DECYZJA WYKONAWCZA KOMISJI (UE) 2021/1773

z dnia 28 czerwca 2021 r.

na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo

(notyfikowana jako dokument nr C(2021) 4801)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

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

a także mając na uwadze, co następuje:

1. **WPROWADZENIE**

(1) W dyrektywie (UE) 2016/680 określono zasady przekazywania danych osobowych przez właściwe organy w Unii państwom trzecim i organizacjom międzynarodowym w stopniu, w jakim takie przekazywanie wchodzi w zakres jej stosowania. Zasady dotyczące międzynarodowego przekazywania danych przez właściwe organy określono w rozdziale V dyrektywy (UE) 2016/680, a konkretniej w art. 35–40. Przepływ danych osobowych do państw spoza Unii Europejskiej oraz z takich państw jest niezbędnym warunkiem skutecznej współpracy w zakresie ścigania przestępstw, należy jednak zagwarantować, aby takie przekazywanie danych osobowych nie obniżało stopnia ochrony zapewnianego tym danym w Unii Europejskiej ([2]).

(2) Na podstawie art. 36 ust. 3 dyrektywy (UE) 2016/680 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 przekazywanie danych osobowych do państwa trzeciego może nastąpić bez konieczności uzyskania dodatkowego zezwolenia (z wyjątkiem sytuacji, w której inne państwo członkowskie, od którego dane uzyskano, musi udzielić zgody na ich przekazanie), jak przewidziano w art. 35 ust. 1 i motywie 66 dyrektywy (UE) 2016/680.

(3) Jak określono w art. 36 ust. 2 dyrektywy (UE) 2016/680, przy przyjmowaniu decyzji stwierdzającej odpowiedni stopień ochrony należy opierać się na wszechstronnej analizie porządku prawnego państwa trzeciego. W swojej ocenie Komisja musi ustalić, czy dane państwo trzecie daje gwarancje zapewniające stopień ochrony „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii Europejskiej (motyw 67 dyrektywy (UE) 2016/680). Oceny spełnienia tego warunku dokonuje się według standardu ustanowionego w przepisach UE, w szczególności w dyrektywie (UE) 2016/680, 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 ([4]).

(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 odpowiedni stopień ochrony ([6]). Odpowiedni standard ochrony nie wymaga zatem dokładnego powielenia przepisów unijnych. Przy określaniu odpowiedniości chodzi raczej o stwierdzenie, czy biorąc pod uwagę istotę prawa do prywatności oraz jego skuteczne wprowadzenie w życie, egzekwowanie i nadzór nad jego przestrzeganiem, dany zagraniczny system zapewnia jako całość wymagany stopień ochrony ([7]).

([1]) Dz.U. L 119 z 4.5.2016, s. 89.
([2]) Zob. motyw 64 dyrektywy (UE) 2016/680.
([3]) Zob. niedawna sprawa C-311/18, Maximilian Schrems/Data Protection Commissioner („Schrems II"), ECLI:EU:C:2020:559.
([4]) Zob. zalecenia 01/2021 w sprawie odpowiedniego stopnia ochrony przekazywanych danych osobowych na mocy dyrektywy o ochronie danych w sprawach karnych, przyjęte w lutym 2021 r., dostępne pod adresem: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pl
([5]) Sprawa C-362/14, Maximilian Schrems/Data Protection Commissioner („Schrems"), ECLI:EU:C:2015:650, pkt 73.
([6]) Schrems, pkt 74.
([7]) Komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", COM(2017) 7 z dnia 10 stycznia 2017 r., sekcja 3.1, s. 6–7, dostępny pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

(5) Komisja uważnie przeanalizowała właściwe prawo i praktykę Zjednoczonego Królestwa. Na podstawie ustaleń przedstawionych poniżej Komisja stwierdza, że Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych przez właściwe organy Unii, zgodnie z zakresem stosowania dyrektywy (UE) 2016/680, właściwym organom w Zjednoczonym Królestwie, zgodnie z zakresem stosowania części 3 ustawy o ochronie danych z 2018 r. (DPA 2018) ([8]).

(6) Niniejsza decyzja skutkuje tym, że dane można przekazywać w ten sposób bez potrzeby uzyskania dalszego zezwolenia przez okres czterech lat, z możliwością przedłużenia obowiązywania decyzji po upływie tego terminu, bez uszczerbku dla warunków określonych w art. 35 dyrektywy (UE) 2016/680.

2. PRZEPISY MAJĄCE ZASTOSOWANIE DO PRZETWARZANIA DANYCH OSOBOWYCH PRZEZ WŁAŚCIWE ORGANY DO CELÓW ŚCIGANIA PRZESTĘPSTW

2.1. Ramy konstytucyjne

(7) Zjednoczone Królestwo jest demokracją parlamentarną. 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 wybranej Izby Gmin; władza wykonawcza jest odpowiedzialna przed obiema izbami parlamentu (Izbą Gmin i Izbą Lordów) odpowiadającymi za nadzorowanie rządu oraz za debatowanie nad ustawami i ich uchwalanie. Parlament Zjednoczonego Królestwa przekazał Parlamentowi Szkockiemu, Zgromadzeniu Narodowemu Walii (Senedd Cymru) oraz Zgromadzeniu Irlandii Północnej odpowiedzialność za stanowienie prawa w niektórych kwestiach krajowych w Szkocji, Walii i Irlandii Północnej. Chociaż ochrona danych jest kwestią zastrzeżoną dla parlamentu Zjednoczonego Królestwa, 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 (działaniami prowadzonymi przez siły policyjne), w Szkocji i Irlandii Północnej zostało powierzone odpowiednio Parlamentowi Szkockiemu i Zgromadzeniu Irlandii Północnej ([9]).

(8) Chociaż Zjednoczone Królestwo nie posiada skodyfikowanej konstytucji w postaci spisanej ustawy zasadniczej, jego zasady konstytucyjne kształtowały się w miarę upływu czasu i wywodzą się w szczególności z orzecznictwa i zwyczaju. Uznano wartość konstytucyjną niektórych ustaw, takich jak Wielka Karta Swobód, ustawa o prawach z 1689 r. i ustawa o prawach człowieka z 1998 r. Prawa podstawowe osób fizycznych ukształtowano, jako element konstytucji, poprzez prawo precedensowe (*common law*), wspomniane ustawy oraz traktaty międzynarodowe, w szczególności europejską konwencję praw człowieka (EKPC), 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]).

(9) Ustawą o prawach człowieka z 1998 r. wprowadzono prawa zawarte w EKPC do prawa Zjednoczonego Królestwa. Ustawa zapewnia każdej osobie fizycznej podstawowe prawa i wolności przewidziane w art. 2–12 i 14 EKPC, art. 1–3 pierwszego protokołu do tej konwencji oraz art. 1 trzynastego protokołu do niej w związku z art. 16–18 EKPC. Należą do nich prawo do poszanowania życia prywatnego i rodzinnego, które z kolei obejmuje prawo do ochrony danych oraz prawo do rzetelnego procesu sądowego ([11]). W szczególności zgodnie z art. 8 EKPC 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.

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

([9]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja F: ściganie przestępstw, dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Zasady konwencji nr 108 zostały pierwotnie wdrożone do prawa Zjednoczonego Królestwa w drodze ustawy o ochronie danych (DPA) 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.).

(10) Zgodnie z ustawą o prawach człowieka z 1998 r. wszelkie działania władzy publicznej muszą być zgodne z prawem zagwarantowanym w EKPC ([12]). Ponadto akty ustawowe i wykonawcze muszą być interpretowane i stosowane w sposób zgodny z tymi prawami ([13]). Każdy, kto uważa, że jego prawa, w tym prawa do prywatności i ochrony danych, zostały naruszone przez władzę publiczną, może dochodzić roszczeń przed sądami Zjednoczonego Królestwa na podstawie ustawy o prawach człowieka z 1998 r., a w ostateczności, po wyczerpaniu krajowych środków ochrony prawnej może wnieść skargę do Europejskiego Trybunału Praw Człowieka na naruszenie praw gwarantowanych w EKPC.

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

(11) Zjednoczone Królestwo wystąpiło z Unii 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, regulujące przetwarzanie 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 zawarte były w odpowiednich częściach ustawy o ochronie danych z 2018 r., która transponowała dyrektywę (UE) 2016/680.

(12) Aby przygotować się do wystąpienia z UE, rząd Zjednoczonego Królestwa przyjął Ustawę o wystąpieniu z Unii Europejskiej z 2018 r. ([15]), którą wprowadzono mające bezpośrednie zastosowanie przepisy Unii do prawa Zjednoczonego Królestwa i zapewniono, aby tzw. „ustawodawstwo krajowe wywodzące się z prawa Unii" nadal miało zastosowanie po zakończeniu okresu przejściowego. Zgodnie z Ustawą o wystąpieniu z Unii Europejskiej z 2018 r. „ustawodawstwo krajowe wywodzące się z prawa Unii" stanowi część 3 DPA 2018 ([16]) transponująca dyrektywę (UE) 2016/680. Zgodnie z Ustawą o wystąpieniu z Unii Europejskiej z 2018 r. sądy Zjednoczonego Królestwa muszą dokonywać wykładni tego niezmienionego „ustawodawstwa krajowego wywodzącego się z prawa Unii" zgodnie ze stosownym orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (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") ([17]).

(13) 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*, w celu wprowadzenia niezbędnych zmian w pozostającym w mocy prawie Unii w następstwie wystąpienia Zjednoczonego Królestwa z Unii. Uprawnienie to wykonano 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) ([18]). Rozporządzeniem tym zmieniono ustawodawstwo Zjednoczonego Królestwa w dziedzinie ochrony danych, w tym DPA 2018, aby dostosować je do kontekstu krajowego ([19]).

([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 („umowa o wystąpieniu"), dostępna pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

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

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

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

([18]) 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.

([19]) Rozporządzeniem w sprawie wyjścia z UE wprowadzono szereg zmian w części 3 DPA 2018. Wiele z tych zmian ma charakter techniczny, jak np. usunięcie odniesień do „państwa członkowskiego" lub „dyrektywy o ochronie danych w sprawach karnych" (zob. np. art. 48 ust. 8 lub art. 73 ust. 5 lit. a) DPA 2018 w odniesieniu do „prawa krajowego"), dzięki czemu część 3 można skutecznie stosować jako prawo krajowe po zakończeniu okresu przejściowego. W niektórych fragmentach wymagane były innego rodzaju zmiany, na przykład w odniesieniu do tego, kto przyjmuje „decyzje stwierdzające odpowiedni stopień ochrony" na potrzeby ram prawnych dotyczących ochrony danych w Zjednoczonym Królestwie (zob. art. 74 A DPA 2018), tj. Sekretarz Stanu zamiast Komisji Europejskiej.

