podmiot przetwarzający wymogu ustanowionego w części 4 DPA 2018 ([485]). Szkoda obejmuje zarówno stratę finansową, jak i szkodę niezwiązaną ze stratą finansową, taką jak cierpienie ([486]).

3.3.4.2. Mechanizmy zaskarżenia dostępne na mocy IPA 2016

(263) Osobom fizycznym przysługują środki zaskarżenia z tytułu naruszenia IPA 2016 przed Trybunałem ds. Uprawnień Dochodzeniowo-Śledczych (Investigatory Powers Tribunal).

(264) Trybunał ds. Uprawnień Dochodzeniowo-Śledczych został ustanowiony na mocy RIPA 2000 i jest niezależny od władzy wykonawczej ([487]). Zgodnie z art. 65 RIPA 2000 Jej Królewska Mość powołuje członków tego Trybunału na pięcioletnią kadencję. Jej Królewska Mość może odwołać członka tego Trybunału na podstawie oświadczenia ([488]) obydwu izb parlamentu ([489]).

([478]) Te ogólne obowiązki w odniesieniu do prywatności są obecnie określone w art. 2 ust. 2 IPA 2016, który stanowi, że organ publiczny działający na podstawie IPA 2016 musi uwzględnić, 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 oraz 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, interes publiczny w zakresie integralności i bezpieczeństwa systemów telekomunikacyjnych i usług pocztowych oraz wszelkie inne aspekty interesu publicznego w zakresie ochrony prywatności.

([479]) Np. na wniosek Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa skrócono z pięciu do trzech dni roboczych liczbę dni, w których może obowiązywać „pilny" nakaz, zanim komisarz sądowy będzie musiał go zatwierdzić, a Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa otrzymała uprawnienia do przekazywania spraw Komisarzowi ds. Uprawnień Dochodzeniowo-Śledczych w celu przeprowadzenia dochodzenia.

([480]) Schrems II, pkt 194.

([481]) Schrems II, pkt 197.

([482]) Art. 94 ust. 11 DPA 2018.

([483]) Art. 99 ust. 4 DPA 2018.

([484]) Art. 100 ust. 1 DPA 2018.

([485]) Art. 169 DPA 2018 zapewnia możliwość wystąpienia z roszczeniem „osobie, która doznała szkody wskutek niespełnienia wymogu ustanowionego w ustawodawstwie w dziedzinie ochrony danych". Zgodnie z informacjami przekazanymi przez władze Zjednoczonego Królestwa w praktyce roszczenie lub skarga przeciwko służbom wywiadowczym będą prawdopodobnie wnoszone do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych, który ma szerokie uprawnienia, może przyznać odszkodowanie, a wniesienie roszczenia nie wiąże się z żadnymi kosztami.

([486]) Art. 169 ust. 5 DPA 2018.

([487]) Zgodnie z załącznikiem 3 do RIPA 2000 członkowie muszą dysponować określonym doświadczeniem w pracy w organach wymiaru sprawiedliwości i mogą zostać powołani na kolejną kadencję.

([488]) „Oświadczenie" oznacza wniosek składany w parlamencie, służący zapoznaniu monarchy z opiniami parlamentu na dany temat.

([489]) Pkt 1 ppkt 5 w załączniku 3 do RIPA 2000.

(265) Zgodnie z art. 65 RIPA 2000 Trybunał jest właściwym organem sądowym dla wszelkich skarg wnoszonych przez osoby poszkodowane w toku postępowania prowadzonego na podstawie IPA 2016 lub RIPA 2000 bądź jakiegokolwiek postępowania służb wywiadowczych ([490]).