(14) W rezultacie po upływie okresu przejściowego określonego w umowie o wystąpieniu normy prawne dotyczące 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, obowiązujące w Zjednoczonym Królestwie nadal będą określone w odpowiednich częściach DPA 2018, szczególnie w części 3 tej ustawy, jednak w formie zmienionej rozporządzeniem w sprawie ochrony danych, prywatności i łączności elektronicznej. Ogólne rozporządzenie o ochronie danych Zjednoczonego Królestwa (RODO UK) nie ma zastosowania do tego rodzaju przetwarzania.

(15) W części 3 DPA 2018 zawarto przepisy dotyczące przetwarzania danych osobowych do celów ścigania przestępstw, w tym zasady ochrony danych, podstawy prawne przetwarzania (legalność), prawa osób, których dane dotyczą, obowiązki właściwych organów pełniących rolę administratora oraz ograniczenia dotyczące dalszego przekazywania. Jednocześnie w częściach 5 i 6 DPA 2018 określono przepisy dotyczące nadzoru i egzekwowania prawa oraz środki zaskarżenia mające zastosowanie do sektora organów ścigania przestępstw.

(16) Ponadto w świetle istotnej roli sił policyjnych w sektorze organów ścigania przestępstw należy przeanalizować przepisy regulujące działania policyjne. Działania te mają charakter zdecentralizowany, jednak poszczególne akty ustawodawcze mające często podobną treść mają zastosowanie do pracy policji w a) Anglii i Walii, b) Szkocji oraz c) Irlandii Północnej ([20]). Co więcej, w różnych rodzajach wytycznych można znaleźć dodatkowe wyjaśnienia dotyczące właściwego wykorzystywania uprawnień policji. Trzy najważniejsze formy wytycznych dla policji to: 1) wytyczne ustawowe wydane na podstawie prawodawstwa, takie jak kodeks etyki ([21]) oraz kodeks postępowania dotyczący zarządzania informacjami policyjnymi ([22]) wydane na podstawie ustawy o policji z 1996 r. ([23]) lub kodeksy ([24]) wydane na podstawie ustawy w sprawie policji i dowodów w sprawach karnych ([25]), 2) zatwierdzone praktyki zawodowe dotyczące zarządzania informacjami policyjnymi ([26]) wydane przez Kolegium Policyjne oraz 3) wytyczne operacyjne (opublikowane przez samą policję). Krajowa Rada Komendantów Policji (organ koordynujący wszystkie siły policyjne w Zjednoczonym Królestwie) publikuje wytyczne operacyjne zatwierdzone przez wszystkie siły policyjne, które to wytyczne mają w związku z tym zastosowanie w całym kraju ([27]). Celem tych wytycznych jest zapewnienie spójności w kontekście zarządzania informacjami ([28]).

(17) Korzystając z uprawnień przewidzianych w art. 39 A ustawy o policji z 1996 r., Sekretarz Stanu wydał w 2005 r. kodeks postępowania dotyczący zarządzania informacjami policyjnymi ([29]). Każdy kodeks postępowania wydany na podstawie ustawy o policji musi zostać zatwierdzony przez Sekretarza Stanu i zanim zostanie zaprezentowany w parlamencie podlega konsultacji Krajowej Agencji ds. Zwalczania Przestępczości. W art. 39 A ust. 7 ustawy o policji nakłada się na policję wymóg należytego poszanowania kodeksów wydanych na podstawie tej ustawy, a zatem od

([20]) Bardziej szczegółowe wyjaśnienia dotyczące sił policyjnych Zjednoczonego Królestwa oraz ich uprawnień można znaleźć w: Ramach wyjaśniających Zjednoczonego Królestwa dotyczących dyskusji na temat odpowiedniego stopnia ochrony, sekcja F: ściganie przestępstw (zob. przypis 9).

([21]) Kodeks postępowania dotyczący zasad i norm postępowania zawodowego dla policjantów w Anglii i Walii, dostępny pod adresem: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Kodeks etyki dla służb policyjnych w Irlandii Północnej, dostępny pod adresem: https://www.nipolicingboard.org.uk/psni-code-ethics; Kodeks etyki dla sił policyjnych w Szkocji, dostępny pod adresem: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Kodeks postępowania dotyczący zarządzania informacjami policyjnymi, dostępny pod adresem: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Ustawa o policji z 1996 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Kodeksy postępowania wydane na podstawie ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r. (Police and Criminal Evidence Act), dostępne pod adresem: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Ustawa w sprawie policji i dowodów w sprawach karnych z 1984 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Zatwierdzone praktyki zawodowe dotyczące zarządzania informacjami policyjnymi, dostępne pod adresem: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Podręcznik dotyczący ochrony danych dla funkcjonariuszy policji zajmujących się ochroną danych, dostępny pod adresem: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Na przykład kodeks postępowania dotyczący zarządzania informacjami policyjnymi (zob. przypis 22) dotyczy zatrzymywania policyjnych informacji operacyjnych (zob. motyw 47 niniejszej decyzji).

([29]) Zgodnie z informacjami przekazanymi przez władze Zjednoczonego Królestwa w okresie rozmów na temat odpowiedniego stopnia ochrony Kolegium Policyjne prowadziło prace nad kodeksem postępowania dotyczącym zarządzania informacjami i rejestrami, który ma zastąpić kodeks postępowania dotyczący zarządzania informacjami policyjnymi. W dniu 25 stycznia 2021 r. opublikowano roboczą wersję kodeksu na potrzeby konsultacji publicznych, która jest dostępna pod adresem: https://www.college.police.uk/article/information-records-management-consultation.

policji oczekuje się jego przestrzegania ([30]). Ponadto wytyczne nieustawowe (takie jak zatwierdzone praktyki zawodowe dotyczące zarządzania informacjami policyjnymi) muszą być zawsze spójne z kodeksem postępowania dotyczącym zarządzania informacjami policyjnymi, który jest w stosunku do nich nadrzędny ([31]). Chociaż może dochodzić do pewnych sytuacji operacyjnych, w których funkcjonariusze policji muszą odstąpić od stosowania tych wytycznych, w każdym przypadku nadal spoczywa na nich obowiązek przestrzegania wymogów określonych w części 3 DPA 2018 ([32]).

(18) Dalsze wytyczne dotyczące ustawodawstwa Zjednoczonego Królestwa w dziedzinie ochrony danych na potrzeby przetwarzania w sektorze organów ścigania przestępstw przedstawia Komisarz ds. Informacji ([33]) (więcej informacji na temat Komisarza ds. Informacji można znaleźć w motywach 93–109). Chociaż wytyczne te nie są prawnie wiążące, to w postępowaniu sądowym sądy musiałyby wziąć pod uwagę wszelkie naruszenia tych wytycznych, ponieważ mają one znaczenie dla wykładni i przedstawiają, w jaki sposób ustawodawstwo w dziedzinie ochrony danych jest interpretowane i egzekwowane przez Komisarza w praktyce ([34]).

(19) Ponadto, jak wspomniano w motywach 8–10, organy ścigania Zjednoczonego Królestwa muszą zapewnić zgodność z europejską konwencją praw człowieka i konwencją nr 108.

(20) Pod względem struktury i głównych elementów ramy prawne Zjednoczonego Królestwa regulujące przetwarzanie danych przez organy ścigania Zjednoczonego Królestwa są zatem bardzo podobne do ram obowiązujących w UE. 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**

(21) Zakres przedmiotowy części 3 DPA 2018 jest zbieżny z zakresem dyrektywy 2016/680 określonym w jej art. 2 ust. 2. Część 3 ma zastosowanie do przetwarzania danych osobowych przez właściwy organ w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania przez właściwy organ w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

(22) Ponadto, aby wchodzić w zakres części 3, administrator musi być „właściwym organem", a przetwarzanie musi odbywać się do „celów ścigania przestępstw". W związku z tym system ochrony danych oceniany w niniejszej decyzji ma zastosowanie do wszystkich działań związanych ze ściganiem przestępstw, podejmowanych przez te właściwe organy.

(23) Pojęcie „właściwego organu" zdefiniowano w art. 30 DPA jako osobę wymienioną w załączniku 7 do DPA 2018, a także jako inną osobę w zakresie, w jakim pełni ona funkcje ustawowe do jakichkolwiek celów ścigania przestępstw. 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-śled-

([30]) W sprawie Korona przeciwko Commission of Police of the Metropolis [2014] EWCA Civ 585 potwierdzono status prawny kodeksu postępowania dotyczącego zarządzania informacjami policyjnymi, a sędzia sądu apelacyjnego Laws stwierdził, że zgodnie z art. 39 A ustawy o policji z 1996 r. komendant policji metropolitalnej ma obowiązek uwzględniać kodeks postępowania dotyczący zarządzania informacjami policyjnymi oraz zatwierdzone praktyki zawodowe dotyczące zarządzania informacjami policyjnymi.

([31]) Policja podlega kontroli przestrzegania kodeksu postępowania dotyczącego zarządzania informacjami policyjnymi ze strony Inspektoratu Policji, Straży Pożarnej i Służb Ratowniczych Jej Królewskiej Mości (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services – HMICFRS).

([32]) Zob. stanowisko Kolegium Policyjnego w sprawie przestrzegania zatwierdzonych praktyk zawodowych we wszystkich obszarach działań policyjnych, w którym wyjaśniono, że „zatwierdzone praktyki zawodowe są zatwierdzane przez samorząd zawodowy policji (Kolegium Policyjne) jako oficjalne źródło policyjnych praktyk zawodowych. Od funkcjonariuszy i pracowników policji oczekuje się, że będą przestrzegali zatwierdzonych praktyk zawodowych przy wykonywaniu swoich obowiązków. Mogą jednak pojawić się okoliczności, w których odejście od zatwierdzonych praktyk zawodowych przez służbę będzie uzasadnione z operacyjnego punktu widzenia, pod warunkiem że istnieje wyraźne uzasadnienie takiego działania. Odpowiedzialność za zaistniałe na poziomie lokalnym lub krajowym ryzyko wynikłe z działania poza ramami wytycznych uzgodnionych na szczeblu krajowym ponosi dana służba, dlatego jeżeli w następstwie takiego działania dojdzie do incydentu lub dochodzenia (np. prowadzonego przez Niezależne Biuro ds. Postępowania Policji), to dana służba ponosi odpowiedzialność za wszelkie zagrożenia", dostępne pod adresem: https://www.app.college.police.uk/faq-page/.

([33]) Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Zob. sprawa Bridges przeciwko Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), w której pomimo odnotowania nieustawowego charakteru wytycznych Komisarza, Wysoki Trybunał stwierdził, że „[r]ozważając, czy administrator danych dopełnił obowiązku określonego w art. 64 [przeprowadzenie oceny skutków dla ochrony danych w odniesieniu do przetwarzania wysokiego ryzyka], Wysoki Trybunał uwzględni wytyczne wydane przez Komisarza ds. Informacji w odniesieniu do ocen skutków dla ochrony danych".

cze [np. Commissioner for Her Majesty's Revenue and Customs (organ podatkowy i celny Zjednoczonego Królestwa), 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) lub Krajowa Agencja ds. Zwalczania Przestępczości], organy prokuratorskie, inne organy wymiaru sprawiedliwości w sprawach karnych i inne podmioty uprawnione lub organizacje, które prowadzą działania związane ze ściganiem przestępstw ([35]). Część 3 DPA 2018 ma również zastosowanie do sądów i trybunałów, w przypadku gdy pełnią swoje funkcje sądowe, z wyjątkiem części dotyczącej praw osób, których dane dotyczą, i nadzoru Komisarza ds. Informacji ([36]). Wykaz właściwych organów przewidziany w załączniku 7 nie jest ostateczny i może być aktualizowany przez Sekretarza Stanu na mocy rozporządzenia z uwzględnieniem zmian w zakresie organizacji urzędów publicznych ([37]).

(24) Przedmiotowe przetwarzanie musi również służyć „celom ścigania przestępstw", które definiuje się jako zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochrona przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom ([38]). Przetwarzanie przez właściwy organ nie podlega przepisom części 3 DPA 2018, jeżeli nie odbywa się ono do celów ścigania przestępstw. Będzie to miało miejsce na przykład wówczas, gdy Competition and Markets Authority (urząd ds. konkurencji i rynków) będzie prowadził dochodzenia w sprawach, które nie dotyczą odpowiedzialności karnej (np. połączenia między przedsiębiorstwami). W takim przypadku zastosowanie będzie miało RODO UK wraz z częścią 2 DPA 2018, ponieważ przetwarzanie danych osobowych przez właściwe organy odbywa się do celów innych niż związane ze ściganiem przestępstw. Aby ustalić, które uregulowania dotyczące ochrony danych (część 3 czy część 2 DPA 2018) mają zastosowanie do przedmiotowego przetwarzania danych osobowych, właściwy organ, tj. administrator danych, musi rozważyć, czy „podstawowym celem" takiego przetwarzania jest jeden z celów ścigania przestępstw określonych w DPA 2018.

(25) Jeżeli chodzi o zakres terytorialny części 3 DPA 2018, art. 207 ust. 2 stanowi, że DPA ma zastosowanie do przetwarzania danych osobowych w kontekście działalności osoby, której zakres działań obejmuje terytorium całego Zjednoczonego Królestwa. Dotyczy to organów publicznych terytoriów Anglii, Walii, Szkocji i Irlandii Północnej, które wchodzą w zakres przedmiotowy części 3 DPA 2018 ([39]).

2.3.1. *Definicja danych osobowych i przetwarzania*

(26) Podstawowe pojęcia „danych osobowych" i „przetwarzania" zostały zdefiniowane w art. 3 DPA 2018 i stosuje się je w całej DPA. Definicje te są zbieżne z odpowiadającymi im definicjami określonymi w art. 3 dyrektywy 2016/680. Zgodnie z DPA 2018 dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ([40]). Zgodnie z art. 3 ust. 3 DPA 2018 osoba fizyczna jest możliwa do zidentyfikowania, jeżeli można ją bezpośrednio lub pośrednio zidentyfikować na podstawie informacji, w tym na podstawie imienia i nazwiska, numeru identyfikacyjnego lub jednej bądź kilku szczególnych cech określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość tej osoby. Pojęcie „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na informacjach lub zestawach informacji, takich jak: a) zbieranie, utrwalanie, organizowanie, porządkowanie lub przechowywanie; b) adaptowanie lub modyfikowanie; c) pobieranie, przeglądanie lub wykorzystywanie; d) ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie; e) dopasowywanie lub łączenie; lub f) ograniczanie, usuwanie lub niszczenie. Ponadto w ustawie zdefiniowano „przetwarzanie danych wrażliwych" jako: „a) przetwarzanie danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne bądź światopoglądowe lub przynależność do związków zawodowych; b) przetwarzanie danych genetycznych lub danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej; c) przetwarzanie danych dotyczących zdrowia; d) przetwarzanie danych dotyczących seksualności lub orientacji seksualnej osoby fizycznej" ([41]). W tym zakresie art. 205 DPA 2018 zawiera definicję „danych biometrycznych" ([42]), „danych dotyczących zdrowia" ([43]) i „danych genetycznych" ([44]).

([35]) Wymieniono je w załączniku 7 DPA 2018 i są to m.in. dyrektorzy prokuratury, Dyrektor Urzędu Prokuratury Irlandii Północnej lub Komisarz ds. Informacji.

([36]) Art. 43 ust. 3 DPA 2018.

([37]) Art. 30 ust. 3 DPA 2018. Służby wywiadowcze (Tajna Służba Wywiadowcza, Służba Bezpieczeństwa i Centrala Łączności Rządowej) nie są właściwymi organami (zob. art. 30 ust. 2 lit. DPA 2018) i część 3 DPA 2018 nie ma zastosowania do żadnych ich działań. Ich działania wchodzą w zakres części 4 DPA 2018.

([38]) Art. 31 DPA 2018.

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

([40]) Dane osobowe dotyczące osoby zmarłej nie są objęte zakresem stosowania DPA 2018.

([41]) Art. 35 ust. 8 DPA 2018.

([42]) „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.

([43]) „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.

([44]) „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.

(27) W art. 32 DPA 2018 doprecyzowano definicje „administratora" i „podmiotu przetwarzającego" w kontekście przetwarzania danych osobowych do celów ścigania przestępstw, ściśle wzorując się na równorzędnych definicjach zawartych w dyrektywie 2016/680. Administratorem jest właściwy organ, który ustala cele i sposoby przetwarzania danych osobowych. Jeżeli przetwarzanie jest wymagane przez przepisy prawa, administratorem jest właściwy organ, na który prawo nakłada taki obowiązek. Podmiot przetwarzający definiuje się jako każdą osobę, która przetwarza dane osobowe w imieniu administratora (inną niż osoba będąca pracownikiem administratora).

2.4. **Zabezpieczenia, prawa i obowiązki**

2.4.1. *Zgodność z prawem i rzetelność przetwarzania*

(28) Zgodnie z art. 35 DPA 2018 przetwarzanie danych osobowych musi być zgodne z prawem i rzetelne, podobnie jak określono w art. 4 ust. 1 lit. a) dyrektywy (UE) 2016/680. Zgodnie z art. 35 ust. 2 DPA 2018 przetwarzanie danych osobowych do jakichkolwiek celów ścigania przestępstw jest zgodne z prawem tylko wtedy, gdy opiera się na przepisach prawa oraz jeżeli osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie w tym celu albo przetwarzanie jest niezbędne do wykonania zadania realizowanego w tym celu przez właściwy organ.

2.4.1.1. Przetwarzanie na podstawie przepisów prawa

(29) Podobnie jak określono w art. 8 dyrektywy (UE) 2016/680, aby zapewnić zgodność z prawem przetwarzania objętego częścią 3 DPA 2018, takie przetwarzanie musi „opierać się na przepisach prawa". Przetwarzanie „zgodne z prawem" oznacza przetwarzanie dopuszczone przez ustawę, prawo precedensowe albo królewskie prerogatywy ([45]).

(30) Uprawnienia właściwych organów są zasadniczo regulowane ustawami, co oznacza, że funkcje i uprawnienia tych organów są wyraźnie określone w przepisach przyjętych przez Parlament ([46]). W niektórych przypadkach policja, jak również inne właściwe organy wymienione w załączniku 7 do DPA 2018, mogą powoływać się na prawo precedensowe w celu przetwarzania danych ([47]). Prawo precedensowe powstało dzięki precedensom ustalonym w orzeczeniach sądów. Prawo precedensowe jest istotne w kontekście uprawnień policji, która z tego źródła prawa wywodzi swój podstawowy obowiązek ochrony obywateli poprzez wykrywanie przestępstw i zapobieganie im ([48]). Wypełniając ten obowiązek, siły policyjne

([45]) Noty wyjaśniające do DPA 2018, pkt 181, dostępne pod adresem: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Na przykład uprawnienia Krajowej Agencji ds. Zwalczania Przestępczości wynikają z ustawy o przestępczości i sądach z 2013 r., dostępnej pod adresem https://www.legislation.gov.uk/ukpga/2013/22/contents. Podobnie uprawnienia Agencji ds. Norm Żywności przewidziano w ustawie o normach żywności z 1999 r., dostępnej pod adresem https://www.legislation.gov.uk/ukpga/1999/28/contents. Inne przykłady obejmują ustawę w sprawie ścigania przestępców z 1985 r., na mocy której utworzono Królewską Służbę Oskarżycielską (zob. https://www.legislation.gov.uk/ukpga/1985/23/contents); ustawę w sprawie Komisarzy Urzędu Skarbowego i Celnego z 2005 r., na mocy której ustanowiono Urząd Podatkowy i Celny Jej Królewskiej Mości (Her Majesty's Revenue and Customs) (zob. https://www.legislation.gov.uk/ukpga/2005/11/contents); ustawę o postępowaniu karnym (Szkocja) z 1995 r., na mocy której utworzono Szkocką Komisję Odwoławczą Spraw Karnych (zob. https://www.legislation.gov.uk/ukpga/1995/46/contents); ustawę o wymiarze sprawiedliwości (Irlandia Północna) z 2002 r., na mocy której ustanowiono prokuraturę w Irlandii Północnej (zob. https://www.legislation.gov.uk/ukpga/2002/26/contents) oraz Urząd ds. Poważnych Nadużyć Finansowych i nadano mu uprawnienia na mocy ustawy o wymiarze sprawiedliwości w sprawach karnych z 1987 r. (zob. https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Przykładowo, zgodnie z informacjami przekazanymi przez władze Zjednoczonego Królestwa, w ramach prokuratury (Crown Office and Procurator Fiscal Service) odpowiedzialnej za ściganie przestępstw w Szkocji, uprawnienia Prokuratora Generalnego stojącego na czele prokuratury w Szkocji do prowadzenia dochodzeń w sprawach dotyczących zgonów oraz ścigania przestępstw wynikają z prawa precedensowego, podczas gdy niektóre jego funkcje określono w ustawie. Ponadto uprawnienia Korony, a co za tym idzie, rządów, departamentów i ministrów, również wynikają z połączenia ustawodawstwa, prawa precedensowego i królewskiej prerogatywy (są to uprawnienia wynikające z prawa precedensowego przysługujące Koronie, ale wykonywane przez ministrów).