(266) Aby wszcząć postępowanie przed Trybunałem ds. Uprawnień Dochodzeniowo-Śledczych („wymóg w zakresie legitymacji procesowej"), zgodnie z art. 65 RIPA 2000 osoba fizyczna musi żywić przekonanie ([491]), że służba wywiadowcza podjęła określone działania w odniesieniu do niej, jakiegokolwiek składnika jej majątku, jakichkolwiek wysyłanych przez nią lub adresowanych do niej wiadomości lub wiadomości, które miały zostać jej przesłane, lub w odniesieniu do korzystania przez nią z jakichkolwiek usług pocztowych, usług telekomunikacyjnych lub systemu telekomunikacyjnego" ([492]). Ponadto skarżący musi być przekonany, że działania te były podejmowane w „okolicznościach budzących wątpliwości" ([493]) lub „przez służby wywiadowcze lub w ich imieniu" ([494]). Ponieważ do owego „przekonania" stosuje się dość szeroką wykładnię ([495]), wniesienie sprawy do Trybunału podlega łagodnym wymogom w zakresie legitymacji procesowej.

(267) W przypadku gdy Trybunał ds. Uprawnień Dochodzeniowo-Śledczych rozpatruje wniesioną do niego skargę, jego obowiązkiem jest zbadanie, czy osoby, wobec których w skardze sformułowano jakikolwiek zarzut, dopuściły się naruszeń w stosunku do skarżącego, jak również zbadanie organu, który rzekomo dopuścił się naruszeń, oraz kwestii, czy miało miejsce zarzucane działanie ([496]). We wszelkich tego rodzaju postępowaniach przy wydawaniu orzeczeń Trybunał musi stosować te same zasady, które zastosowałby sąd w przypadku wniosku o kontrolę sądową ([497]). Ponadto adresaci nakazów lub zawiadomień na podstawie IPA 2016, a także każda inna osoba pełniąca urząd podlegający zwierzchnictwu władzy królewskiej, zatrudniona przez siły policyjne lub Komisarza ds. Dochodzeń Policyjnych i Kontroli mają obowiązek ujawnić lub dostarczyć temu Trybunałowi wszelkie dokumenty i informacje, jakich Trybunał zażąda na potrzeby wykonywania prawa orzekania ([498]).

(268) Trybunał ds. Uprawnień Dochodzeniowo-Śledczych musi powiadomić skarżącego o tym, czy wydał orzeczenie na jego korzyść, czy nie ([499]). Zgodnie z art. 67 ust. 6 i 7 RIPA 2000 Trybunał jest uprawniony do wydawania nakazów tymczasowych oraz zasądzania odszkodowania lub zastosowania innego nakazu, jaki uzna za stosowny. Może to obejmować nakaz unieważnienia lub anulowania nakazu lub zezwolenia oraz nakaz zniszczenia wszelkich zapisów informacji uzyskanych w ramach wykonywania uprawnień przyznanych na podstawie nakazu, zezwolenia lub

([490]) Art. 65 ust. 5 RIPA 2000.

([491]) W odniesieniu do kryterium „przekonań" zob. sprawa Human Rights Watch przeciwko Secretary of State [2016] UKIP-Trib15_165-CH, pkt 41. W tej sprawie Trybunał ds. Uprawnień Dochodzeniowo-Śledczych, odwołując się do orzecznictwa Europejskiego Trybunału Praw Człowieka, orzekł, że właściwym kryterium jest określenie, czy w odniesieniu do będącego przedmiotem dochodzenia przekonania, że działanie objęte art. 68 ust. 5 RIPA 2000 zostało podjęte przez którąkolwiek ze służb wywiadowczych lub w jej imieniu, istnieje jakakolwiek podstawa takiego przekonania, która umożliwiała osobie fizycznej twierdzenie, że jest ona ofiarą naruszenia spowodowanego samym istnieniem niejawnych środków lub ustawodawstwa pozwalającego na stosowanie niejawnych środków, pod warunkiem że jest ona w stanie wykazać, że ze względu na jej sytuację osobistą jest potencjalnie zagrożona zastosowaniem wobec niej takich środków.

([492]) Art. 65 ust. 4 lit. a) RIPA 2000.