([48]) Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja F: ściganie przestępstw, s. 8 (zob. przypis 9).

opierają się jednak zarówno na prawie precedensowym, jak i na uprawnieniach ustawodawczych ([49]). Uprawnienia ustawowe policji mają pierwszeństwo przed wszelkimi uprawnieniami wynikającymi z prawa precedensowego ([50]).

(31) Sądy uznały, że zakres uprawnień i obowiązków funkcjonariuszy policji wynikających z prawa precedensowego obejmuje „wszelkie kroki, które wydają im się niezbędne do utrzymania pokoju, zapobiegania przestępczości lub ochrony mienia przed szkodami poniesionymi wskutek przestępstwa" ([51]). Uprawnienia wynikające z prawa precedensowego nie są pozbawione zastrzeżeń. Podlegają one licznym ograniczeniom, w tym ograniczeniom ustanowionym przez sądy ([52]) i prawodawstwo, w szczególności ustawę o prawach człowieka z 1998 r. i ustawę o równouprawnieniu z 2010 r ([53]). Ponadto w odniesieniu do właściwych organów przetwarzających dane na podstawie części 3 DPA 2018 dotyczy to wykonywania uprawnień wynikających z prawa precedensowego zgodnie z wymogami określonymi w DPA 2018 ([54]). Ponadto decyzja o wykonaniu jakiegokolwiek rodzaju przetwarzania danych musi uwzględniać wymogi obowiązujących wytycznych, takich jak kodeks postępowania dotyczący zarządzania informacjami policyjnymi, jak również wytyczne dotyczące jednego z państw Zjednoczonego Królestwa ([55]). Rząd i służby policji ds. operacyjnych wydają szereg wytycznych mających na celu zagwarantowanie, by funkcjonariusze policji wykonywali swoje uprawnienia w granicach określonych przez prawo precedensowe bądź wynikających z ustawy ([56]).

(32) Królewskie prerogatywy stanowią kolejny składnik „prawa" i odnoszą się do niektórych uprawnień powierzonych Koronie, a realizowanych przez władzę wykonawczą, które nie są oparte na ustawach, lecz wynikają z suwerenności monarchy ([57]). Istnieje bardzo niewiele przykładów uprawnień prerogatywnych, które są istotne w kontekście ścigania przestępstw. Dotyczą one na przykład ram wzajemnej pomocy prawnej umożliwiających Sekretarzowi Stanu udostępnianie państwom trzecim danych do celów ścigania przestępstw, przy czym uprawnienia do tego rodzaju

([49]) Najważniejsze akty prawne określające system głównych uprawnień policyjnych (aresztowanie, przeszukanie, zezwolenie na dalsze zatrzymanie, pobieranie odcisków palców, pobieranie próbek z miejsc intymnych, prowadzenie podsłuchu, dostęp do danych pochodzących z łączności) to: (i) w odniesieniu do Anglii i Walii – ustawa w sprawie policji i dowodów w sprawach karnych z 1984 r., dostępna pod adresem https://www.legislation.gov.uk/ukpga/1984/60/contents (zmieniona ustawą o ochronie wolności z 2012 r., dostępna pod adresem: https://www.legislation.gov.uk/ukpga/2012/9/contents) oraz ustawa o uprawnieniach dochodzeniowo-śledczych z 2016 r., dostępna pod adresem https://www.legislation.gov.uk/ukpga/2016/25/contents), (ii) w odniesieniu do Szkocji – ustawa w sprawie szkockiego wymiaru sprawiedliwości w sprawach karnych z 2016 r., dostępna pod adresem https://www.legislation.gov.uk/asp/2016/1/contents oraz ustawa o postępowaniu karnym (Szkocja) z 1995 r., dostępna pod adresem https://www.legislation.gov.uk/ukpga/1995/46/contents) (iii) w odniesieniu do Irlandii Północnej – zarządzenie w sprawie policji i dowodów w sprawach karnych (Irlandia Północna) z 1989 r., dostępne pod adresem https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Władze Zjednoczonego Królestwa wyjaśniły, że w Zjednoczonym Królestwie od dawna panuje nadrzędność prawa stanowionego, począwszy od wyroku w sprawie Entick przeciwko Carrington [1765] EWHC KB J98, w którym uznano, że istnieją ograniczenia w wykonywaniu uprawnień przez władzę wykonawczą i ustanowiono zasadę, że uprawnienia wynikające z prawa precedensowego oraz uprawnienia prerogatywne monarchy i rządu podlegają przepisom prawa krajowego.

([51]) Zob. sprawa Rice przeciwko Connolly [1966] 2 QB 414.

([52]) Zob. sprawa Korona (Catt) przeciwko Association of Chief Police Officers [2015] AC 1065, w której w odniesieniu do uprawnień policji do pozyskiwania i przechowywania informacji o osobie fizycznej (która popełniła przestępstwo), Lord Sumption orzekł, że zgodnie z prawem precedensowym policja jest uprawniona do uzyskiwania i przechowywania informacji dla celów policyjnych, tj. szeroko rozumianego utrzymania porządku publicznego oraz zapobiegania popełnianiu przestępstw i ich wykrywania. Uprawnienia te nie upoważniają do stosowania inwazyjnych metod pozyskiwania informacji, takich jak wejście na teren prywatny lub działania (inne niż aresztowanie na mocy uprawnień wynikających z prawa precedensowego), które stanowiłyby napaść. Sąd uznał, że w tej sprawie uprawnienia wynikające z prawa precedensowego były w pełni wystarczające, aby zezwolić na uzyskanie i przechowywanie informacji publicznych dotyczących tych odwołań.

([53]) Ustawa o równouprawnieniu z 2010 r., dostępna pod adresem https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Aby zapoznać się z przykładem sprawy, w której uprawnienia policji wynikające z prawa precedensowego są oceniane w ramach DPA 1998, zob. orzeczenie Wysokiego Trybunału w sprawie Bridges przeciwko Chief Constable of South Wales Police (zob. przypis 33). Zob. również sprawy Vidal-Hall przeciwko Google Inc [2015] EWCA Civ 311 i Richard przeciwko BBC [2018] EWHC 1837 (Ch).

([55]) Zob. np. wytyczne Policji Irlandii Północnej [The Police Service of Northern Ireland] dotyczące instrukcji służbowych w zakresie zarządzania rejestrami, dostępne pod adresem: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Izba Gmin opublikowała dokument informacyjny, w którym przedstawiono najważniejsze uprawnienia policji w Anglii i Walii wynikające z prawa precedensowego i ustawy (zob. https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Przykładowo, w dokumencie tym zaznaczono, że mimo iż uprawnienia do utrzymania „pokoju w Koronie", podobnie jak „użycie siły" i „prawo do zatrzymania i przeszukania" są uprawnieniami wywodzącymi się z prawa precedensowego, to zawsze wynikają z ustawy. Ponadto rząd szkocki podaje na swojej stronie internetowej informacje na temat uprawnień policji do aresztowania oraz zatrzymania i przeszukania (zob. https://www.gov.scot/policies/police/police-powers/).

([57]) Zgodnie z informacjami przekazanymi przez władze Zjednoczonego Królestwa uprawnienia prerogatywne wykonywane przez rząd obejmują na przykład zawieranie umów i ich ratyfikację, stosunki dyplomatyczne, użycie sił zbrojnych na terytorium Zjednoczonego Królestwa w celu utrzymania pokoju i wsparcia policji.

udostępniania danych nie zawsze są określone w ustawie ([58]). Królewskie prerogatywy są związane zasadami prawa precedensowego ([59]) i mają niższą rangę od ustawy, a zatem podlegają ograniczeniom przewidzianym w ustawie o prawach człowieka z 1998 r. i DPA 2018 ([60]).

(33) Podobnie jak określono w art. 8 dyrektywy (UE) 2016/680, przepisy Zjednoczonego Królestwa wymagają, aby w celu przestrzegania zasady zgodności z prawem właściwe organy zagwarantowały, by w przypadku gdy przetwarzanie opiera się na przepisach prawa, było ono również niezbędne do wykonania zadania realizowanego w celu ścigania przestępstw. Komisarz ds. Informacji udziela wytycznych w tym zakresie i wyjaśnia, że „musi być to ukierunkowany i proporcjonalny sposób osiągnięcia celu. Zasada zgodności z prawem nie będzie spełniona, jeżeli cel można osiągnąć w sposób zasadny za pomocą innych, mniej inwazyjnych środków. Nie wystarczy twierdzić, że przetwarzanie jest niezbędne ze względu na wybrany sposób prowadzenia działalności. Kluczowe znaczenie ma to, czy przetwarzanie jest niezbędne do osiągnięcia określonego celu" ([61]).

2.4.1.2. Przetwarzanie na podstawie „zgody" osoby, której dane dotyczą

(34) Jak wspomniano w motywie 28, art. 35 ust. 2 DPA 2018 przewiduje możliwość przetwarzania danych osobowych na podstawie „zgody" osoby fizycznej.

(35) Nie wydaje się jednak, aby zgoda stanowiła istotną podstawę prawną w odniesieniu do operacji przetwarzania wchodzących w zakres stosowania niniejszej decyzji. W rzeczywistości operacje przetwarzania objęte niniejszą decyzją zawsze będą dotyczyły danych, które zostały przekazane przez właściwy organ państwa członkowskiego właściwemu organowi Zjednoczonego Królestwa na podstawie dyrektywy (UE) 2016/680. Dlatego zazwyczaj nie będą one dotyczyły tego rodzaju bezpośredniej interakcji (zbierania) między organem publicznym a osobami, których dane dotyczą, która może opierać się na zgodzie w myśl art. 35 ust. 2 lit. a) ustawy DPA 2018.