([493]) Okoliczności te odnoszą się do działań organów publicznych podejmowanych na podstawie upoważnienia (np. nakazu, zezwolenia na pozyskanie komunikacji/zawiadomienia o pozyskaniu komunikacji itp.), lub do takich sytuacji, w których (niezależnie od tego, czy wydano takie upoważnienie) działanie takie nie byłoby właściwe bez tego upoważnienia lub przynajmniej bez należytego rozważenia, czy należy wystąpić o takie upoważnienie. Za działanie podejmowane w okolicznościach budzących wątpliwości uznaje się zachowanie na podstawie upoważnienia udzielonego przez komisarza sądowego (art. 65 (7ZA) RIPA 2000), natomiast innych działań podejmowanych za zgodą osoby sprawującej urząd sądowy nie uznaje się za podejmowane w okolicznościach budzących wątpliwości (art. 65 ust. 7 i 8 RIPA 2000).

([494]) Zgodnie z informacjami przekazanymi przez władze Zjednoczonego Królestwa niski próg wymagany do złożenia skargi powoduje, że nierzadko w ramach prowadzonego dochodzenia Trybunał stwierdza, że w rzeczywistości organ publiczny nigdy nie prowadził dochodzenia wobec skarżącego. W najnowszym sprawozdaniu statystycznym Trybunał ds. Uprawnień Dochodzeniowo-Śledczych precyzuje, że w 2016 r. do Trybunału wpłynęło 209 skarg, z czego 52 % uznano za niepoważne lub uciążliwe, a 25 % pozostało bez rozstrzygnięcia. Władze Zjednoczonego Królestwa wyjaśniły, że oznacza to, że w odniesieniu do skarżącego nie skorzystano z żadnego niejawnego działania/upoważnienia, albo że zastosowano niejawne techniki, a Trybunał uznał, że działanie to było zgodne z prawem. Ponadto 11 % skarg odrzucono ze względu na brak właściwości do ich rozpoznania, wycofano lub uznano za nieważne, 5 % uznano za wniesione po terminie, a w przypadku 7 % wydano orzeczenie korzystne dla skarżącego. Sprawozdanie statystyczne Trybunału ds. Uprawnień Dochodzeniowo-Śledczych z 2016 r., dostępne pod adresem: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Zob. sprawa Human Rights Watch przeciwko Secretary of State [2016] UKIPTrib15_165-CH. W tej sprawie Trybunał ds. Uprawnień Dochodzeniowo-Śledczych, odwołując się do orzecznictwa Europejskiego Trybunału Praw Człowieka, orzekł, że właściwym kryterium w odniesieniu do przekonania, że działanie objęte art. 68 ust. 5 RIPA 2000 zostało podjęte przez którąkolwiek ze służb wywiadowczych lub w jej imieniu, jest określenie, czy istnieje jakakolwiek podstawa takiego przekonania, w tym fakt, że osoba fizyczna może twierdzić, że jest ofiarą naruszenia spowodowanego samym istnieniem niejawnych środków lub ustawodawstwa pozwalającego na stosowanie niejawnych środków, pod warunkiem że jest ona w stanie wykazać, że ze względu na jej sytuację osobistą jest potencjalnie zagrożona zastosowaniem wobec niej takich środków (zob. Human Rights Watch przeciwko Secretary of State, pkt 41).

([496]) Art. 67 ust. 3 RIPA 2000.

([497]) Art. 67 ust. 2 RIPA 2000.

([498]) Art. 68 ust. 6–7 RIPA 2000.

([499]) Art. 68 ust. 4 RIPA 2000.

zawiadomienia lub w inny sposób przechowywanych przez organ publiczny w odniesieniu do jakiejkolwiek osoby ([500]). Zgodnie z art. 67A RIPA 2000 orzeczenie Trybunału można zaskarżyć pod warunkiem uzyskania zgody Trybunału lub właściwego sądu apelacyjnego.

(269) Warto wreszcie zauważyć, że rolę Trybunału ds. Uprawnień Dochodzeniowo-Śledczych omawiano kilkakrotnie w kontekście czynności prawnych przed Europejskim Trybunałem Praw Człowieka, zwłaszcza w sprawie Kennedy przeciwko Zjednoczonemu Królestwu ([501]), a ostatnio w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu ([502]), w przypadku której Trybunał uznał, że „Trybunał ds. Uprawnień Dochodzeniowo-Śledczych zaoferował solidne sądowe środki zaskarżenia każdemu, kto podejrzewał, że jego komunikacja była przechwytywana przez służby wywiadowcze" ([503]).