(36) Chociaż poleganie na zgodzie nie jest zatem uznawane za istotne dla oceny przeprowadzonej na mocy niniejszej decyzji, warto zauważyć – w celu uzyskania pełnego obrazu sytuacji – że w kontekście ścigania przestępstw przetwarzanie danych nigdy nie odbywa się wyłącznie na podstawie zgody, ponieważ właściwy organ musi zawsze posiadać odpowiednie uprawnienia, które umożliwiają mu przetwarzanie danych ([62]). Mówiąc ściślej, oznacza to – podobnie do tego, co dopuszcza dyrektywa (UE) 2016/680 ([63]) – że zgoda służy jako dodatkowy warunek umożliwiający przeprowadzenie niektórych ograniczonych i szczególnych operacji przetwarzania, które w inny sposób nie mogłyby zostać przeprowadzone, na przykład pobranie i przetwarzanie próbki DNA osoby fizycznej niebędącej osobą podejrzaną. W tym przypadku przetwarzanie nie będzie mogło się odbyć, jeżeli nie wyrażono zgody lub została ona cofnięta ([64]).

([58]) W tym względzie zob. ocenę systemu Zjednoczonego Królestwa w zakresie dalszego przekazywania danych w motywach 74–87.

([59]) Zob. sprawa Bancoult przeciwko Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, w której sądy orzekły, że uprawnienia prerogatywne do wydawania zarządzeń w Radzie również podlegają zwykłym zasadom kontroli sądowej.

([60]) Zob. sprawa Attorney-General przeciwko De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, w której sąd orzekł, że nie można korzystać z uprawnień prerogatywnych, w przypadku gdy zastępują je uprawnienia ustawowe; sprawa Laker Airways Ltd przeciwko Department of Trade [1977] QB 643, w której sąd stwierdził, że nie można korzystać z uprawnień prerogatywnych w celu uniemożliwienia stosowania prawa stanowionego; sprawa Korona przeciwko Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, w której sąd orzekł, że nie można korzystać z uprawnień prerogatywnych, jeżeli są one sprzeczne z uchwalonymi przepisami, nawet jeżeli nie weszły one jeszcze w życie; sprawa Korona (Miller) przeciwko Secretary of State for Exiting the European Union [2017] UKSC 5, w której sąd potwierdził możliwość dostosowania i zniesienia uprawnień prerogatywnych przez prawo stanowione. Aby zapoznać się z ogólnym przeglądem relacji między królewskimi prerogatywami a uprawnieniami wynikającymi z ustawy lub prawa precedensowego, zob. dokument informacyjny Izby Gmin, dostępny pod adresem: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „O czym mówi pierwsza zasada?" dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Wynika to z brzmienia odpowiedniego przepisu DPA 2018, zgodnie z którym przetwarzanie danych osobowych do jakichkolwiek celów ścigania przestępstw jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – „opiera się na przepisach prawa" oraz jeżeli a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie w tym celu albo b) przetwarzanie jest niezbędne do wykonania zadania realizowanego w tym celu przez właściwy organ".

([63]) Zob. motywy 35 i 37 dyrektywy (UE) 2016/680.

([64]) Władze Zjednoczonego Królestwa wyjaśniły, że jednym z przykładowych przypadków, w których zgoda może stanowić odpowiednią podstawę uzasadniającą przetwarzanie danych, jest uzyskanie przez policję próbki DNA w odniesieniu do osoby zaginionej w celu dopasowania jej do ciała, jeżeli zostanie ono odnalezione. W takich okolicznościach zastosowanie przez policję przymusu wobec osoby, której dane dotyczą, w celu dostarczenia próbki byłoby niewłaściwe; zamiast tego policja zwróciłaby się z prośbą do danej osoby fizycznej o udzielenie zgody, która jest dobrowolna i którą można w każdej chwili cofnąć. Jeżeli zgoda zostanie wycofana, danych nie wolno dłużej przetwarzać, chyba że ustanowiono nową podstawę prawną uzasadniającą dalsze przetwarzanie próbki (np. osoba, której dane dotyczą, została uznana za osobę podejrzaną). Kolejnym przykładem może być sytuacja, gdy policja prowadzi dochodzenie w sprawie przestępstwa, którego ofiara (może to być ofiara rozboju, przestępstwa na tle seksualnym, przemocy domowej lub innego przestępstwa, a także krewni ofiary zabójstwa) mogłaby skorzystać ze skierowania do organizacji Victim Support (niezależnej organizacji charytatywnej wspierającej ofiary przestępstw i traumatycznych zdarzeń). W takim przypadku policja udostępnia organizacji Victim Support dane osobowe, takie jak nazwisko i dane kontaktowe ofiary, wyłącznie za jej zgodą.

(37) W przypadkach wymagających uzyskania zgody osoby fizycznej zgoda ta musi być jednoznaczna i obejmować wyraźne działanie potwierdzające ([65]). Od sił policyjnych wymaga się posiadania oświadczenia o ochronie prywatności, zawierającego m.in. niezbędne informacje związane z prawidłowym wykorzystywaniem zgody. Ponadto niektóre jednostki policji publikują dodatkowe materiały na temat sposobu, w jaki przestrzegają przepisów w dziedzinie ochrony danych, w tym jak i kiedy wykorzystują zgodę jako podstawę prawną ([66]).

2.4.1.3. Przetwarzanie danych wrażliwych

(38) Jeżeli przetwarzane są „szczególne kategorie" danych, powinny istnieć szczególne zabezpieczenia. W tym zakresie, podobnie jak przewidziano w art. 10 dyrektywy (UE) 2016/680, część 3 DPA 2018 przewiduje silniejsze zabezpieczenia w odniesieniu do tzw. „przetwarzania danych wrażliwych" ([67]).

(39) Zgodnie z art. 35 ust. 3 DPA 1998 właściwe organy mogą przetwarzać dane wrażliwe do celów ścigania przestępstw wyłącznie w dwóch przypadkach: 1) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie do celów ścigania przestępstw, a w chwili dokonywania przetwarzania administrator dysponuje odpowiednim dokumentem dotyczącym polityki ([68]); lub 2) przetwarzanie jest absolutnie niezbędne do celów ścigania przestępstw, przetwarzanie spełnia co najmniej jeden z warunków określonych w załączniku 8 do DPA 2018, a w chwili dokonywania przetwarzania administrator dysponuje odpowiednim dokumentem dotyczącym polityki ([69]).

(40) Jeżeli chodzi o pierwszy przypadek i jak wyjaśniono w motywie 38, poleganie na zgodzie nie jest uznawane za istotne w odniesieniu do objętego niniejszą decyzją rodzaju przekazywania danych ([70]).

(41) W przypadku gdy przetwarzanie danych wrażliwych nie odbywa się na podstawie zgody, przeprowadza się je z zastosowaniem jednego z warunków wymienionych w załączniku 8 do DPA 2018. Warunki te odnoszą się do przetwarzania niezbędnego do realizacji celów ustawowych; sprawowania wymiaru sprawiedliwości; ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; zabezpieczenia dzieci i osób fizycznych narażonych na ryzyko; roszczeń; czynności sądowych; zapobiegania nadużyciom finansowym; archiwizacji; w przypadku danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą. Z wyjątkiem przypadku, w którym dane zostały w sposób oczywisty upublicznione, wszystkie warunki określone w załączniku 8 podlegają kryterium „absolutnej niezbędności". Jak wyjaśnił Komisarz ds. Informacji, „absolutna niezbędność

([65]) Nie istnieje odrębna definicja „zgody" do celów przetwarzania danych osobowych na podstawie części 3 DPA 2018. Komisarz ds. Informacji przedstawił wytyczne dotyczące pojęcia „zgody" w ramach części 3 DPA 2018, wyjaśniając, że ma ona takie samo znaczenie jak definicja zawarta w RODO i powinna być do niej dostosowana, zwłaszcza że „zgoda musi być dobrowolna, konkretna i świadoma oraz musi istnieć rzeczywista możliwość dokonania wyboru w odniesieniu do wyrażenia zgody na przetwarzanie danych" (Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „O czym mówi pierwsza zasada?" (zob. przypis 64) i Przewodnik dotyczący ochrony danych w zakresie zgody, dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Zob. np. informacje na stronie internetowej policji z Lincolnshire (zob. https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) lub na stronie internetowej policji z West Yorkshire (zob. https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Art. 35 ust. 8 DPA 2018.

([68]) Art. 35 ust. 4 DPA 2018.

([69]) Art. 35 ust. 5 DPA 2018.

([70]) W celu uzyskania pełnego obrazu sytuacji warto zauważyć, że jeżeli przetwarzanie odbywa się na podstawie zgody, musi być ona dobrowolna, konkretna i świadoma oraz musi istnieć konkretna możliwość dokonania wyboru w odniesieniu do wyrażenia zgody na przetwarzanie danych. Ponadto od administratora wymaga się dysponowania „odpowiednim dokumentem dotyczącym polityki" w przypadku przetwarzania danych na podstawie zgody osoby, której dane dotyczą. W art. 42 DPA 2018 określono wymogi, które musi spełniać odpowiedni dokument dotyczący polityki. Wskazano, że dokument ten musi co najmniej zawierać wyjaśnienie procedur administratora w zakresie zapewniania zgodności z zasadami ochrony danych oraz polityki administratora w odniesieniu do zatrzymywania i usuwania danych osobowych. Zgodnie z art. 42 DPA 2018 oznacza to, że administrator musi przedstawić dokument, który a) zawiera wyjaśnienie procedur stosowanych przez niego w celu zapewnienia zgodności z zasadami ochrony danych; oraz b) zawiera wyjaśnienie polityki administratora w zakresie zatrzymywania i usuwania danych osobowych przetwarzanych na podstawie zgody osoby, której dane dotyczą, lub wskazuje, jak długo takie dane osobowe mogą być zatrzymywane. W szczególności dokument dotyczący polityki zobowiązuje administratora, aby w odniesieniu do obowiązku prowadzenia rejestru czynności przetwarzania zawsze uwzględniał elementy, o których mowa w lit. a) i b). Komisarz ds. Informacji opublikował wzór dokumentu (Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw. „Warunki przetwarzania danych wrażliwych", dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) i może zastosować środek przymusu, jeżeli administratorzy nie spełnią tych wymogów. Przy rozpatrywaniu potencjalnych naruszeń DPA 2018 sądy również poddają analizie odpowiedni dokument dotyczący polityki. Na przykład w niedawnej sprawie Korona (Bridges) przeciwko Chief Constable of South Wales Police sądy dokonały przeglądu odpowiedniego dokumentu dotyczącego polityki administratora i uznały, że jest on właściwy, ale mógłby zawierać więcej szczegółów. W związku z tym policja południowej Walii (South Wales Police) dokonała przeglądu odpowiedniego dokumentu dotyczącego polityki i zaktualizowała go zgodnie z nowymi wytycznymi Komisarza ds. Informacji (zob. przypis 33). Ponadto zgodnie z art. 42 ust. 3 DPA 2018 odpowiedni dokument dotyczący polityki powinien podlegać regularnemu przeglądowi ze strony administratora danych. Ponadto zgodnie z art. 42 ust. 4 DPA 2018 od administratora, w ramach dodatkowego zabezpieczenia, wymaga się prowadzenia rozszerzonego rejestru czynności przetwarzania, obejmującego dodatkowe elementy w stosunku do ogólnego obowiązku, który spoczywa na administratorze w zakresie prowadzenia rejestru czynności przetwarzania, określonego w art. 61 DPA 2018.