3.3.4.3. Inne dostępne mechanizmy dochodzenia roszczeń

(270) Jak wyjaśniono w motywach 109–111, środki zaskarżenia przewidziane w ustawie o prawach człowieka z 1998 r. i środki umożliwiające zaskarżenie przed Europejski Trybunał Praw Człowieka ([504]) są również dostępne w obszarze bezpieczeństwa narodowego. W art. 65 ust. 2 RIPA 2000 przyznano Trybunałowi ds. Uprawnień Dochodzeniowo-Śledczych właściwość wyłączną w zakresie wszystkich roszczeń wynikających z ustawy o prawach człowieka w odniesieniu do agencji wywiadowczych ([505]). Jak zauważył Wysoki Trybunał, oznacza to, że „kwestia, czy doszło do naruszenia ustawy o prawach człowieka w zakresie okoliczności faktycznych konkretnej sprawy, może być zasadniczo podniesiona i rozstrzygnięta przez niezależny sąd, który może mieć dostęp do wszystkich istotnych materiałów, w tym materiałów niejawnych. [...] W tym kontekście należy również pamiętać, że orzeczenia samego Trybunału mogą obecnie stać się przedmiotem odwołania do odpowiedniego sądu apelacyjnego (w Anglii i Walii byłby to Sąd Apelacyjny) oraz że Sąd Najwyższy orzekł niedawno, że Trybunał może co do zasady podlegać kontroli sądowej: zob. Korona (Privacy International) przeciwko Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219" ([506]).

(271) Z powyższego wynika, że gdy organy ścigania lub organy bezpieczeństwa narodowego Zjednoczonego Królestwa uzyskują dostęp do danych osobowych objętych zakresem niniejszej decyzji, dostęp taki jest regulowany przepisami określającymi warunki, na jakich dostęp ten może mieć miejsce, i zapewniają ograniczenie dostępu do danych i ich dalszego wykorzystywania do tego, co jest niezbędne i proporcjonalne do celu związanego ze ściganiem przestępstw lub bezpieczeństwem narodowym. Ponadto dostęp taki w większości przypadków wymaga uprzedniego zezwolenia organu sądowego, poprzez zatwierdzenie nakazu lub nakazu wydania dowodów, a w każdym przypadku podlega niezależnemu nadzorowi. Po uzyskaniu przez organy publiczne dostępu do danych, ich przetwarzanie, w tym dalsze udostępnianie i dalsze przekazywanie, podlega szczególnym zabezpieczeniom służącym ochronie danych na podstawie części 3 DPA 2018, odzwierciedlającym zabezpieczenia przewidziane w dyrektywie (UE) 2016/680, w przypadku przetwarzania przez organy ścigania, oraz części 4 DPA 2018 w przypadku przetwarzania przez agencje wywiadowcze. Ponadto osoby, których dane dotyczą, korzystają w tym obszarze ze skutecznych administracyjnych i sądowych środków zaskarżenia, w tym prawa do uzyskania dostępu do swoich danych, ich sprostowania lub usunięcia.

(272) Biorąc pod uwagę znaczenie takich warunków, ograniczeń i zabezpieczeń dla celów niniejszej decyzji, Komisja będzie ściśle monitorować stosowanie i interpretację przepisów Zjednoczonego Królestwa regulujących dostęp rządu do danych. Będzie to obejmować odpowiednie kwestie w zakresie prawodawstwa, i regulacji i orzecznictwa, a także działania Komisarza ds. Informacji i innych organów nadzoru w tej dziedzinie. Szczególna uwaga zostanie

([500]) Przykładem zastosowania tych uprawnień jest sprawa Liberty i in. przeciwko Security Service, SIS, GCHQ [2015] UKIP Trib 13_77-H_2. Trybunał wydał orzeczenie na korzyść dwóch skarżących, ponieważ w jednym przypadku czas zatrzymania ich komunikacji wykraczał poza wyznaczone granice, a w drugim – ponieważ nie przestrzegano procedury badania określonej w przepisach wewnętrznych GCHQ. W pierwszej sprawie Trybunał nakazał służbom wywiadowczym zniszczenie komunikacji, którą zatrzymano przez okres dłuższy niż odpowiedni termin. W drugim przypadku nie wydano nakazu zniszczenia, ponieważ nie zatrzymano komunikacji.

([501]) Kennedy, zob. przypis 129.

([502]) Europejski Trybunał Praw Człowieka, Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (zob. przypis 268), pkt 413–415.

([503]) Europejski Trybunał Praw Człowieka, Big Brother Watch, pkt 425.

([504]) Jak wynika na przykład z niedawnego wyroku Wielkiej Izby Europejskiego Trybunału Praw Człowieka w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu (zob. przypis 279 powyżej), umożliwia to sądowi międzynarodowemu skuteczną kontrolę sądową – podobną do kontroli, której podlegają państwa członkowskie UE – nad przestrzeganiem przez organy publiczne praw podstawowych przy dostępie do danych osobowych. Ponadto wykonanie wyroków Europejskiego Trybunału Praw Człowieka podlega szczególnemu nadzorowi ze strony Rady Europy.

([505]) W sprawie Belhaj i in. [2017] UKSC 3 ustalenie bezprawności przechwycenia materiału objętego prawniczą tajemnicą zawodową oparto bezpośrednio na art. 8 EKPC (zob. ustalenie 11).

([506]) Wysoki Trybunał, Liberty, [2019] EWHC 2057 (Admin), pkt 170.

również poświęcona wykonaniu przez Zjednoczone Królestwo odpowiednich wyroków Europejskiego Trybunału Praw Człowieka, w tym środków określonych w planach działania i sprawozdaniach z działań przedłożonych Komitetowi Ministrów w kontekście nadzoru nad przestrzeganiem orzeczeń Trybunału.

## 4. **WNIOSEK**

(273) Komisja uważa, że RODO UK i DPA 2018 zapewniają stopień ochrony danych osobowych przekazywanych z Unii Europejskiej, który zasadniczo odpowiada stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

(274) 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 naruszania 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.

(275) 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 zgodnych z interesem publicznym, w szczególności do celów ścigania przestępstw i bezpieczeństwa narodowego, będą ograniczać się do tego, co jest ściśle niezbędne do osiągnięcia danego uzasadnionego celu, oraz że istnieje skuteczna ochrona prawna przed takimi ingerencjami.

(276) W świetle ustaleń niniejszej decyzji należy zatem uznać, że Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony w rozumieniu art. 45 rozporządzenia (UE) 2016/679, interpretowanego w świetle Karty praw podstawowych Unii Europejskiej.

(277) Wniosek ten opiera się zarówno na odpowiednim systemie krajowym Zjednoczonego Królestwa, jak i na jego zobowiązaniach międzynarodowych, w szczególności na przystąpieniu do Konwencji o ochronie praw człowieka i podstawowych wolności i poddaniu się jurysdykcji Europejskiego Trybunału Praw Człowieka. Nieprzerwane przestrzeganie takich zobowiązań międzynarodowych stanowi zatem szczególnie istotny element oceny, na której opiera się niniejsza decyzja.

## 5. **SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH**

(278) 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.

(279) 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 niniejszej decyzji 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.

(280) Należy przypomnieć, że zgodnie z art. 58 ust. 5 rozporządzenia (UE) 2016/679 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems I ([507]), 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 odesłaniem prejudycjalnym do Trybunału Sprawiedliwości ([508]).

([507]) Schrems, pkt 65.

([508]) Schrems, 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".