w tym kontekście oznacza, że przetwarzanie musi odnosić się do pilnej potrzeby społecznej, której nie można wypełnić w sposób zasadny za pomocą mniej inwazyjnych środków" ([71]). Ponadto niektóre z wymienionych warunków podlegają dodatkowym ograniczeniom. Na przykład, aby powołać się na warunek związany z „celami ustawowymi" i „warunek zabezpieczenia" (załącznik 8 pkt 1 i 4), należy spełnić dodatkowe kryterium istotnego interesu publicznego. Ponadto, w odniesieniu do warunków dotyczących zabezpieczenia dziecka (załącznik 8 pkt 4), osoba, której dane dotyczą, musi również być w określonym wieku i uznana za narażoną na ryzyko. Co więcej, administrator może zastosować warunek przewidziany w załączniku 8 pkt 4 wyłącznie w przypadku wystąpienia szczególnych okoliczności ([72]). Podobne ograniczenia wprowadzono dla warunków „czynności sądowych" i „zapobiegania nadużyciom finansowym" (załącznik 8, odpowiednio pkt 7 i 8). W obu przypadkach mają one zastosowanie wyłącznie do określonych administratorów. W przypadku czynności sądowych wyłącznie sąd lub inny organ sądowy może skorzystać z takiego warunku, a w przypadku zapobiegania nadużyciom finansowym wyłącznie administratorzy będący organizacjami zwalczającymi nadużycia finansowe mogą powoływać się na ten warunek.

(42) Oprócz tego, gdy przetwarzanie opiera się na jednym z warunków wymienionych w załączniku 8 i odbywa się odpowiednio zgodnie z art. 42 DPA 2018, musi istnieć „odpowiedni dokument dotyczący polityki" – zawierający wyjaśnienie procedur administratora w zakresie zapewniania zgodności z zasadami ochrony danych oraz polityki administratora w odniesieniu do zatrzymywania i usuwania danych osobowych – oraz mają zastosowanie obowiązki prowadzenia rozszerzonego rejestru.

2.4.2. *Ograniczenie celu*

(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. Ta zasada ochrony danych zagwarantowana jest w art. 36 DPA 2018. W przepisie tym, podobnie jak w art. 4 ust. 1 lit. b) dyrektywy (UE) 2016/680, wymaga się, aby: a) cel związany ze ściganiem przestępstw, dla którego w jakimkolwiek przypadku zbiera się dane osobowe, był konkretny, wyraźny i uzasadniony oraz b) danych osobowych zebranych w ten sposób nie przetwarzano w sposób niezgodny z celem, dla którego je zebrano.

(44) W przypadku gdy właściwe organy przetwarzają dane do celów ścigania przestępstw, może to obejmować archiwizację, badania naukowe lub historyczne oraz cele statystyczne ([73]). W odniesieniu do takich przypadków w DPA 2018 wyjaśniono również, że archiwizacja (lub przetwarzanie do celów badań naukowych lub historycznych oraz do celów statystycznych) nie jest dozwolona, jeżeli przeprowadza się ją w związku z decyzjami podjętymi w stosunku do konkretnej osoby, której dane dotyczą, lub jeżeli może spowodować u niej znaczną szkodę lub cierpienie ([74]).

2.4.3. *Prawidłowość i minimalizacja danych*

(45) Dane powinny być prawidłowe i w razie potrzeby uaktualniane. Powinny być one również adekwatne, stosowne i nienadmierne w stosunku do celów, w których są przetwarzane. Przestrzeganie tych zasad, określonych w art. 4 ust. 1 lit. c), d) i e) dyrektywy (UE) 2016/680, zapewniono również w art. 37 i 38 DPA 2018. Należy podjąć wszelkie uzasadnione działania, aby zapewnić, że dane osobowe, które są nieprawidłowe ([75]) zostaną bezzwłocznie usunięte lub spros-

([71]) Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „Warunki przetwarzania danych wrażliwych" (zob. przypis 70).

([72]) Przetwarzanie odbywa się bez zgody osoby, której dane dotyczą, gdy: a) osoba, której dane dotyczą, nie może udzielić zgody na przetwarzanie; b) nie można w sposób uzasadniony oczekiwać od administratora, że uzyska zgodę osoby, której dane dotyczą, na przetwarzanie; c) przetwarzanie musi być dokonane bez zgody osoby, której dane dotyczą, ponieważ uzyskanie jej zgody naruszyłoby zapewnienie ochrony, o której mowa w pkt 1 lit. a).

([73]) Zob. art. 41 ust. 1 DPA 2018.

([74]) Zob. art. 41 ust. 2 DPA 2018.

([75]) W art. 205 DPA 2018 zdefiniowano termin „nieprawidłowe" jako „niepoprawne lub wprowadzające w błąd" dane osobowe. Władze Zjednoczonego Królestwa wyjaśniły, że typowe jest to, że dane związane z postępowaniami przygotowawczymi są często niekompletne, ale niezależnie od tego mogą być prawidłowe.

towane ([76]), biorąc pod uwagę cel związany ze ściganiem przestępstw, dla którego są przetwarzane ([77]), oraz aby zapewnić, by dane osobowe, które są niedokładne, niekompletne lub już nieaktualne, nie były przekazywane ani udostępniane do żadnego z celów związanych ze ściganiem przestępstwa ([78]).

(46) Ponadto, podobnie jak w art. 7 dyrektywy (UE) 2016/680, w ramach systemu ochrony danych Zjednoczonego Królestwa określono, że dane osobowe oparte na faktach muszą być odróżniane, tak dalece, jak to możliwe, od danych osobowych opartych na indywidualnych ocenach ([79]). W stosownych przypadkach i w miarę możliwości należy dokonać wyraźnego rozróżnienia między danymi osobowymi odnoszącymi się do różnych kategorii osób, których dane dotyczą, takich jak osoby podejrzane, osoby skazane za czyn zabroniony, ofiary czynu zabronionego i świadkowie ([80]).

2.4.4. *Ograniczenie przechowywania*

(47) Zgodnie z art. 5 dyrektywy (UE) 2016/680 dane powinny być co do zasady przechowywane przez okres nie dłuższy, niż jest to niezbędne do celów, w których przetwarza się dane osobowe. Zgodnie z art. 39 DPA 2018, podobnie jak określono w art. 5 tej dyrektywy, zabronione jest przechowywanie danych osobowych przetwarzanych dla któregokolwiek z celów związanych ze ściganiem przestępstw dłużej, niż jest to konieczne w związku z celem, dla którego się je przetwarza. System prawny Zjednoczonego Królestwa wymaga ustanowienia odpowiednich terminów dla okresowego przeglądu potrzeby dalszego przechowywania danych osobowych dla któregokolwiek z celów związanych ze ściganiem przestępstw. Dalsze zasady dotyczące praktyk związanych z zatrzymywaniem danych osobowych oraz obowiązujące terminy określono w odpowiednich przepisach i wytycznych regulujących uprawnienia i funkcjonowanie policji. Na przykład w Anglii i Walii kodeks postępowania dotyczący zarządzania informacjami policyjnymi [MoPI Code of Practice] Kolegium Policyjnego wraz z zatwierdzonymi praktykami zawodowymi dotyczącymi zarządzania informacjami policyjnymi [APP Guidance on the Management of Police Information] stanowi ramy zapewniające spójny, oparty na analizie ryzyka proces zatrzymywania, przeglądu i usuwania danych w odniesieniu do zarządzania operacyjnymi informacjami policyjnymi ([81]). Za pośrednictwem tych ram określono jasne oczekiwania dla wszystkich służb co do tego, jak należy tworzyć, udostępniać i wykorzystywać informacje oraz zarządzać nimi w obrębie poszczególnych sił policyjnych i innych agencji oraz pomiędzy tymi podmiotami ([82]). Oczekuje się, że policja będzie przestrzegać kodeksu postępowania, a zgodność z nim weryfikuje Inspektorat Policji, Straży Pożarnej i Służb Ratowniczych Jej Królewskiej Mości (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services) ([83]).

(48) Policja Irlandii Północnej (The Police Service of Northern Ireland, PSNI) nie jest prawnie zobowiązana do przestrzegania kodeksu postępowania dotyczącego zarządzania informacjami policyjnymi. Ramy dotyczące zarządzania informacjami policyjnymi przyjęte w 2011 r. uzupełniono jednak w podręczniku PSNI ([84]), w którym określono zasady i procedury dotyczące sposobu stosowania kodeksu postępowania dotyczącego zarządzania informacjami policyjnymi w Irlandii Północnej.

([76]) Art. 38 ust. 1 lit. b) DPA 2018.

([77]) Zgodnie z Ramami wyjaśniającymi Zjednoczonego Królestwa dotyczącymi dyskusji na temat odpowiedniego stopnia ochrony „zapewnia to uznanie zarówno praw osób, których dane dotyczą, jak i potrzeb operacyjnych organów ścigania. Powyższy punkt dokładnie rozważono na etapie opracowywania projektu ustawy o ochronie danych, ponieważ mogą istnieć szczególne i ograniczone powody operacyjne, dla których nie można sprostować danych. Najprawdopodobniej będzie to miało miejsce w przypadku konieczności zachowania nieprawidłowych danych osobowych w ich pierwotnej formie do celów dowodowych" (zob. Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja F: ściganie przestępstw, s. 21, zob. przypis 9).

([78]) Art. 38 ust. 4 DPA 2018. Ponadto zgodnie z art. 38 ust. 5 DPA 2018 jakość danych osobowych należy weryfikować przed ich przekazaniem lub udostępnieniem; we wszystkich przypadkach przesyłania danych osobowych muszą być zawarte niezbędne informacje umożliwiające odbiorcy ocenę stopnia prawidłowości, kompletności i wiarygodności danych oraz stopnia ich aktualności, a jeżeli po przekazaniu danych osobowych okaże się, że dane były nieprawidłowe lub że ich przekazanie było niezgodne z prawem, należy bezzwłocznie powiadomić odbiorcę.