## 6. MONITOROWANIE, ZAWIESZENIE, UCHYLENIE LUB ZMIANA NINIEJSZEJ DECYZJI

(281) Zgodnie z art. 45 ust. 4 rozporządzenia (UE) 2016/679 Komisja jest zobowiązana na bieżąco monitorować odpowiednie zmiany w Zjednoczonym Królestwie po przyjęciu niniejszej decyzji, aby ocenić, czy nadal zapewnia ono zasadniczo odpowiadający stopień ochrony. Takie monitorowanie jest szczególnie ważne w tym przypadku, ponieważ nowy system ochrony danych Zjednoczonego Królestwa, którym będzie ono zarządzać, stosować go i egzekwować jego stosowanie, nie będzie już podlegać prawu Unii; może również ulegać zmianom. W związku z tym szczególna uwaga zostanie zwrócona 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 niniejszej decyzji; na skuteczność korzystania z indywidualnych praw, w tym wszelkie istotne zmiany w prawie i praktyce dotyczących wyjątków lub ograniczeń takich praw (w szczególności wyjątku dotyczącego utrzymania skutecznej kontroli imigracyjnej) oraz przestrzegania ograniczeń i zabezpieczeń w odniesieniu do dostępu rządowego. W ramach monitorowania Komisja uwzględni m.in. zmiany w orzecznictwie i nadzór ze strony Komisarza ds. Informacji i innych niezależnych organów.

(282) 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 niniejszej decyzji, a także o wszelkich zmianach praktyk związanych z przetwarzaniem danych osobowych poddanych ocenie w niniejszej decyzji, zarówno w odniesieniu do przetwarzania danych osobowych przez administratorów i podmioty przetwarzające na mocy RODO UK, jak i ograniczeń i zabezpieczeń dotyczących dostępu do danych przez organy publiczne. Powinno to obejmować zmiany dotyczące elementów, o których mowa w motywie 281.

(283) 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 i 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, wykrywanie lub ściganie czynów zabronionych, lub za bezpieczeństwo narodowe, w tym wszelkich organów nadzoru, nie gwarantują wymaganego stopnia ochrony.

(284) W przypadku gdy z dostępnych informacji, w szczególności informacji uzyskanych w wyniku monitorowania niniejszej decyzji lub przedstawionych przez władze Zjednoczonego Królestwa lub państw członkowskich, wynika, że stopień ochrony zapewniany przez Zjednoczone Królestwo może nie być już odpowiedni, Komisja powinna powiadomić o tym właściwe organy Zjednoczonego Królestwa i zwrócić się o zastosowanie właściwych środków w określonym terminie, który nie może przekraczać trzech miesięcy. W razie potrzeby okres ten może zostać przedłużony o określony czas, biorąc pod uwagę charakter danej kwestii i środki, które należy zastosować. Procedura taka byłaby uruchamiana m.in. 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.

(285) Jeśli po upływie tego określonego terminu właściwe organy Zjednoczonego Królestwa nie zastosują tych środków lub w inny zadowalający sposób nie wykażą, 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 uchylenia niniejszej decyzji.

(286) Ewentualnie Komisja rozpocznie tę procedurę w celu zmiany decyzji, zwłaszcza 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.

(287) 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. OKRES OBOWIĄZYWANIA I PRZEDŁUŻENIE OBOWIĄZYWANIA NINIEJSZEJ DECYZJI

(288) Komisja musi wziąć pod uwagę, że wraz z zakończeniem okresu przejściowego przewidzianego w umowie o wystąpieniu oraz z chwilą, gdy przestanie obowiązywać przepis przejściowy określony w art. 782 umowy o handlu i współpracy między Zjednoczonym Królestwem a UE, Zjednoczone Królestwo będzie zarządzać nowym systemem ochrony danych w porównaniu z systemem, który obowiązywał, gdy Zjednoczone Królestwo było związane prawem Unii, a także stosować go i egzekwować jego stosowanie. Może to w szczególności obejmować poprawki lub zmiany w ramach ochrony danych poddanych ocenie w niniejszej decyzji, jak również inne istotne zmiany.

(289) W związku z tym należy zapewnić, aby niniejsza decyzja była stosowana przez okres czterech lat od chwili jej wejścia w życie.