([79]) Art. 38 ust. 2 DPA 2018.

([80]) Art. 38 ust. 3 DPA 2018.

([81]) Ramy te zapewniają spójność w stosowaniu zasad dotyczących przechowywania pozyskanych danych osobowych. Okres przeglądu zależy od przestępstw, które są podzielone na 4 grupy: 1) niektóre sprawy z zakresu ochrony publicznej; 2) inne przestępstwa na tle seksualnym z użyciem przemocy i poważne przestępstwa; 3) wszystkie inne przestępstwa; 4) różne. Więcej szczegółowych informacji można znaleźć w Zatwierdzonych praktykach zawodowych dotyczących zarządzania informacjami policyjnymi (zob. przypis 26).

([82]) Zgodnie z informacjami przekazanymi przez władze Zjednoczonego Królestwa, inne organizacje mogą swobodnie przestrzegać zasad kodeksu postępowania dotyczącego zarządzania informacjami policyjnymi (MoPI Code of Practice), jeżeli tak zdecydują, na przykład Urząd Podatkowy i Celny Jej Królewskiej Mości (Her Majesty's Revenue and Customs) oraz Krajowa Agencja ds. Zwalczania Przestępczości dobrowolnie przyjmują wiele zasad tego kodeksu postępowania, aby zapewnić spójność w zakresie ścigania przestępstw. Ogólnie rzecz biorąc, większość organizacji zapewnia swoim pracownikom szczegółowe polityki i wytyczne dla całego personelu dotyczące sposobu postępowania z danymi osobowymi w ramach pełnionej przez nich funkcji, które to polityki i wytyczne są dostosowane do konkretnej organizacji. Zazwyczaj obejmuje to również obowiązkowe szkolenia.

([83]) Kodeks postępowania dotyczący zarządzania informacjami policyjnymi (MoPI Code of Practice) wydano na mocy uprawnień wynikających z ustawy o policji z 1996 r., która umożliwia Kolegium Policyjnemu wydawanie kodeksów postępowania związanych ze skutecznym funkcjonowaniem policji. Każdy kodeks postępowania opracowany na podstawie wspomnianej ustawy musi zostać zatwierdzony przez Sekretarza Stanu i zanim zostanie zaprezentowany w parlamencie podlega konsultacji Krajowej Agencji ds. Zwalczania Przestępczości. W art. 39 A ust. 7 ustawy o policji z 1996 r. nakłada się na policję wymóg należytego poszanowania kodeksów wydanych na podstawie ustawy o policji z 1996 r.

([84]) PSNI MoPI Handbook [Podręcznik Policji Irlandii Północnej dotyczący zarządzania informacjami policyjnymi], rozdziały 1–6.

(49) W Szkocji siły policyjne opierają się na obowiązującej procedurze działania dotyczącej zatrzymywania rejestrów ([85]), która służy wsparciu polityki zarządzania rejestrami Policji Szkocji (The Police Service of Scotland) ([86]). W tej obowiązującej procedurze działania określono szczegółowe zasady zatrzymywania rejestrów będących w posiadaniu Policji Szkocji.

(50) Oprócz nadrzędnego wymogu przeglądu rejestrów, który ma zastosowanie w całym Zjednoczonym Królestwie, więcej szczegółowych informacji zawarto w przepisach lokalnych. Aby podać kilka przykładów, w odniesieniu do Anglii i Walii, ustawa w sprawie policji i dowodów w sprawach karnych, zmieniona ustawą o ochronie wolności z 2012 r. (Protection of Freedom Act), zawiera przepisy dotyczące zatrzymywania odcisków palców i profili DNA, jak również szczegółowe uregulowania dotyczące osób, które nie zostały skazane ([87]). Na podstawie ustawy o ochronie wolności utworzono również stanowisko Komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego (Commissioner for the Retention and Use of Biometric Material, „Komisarz ds. Biometrii") ([88]). Przepisy szczegółowe dotyczące wizerunków osób zatrzymanych określono w przeglądzie dotyczącym wizerunków osób zatrzymanych [Custody Image Review] z 2017 r. ([89]) Jeżeli chodzi o Szkocję, w ustawie o postępowaniu karnym (Szkocja) z 1995 r. określono zasady dotyczące pozyskiwania i zatrzymywania odcisków palców i próbek biologicznych ([90]). Podobnie jak w przypadku Anglii i Walii, w ustawodawstwie uregulowano zatrzymywanie danych biometrycznych w różnych przypadkach ([91]).

2.4.5. *Bezpieczeństwo danych*

(51) Dane osobowe muszą być 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 organy publiczne 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.

(52) Zasady te znajdują odzwierciedlenie w art. 40 DPA 2018, zgodnie z którym, podobnie jak określono w art. 4 ust. 1 lit. f) dyrektywy (UE) 2016/680, dane osobowe przetwarzane w którymkolwiek z celów związanych ze ściganiem przestępstw muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, za

([85]) Obowiązująca procedura działania dotycząca zatrzymywania rejestrów, dostępna pod adresem: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Więcej szczegółowych informacji na temat zarządzania rejestrami można znaleźć w informacjach związanych z National Records of Scotland, dostępnych pod adresem: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Okresy zatrzymywania różnią się w zależności od tego, czy dana osoba została skazana, czy nie (art. 63I–63KI ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.). Na przykład w przypadku osoby dorosłej skazanej za przestępstwo podlegające wpisowi do rejestru, jej odciski palców i profil DNA mogą być zatrzymywane przez czas nieokreślony (art. 63I ust. 2 ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.), natomiast okres zatrzymywania jest ograniczony, jeżeli osoba skazana ma mniej niż 18 lat, popełniła wykroczenie podlegające wpisowi do rejestru i nie była wcześniej skazana (art. 63K ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.). Okres zatrzymywania danych w przypadku osoby aresztowanej lub oskarżonej, ale nie skazanej, jest ograniczony do trzech lat (art. 63F ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.). Przedłużenie tego okresu zatrzymywania musi zatwierdzić organ sądowy (art. 63F ust. 7 ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.). W przypadku osób aresztowanych lub oskarżonych, ale nie skazanych za wykroczenie, zatrzymywanie nie jest możliwe (art. 63D i art. 63H ustawy w sprawie policji i dowodów w sprawach karnych z 1984 r.).

([88]) W art. 20 ustawy o ochronie wolności z 2012 r. ustanowiono stanowisko Komisarza ds. Biometrii. 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: Kodeks zarządzania w zakresie nominacji publicznych – GOV.UK (www.gov.uk)), 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.

([89]) Przegląd wykorzystywania i zatrzymywania wizerunków osób zatrzymanych, dostępny pod adresem: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Art. 18 i nast. ustawy o postępowaniu karnym (Szkocja) z 1995 r.

([91]) Okresy zatrzymywania różnią się w zależności od tego, czy dana osoba została skazana (art. 18 ust. 3 ustawy o postępowaniu karnym (Szkocja) z 1995 r.) lub czy jest nieletnia. W drugim z powyższych przypadków okres zatrzymywania wynosi 3 lata od wyroku skazującego wydanego przez sąd ds. osób nieletnich (art. 18E ust. 8 ustawy o postępowaniu karnym (Szkocja) z 1995 r.). Nie można zatrzymywać danych osób aresztowanych, ale nie skazanych (art. 18 ust. 3 ustawy o postępowaniu karnym (Szkocja) z 1995 r.), z wyjątkiem szczególnych przypadków i w zależności od wagi przestępstwa (art. 18 A ustawy o postępowaniu karnym (Szkocja) z 1995 r.). W ustawie o szkockim Komisarzu ds. Biometrii z 2020 r. (zob. https://www.legislation.gov.uk/asp/2020/8/contents) ustanowiono stanowisko szkockiego Komisarza ds. Biometrii, który przygotowuje i weryfikuje kodeksy postępowania (zatwierdzone przez Parlament Szkocki) dotyczące pozyskiwania, zatrzymywania, wykorzystywania i niszczenia danych biometrycznych na potrzeby wymiaru sprawiedliwości w sprawach karnych i policji (art. 7 ustawy o szkockim Komisarzu ds. Biometrii z 2020 r.).

pomocą odpowiednich środków technicznych lub organizacyjnych. Obejmuje to ochronę danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem ([92]). W art. 66 DPA 2018 określono ponadto, że każdy administrator i każdy podmiot przetwarzający musi wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiedni do ryzyka wynikającego z przetwarzania danych osobowych. Zgodnie z notami wyjaśniającymi administrator musi ocenić ryzyko i na podstawie tej oceny wdrożyć odpowiednie środki bezpieczeństwa, na przykład szyfrowanie lub określone poziomy poświadczenia bezpieczeństwa dla personelu przetwarzającego dane ([93]). W ocenie należy również uwzględnić np. charakter przetwarzanych danych oraz wszelkie inne istotne czynniki lub okoliczności, które mogą mieć wpływ na bezpieczeństwo przetwarzania.

(53) Przepisy regulujące zgodność z zasadami bezpieczeństwa danych są bardzo podobne do uregulowań zawartych w art. 29–31 dyrektywy (UE) 2016/680. W szczególności w przypadku naruszenia ochrony danych osobowych w odniesieniu do danych osobowych, za które odpowiada administrator, zgodnie z art. 67 ust. 1 DPA 2018 administrator musi bez zbędnej zwłoki, w miarę możliwości nie później niż 72 godziny od powzięcia wiadomości o naruszeniu, zgłosić naruszenie ochrony danych osobowych Komisarzowi ds. Informacji ([94]). Obowiązek zgłoszenia nie ma zastosowania, gdy jest mało prawdopodobne, że naruszenie ochrony danych osobowych spowoduje ryzyko naruszenia praw i wolności osób fizycznych ([95]). Administrator musi udokumentować fakty związane z każdym naruszeniem ochrony danych osobowych, jego skutki i podjęte działania naprawcze w sposób umożliwiający Komisarzowi ds. Informacji sprawdzenie zgodności z DPA ([96]). Jeżeli podmiot przetwarzający dane stwierdzi naruszenie bezpieczeństwa, musi on bez zbędnej zwłoki zgłosić je administratorowi ([97]).