(290) W przypadku gdy w szczególności z informacji uzyskanych w wyniku monitorowania niniejszej decyzji będzie wynikało, że ustalenia dotyczące odpowiedniego stopnia ochrony zapewnianego w Zjednoczonym Królestwie są nadal uzasadnione pod względem faktycznym i prawnym, Komisja powinna, najpóźniej sześć miesięcy przed zakończeniem okresu stosowania niniejszej decyzji, wszcząć procedurę zmiany niniejszej decyzji poprzez przedłużenie jej zakresu czasowego, co do zasady, na dodatkowy okres czterech lat. Każdy taki akt wykonawczy zmieniający niniejszą decyzję należy przyjąć zgodnie z procedurą, o której mowa w art. 93 ust. 2 rozporządzenia (UE) 2016/679.

## 8. **UWAGI KOŃCOWE**

(291) Europejska Rada Ochrony Danych opublikowała swoją opinię ([509]), która została uwzględniona podczas przygotowywania niniejszej decyzji.

(292) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na mocy art. 93 rozporządzenia (UE) 2016/679,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

*Artykuł 1*

1. Do celów art. 45 rozporządzenia (UE) 2016/679 Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych w ramach zakresu stosowania rozporządzenia (UE) 2016/679 z Unii Europejskiej do Zjednoczonego Królestwa.

2. Niniejsza 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 DPA 2018.

*Artykuł 2*

W każdym przypadku, gdy właściwe organy nadzorcze w państwach członkowskich, w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, wykonują swoje uprawnienia na podstawie art. 58 rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych wchodzącego w zakres stosowania określony w art. 1, dane państwo członkowskie niezwłocznie informuje o tym fakcie Komisję.

*Artykuł 3*

1. Komisja stale monitoruje stosowanie ram prawnych, na których opiera się niniejsza decyzja, w tym warunków, na jakich odbywa się dalsze przekazywanie danych, wykonywanie praw indywidualnych oraz uzyskiwanie przez organy publiczne Zjednoczonego Królestwa dostępu do danych przekazywanych na podstawie niniejszej decyzji, w celu ustalenia, czy Zjednoczone Królestwo nadal zapewnia odpowiedni stopień ochrony w rozumieniu art. 1.

2. Państwa członkowskie oraz Komisja informują się nawzajem o przypadkach, w których Komisarz ds. Informacji lub jakikolwiek inny właściwy organ Zjednoczonego Królestwa nie zapewnili zgodności z ramami prawnymi, na których opiera się niniejsza decyzja.

3. Państwa członkowskie i Komisja informują się nawzajem o wszelkich sygnałach wskazujących, że ingerencje organów publicznych Zjednoczonego Królestwa w prawo osób fizycznych do ochrony ich danych osobowych wykraczają poza to, co jest ściśle niezbędne, lub że nie zapewniono skutecznej ochrony prawnej przed takimi ingerencjami.

4. Jeśli Komisja posiada dowody na to, że odpowiedni stopień ochrony nie jest już zapewniony, Komisja powiadamia o tym właściwe organy Zjednoczonego Królestwa i może zawiesić, uchylić albo zmienić niniejszą decyzję.

([509]) Opinia 14/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej przyjętej na podstawie rozporządzenia (UE) 2016/679 w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie, dostępna pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komisja może zawiesić, uchylić albo zmienić niniejszą decyzję, jeżeli brak współpracy ze strony rządu Zjednoczonego Królestwa nie pozwala Komisji stwierdzić, czy istnieją przesłanki do podważenia ustalenia zawartego w art. 1 ust. 1.

*Artykuł 4*

Niniejsza decyzja traci moc z dniem 27 czerwca 2025 r., chyba że okres jej stosowania zostanie przedłużony zgodnie z procedurą, o której mowa w art. 93 ust. 2 rozporządzenia (UE) 2016/679.

*Artykuł 5*

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 28 czerwca 2021 r.

*W imieniu Komisji*
Didier REYNDERS
*Członek Komisji*