(54) Zgodnie z art. 68 ust. 1 DPA 2018, jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu ([98]). Zawiadomienie musi zawierać te same informacje co zawiadomienie skierowane do Komisarza ds. Informacji opisane w motywie 53. Obowiązek ten nie ma zastosowania, jeżeli administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony, które zastosowano do danych osobowych, których dotyczyło naruszenie. Nie ma on również zastosowania, jeżeli administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osób, których dane dotyczą. Ponadto administrator nie jest zobowiązany do zawiadomienia osoby, której dane dotyczą, jeżeli wymagałoby to niewspółmiernie dużego wysiłku ([99]). W takim przypadku osobę, której dane dotyczą, należy poinformować w inny równie skuteczny sposób, np. poprzez publiczny komunikat ([100]). Jeżeli administrator nie poinformował osoby, której dane dotyczą, o naruszeniu, Komisarz ds. Informacji, po otrzymaniu zawiadomienia zgodnie z art. 67 DPA i po rozważeniu prawdopodobieństwa, że naruszenie spowoduje wysokie ryzyko, może zobowiązać administratora do zawiadomienia osoby, której dane dotyczą, o naruszeniu ([101]).

([92]) Zgodnie z notami wyjaśniającymi do DPA 2018 (zob. przypis 45), administrator musi w szczególności: zaprojektować i zorganizować swoje zabezpieczenia tak, aby dopasować je do charakteru przechowywanych przez niego danych osobowych oraz szkód, jakie mogą wyniknąć z naruszenia bezpieczeństwa; jasno określić, kto w jego organizacji odpowiada za zapewnienie bezpieczeństwa informacji; upewnić się, że posiada odpowiednie zabezpieczenia fizyczne i techniczne, wspierane przez solidne polityki i procedury, oraz rzetelny, dobrze wyszkolony personel; oraz być gotowy do szybkiej i skutecznej reakcji na każde naruszenie bezpieczeństwa.

([93]) Pkt 221 not wyjaśniających do DPA 2018 (zob. przypis 45).

([94]) Art. 67 ust. 4 DPA 2018 stanowi, że zawiadomienie musi zawierać opis charakteru naruszenia ochrony danych osobowych (w tym, w miarę możliwości, kategorie i przybliżoną liczbę osób, których dane dotyczą, a także kategorie i przybliżoną liczbę zapisów danych osobowych, których dotyczy naruszenie), nazwę i dane kontaktowe punktu kontaktowego, opis prawdopodobnych konsekwencji naruszenia ochrony danych osobowych oraz opis środków wdrożonych lub proponowanych do wdrożenia przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych (w tym, w stosownych przypadkach, środków mających na celu złagodzenie jego ewentualnych negatywnych skutków).

([95]) Art. 67 ust. 2 DPA 2018.

([96]) Art. 67 ust. 6 DPA 2018.

([97]) Art. 67 ust. 9 DPA 2018.

([98]) Zgodnie z art. 68 ust. 7 DPA 2018 administrator może ograniczyć, w całości lub w części, przekazywanie informacji osobie, której dane dotyczą, w takim zakresie i tak długo, jak długo ograniczenie to jest – uwzględniając prawa podstawowe i prawnie uzasadnione interesy osoby, której dane dotyczą – środkiem niezbędnym i proporcjonalnym, aby a) uniemożliwić utrudnianie czynności postępowania urzędowego lub sądowego, postępowania przygotowawczego lub procedury; b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar; c) chronić bezpieczeństwo publiczne; d) chronić bezpieczeństwo narodowe; e) chronić prawa i wolności innych osób.

([99]) Art. 68 ust. 3 DPA 2018.

([100]) Art. 68 ust. 5 DPA 2018.

([101]) Art. 68 ust. 6 DPA 2018, z zastrzeżeniem ograniczenia przewidzianego w art. 68 ust. 8 DPA 2018.

2.4.6. *Przejrzystość*

(55) Osoby, których dane dotyczą, muszą być informowane o głównych cechach przetwarzania ich danych osobowych. Ta zasada ochrony danych znajduje odzwierciedlenie w art. 44 DPA 2018, który podobnie jak art. 13 dyrektywy (UE) 2016/680 stanowi, że administrator ma ogólny obowiązek udostępniania osobom, których dane dotyczą, informacji o przetwarzaniu ich danych osobowych (poprzez ogólne udostępnienie informacji do wiadomości publicznej lub w dowolny inny sposób) ([102]). Informacje, których udostępnienie jest wymagane, obejmują a) tożsamość i dane kontaktowe administratora; b) dane kontaktowe inspektora ochrony danych, w razie potrzeby; c) cele, do których administrator przetwarza dane osobowe; d) informacje o prawie osoby, której dane dotyczą, do żądania od administratora dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych, a także ograniczenia ich przetwarzania; oraz e) informacje o prawie do wniesienia skargi do Komisarza ds. Informacji oraz dane kontaktowe Komisarza ([103]).

(56) W szczególnych przypadkach w celu umożliwienia osobie, której dane dotyczą, wykonania jej praw określonych w DPA 2018 (np. gdy przetwarzane dane osobowe zebrano bez wiedzy osoby, której dane dotyczą) administrator musi również udzielić osobie, której dane dotyczą, informacji o a) podstawie prawnej przetwarzania; b) informacji o okresie przechowywania danych osobowych lub, gdy nie jest to możliwe, kryteriach służących określeniu tego okresu; c) w stosownym przypadku informacji o kategoriach odbiorców danych osobowych (w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych); d) takich dalszych informacji, jakie są niezbędne do umożliwienia osobie, której dane dotyczą, wykonania jej praw określonych w części 3 DPA 2018 ([104]).

2.4.7. *Prawa indywidualne*

(57) Osobom, których dane dotyczą, należy przyznać szereg możliwych do wyegzekwowania praw. W części 3 rozdział 3 DPA 2018 zapewniono osobom fizycznym prawa dostępu, sprostowania i usunięcia oraz ograniczenia ([105]), które są porównywalne z prawami przewidzianymi w rozdziale 3 dyrektywy (UE) 2016/680.

(58) Prawo dostępu określono w art. 45 DPA 2018. Po pierwsze osoba fizyczna jest uprawniona do uzyskania od administratora potwierdzenia, czy jej dane osobowe są przetwarzane, czy nie ([106]). Po drugie, jeżeli dane osobowe są przetwarzane, osoba, której dane dotyczą, ma prawo dostępu do tych danych i otrzymania następujących informacji na temat przetwarzania: a) celów i podstaw prawnych przetwarzania; b) kategorii odnośnych danych; c) odbiorcy, któremu ujawniono dane; d) okresu przechowywania danych osobowych; e) prawa osoby, której dane dotyczą, do sprostowania i usunięcia danych osobowych; f) prawa do wniesienia skargi; oraz g) wszelkich informacji o pochodzeniu odnośnych danych osobowych ([107]).

(59) Zgodnie z art. 46 DPA 2018 osoba, której dane dotyczą, ma prawo zażądać od administratora sprostowania nieprawidłowych danych osobowych, które jej dotyczą. Administrator musi sprostować (lub, jeżeli dane są nieprawidłowe, ponieważ są niekompletne, uzupełnić) dane bez zbędnej zwłoki. Jeżeli dane osobowe muszą być przechowywane do celów dowodowych, administrator musi (zamiast sprostowania danych osobowych) ograniczyć ich przetwarzanie ([108]).

([102]) W Przewodniku dotyczącym przetwarzania danych do celów ścigania przestępstw podano następujący przykład: „Na stronie internetowej znajduje się ogólne oświadczenie o ochronie prywatności, które zawiera podstawowe informacje o organizacji, celu przetwarzania danych osobowych, prawach osoby, której dane dotyczą, oraz jej prawie do wniesienia skargi do Komisarza ds. Informacji. Dysponujesz danymi wywiadowczymi o tym, że pewna osoba fizyczna była obecna w miejscu popełnienia przestępstwa w czasie, gdy do niego doszło. Podczas pierwszego przesłuchania tej osoby fizycznej należy podać jej ogólne informacje, jak również dalsze informacje uzupełniające, aby umożliwić tej osobie korzystanie z jej praw. Zakres przekazywanych informacji dotyczących rzetelnego przetwarzania można ograniczyć wyłącznie wtedy, gdy ich podanie będzie miało negatywny wpływ na prowadzenie postępowania przygotowawczego" (Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „Jakie informacje należy przekazać osobie fizycznej?", dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) W Przewodniku dotyczącym przetwarzania danych do celów ścigania przestępstw podano, że przekazywane informacje na temat przetwarzania danych osobowych muszą być zwięzłe, zrozumiałe i łatwo dostępne; napisane jasnym i prostym językiem, z dostosowaniem go do potrzeb osób wymagających szczególnego traktowania, takich jak dzieci; oraz nieodpłatne (Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „W jaki sposób należy przekazywać te informacje?", dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Art. 44 ust. 2 DPA 2018.

([105]) Szczegółową analizę praw osób, których dane dotyczą, można znaleźć w: Przewodniku dotyczącym przetwarzania danych do celów ścigania przestępstw, w części dotyczącej praw indywidualnych, dostępnej pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Art. 45 ust. 1 DPA 2018.

([107]) Art. 45 ust. 2 DPA 2018.

([108]) Art. 46 ust. 4 DPA 2018.

(60) W art. 47 DPA 2018 zapewniono osobom fizycznym prawo do usunięcia danych i ograniczenia przetwarzania. Administrator musi ([109]) usunąć dane osobowe bez zbędnej zwłoki, jeżeli przetwarzanie danych osobowych naruszałoby którąkolwiek z zasad ochrony danych, podstawy prawne przetwarzania lub zabezpieczenia związane z archiwizacją i przetwarzaniem danych wrażliwych. Administrator musi również usunąć dane, jeżeli jest do tego prawnie zobowiązany. Jeżeli dane osobowe muszą być przechowywane do celów dowodowych, administrator musi (zamiast sprostowania danych osobowych) ograniczyć ich przetwarzanie ([110]). Administrator musi ograniczyć przetwarzanie danych osobowych, jeżeli osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych, ale nie jest możliwe ustalenie, czy są one prawidłowe, czy nie ([111]).

(61) Jeżeli osoba, której dane dotyczą, zażąda sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania, administrator musi poinformować osobę, której dane dotyczą, na piśmie, czy uwzględniono wniosek, a jeżeli go odrzucono, poinformować osobę, której dane dotyczą, o przyczynach odmowy i dostępnych środkach zaskarżenia (prawie osoby, której dane dotyczą, do złożenia wniosku do Komisarza ds. Informacji o zbadanie, czy ograniczenie zastosowano zgodnie z prawem, prawie do wniesienia skargi do Komisarza ds. Informacji oraz prawie do wystąpienia do sądu o wydanie nakazu dostosowania się do przepisów) ([112]).

(62) Jeżeli administrator danych dokonuje sprostowania danych osobowych otrzymanych od innego właściwego organu, powiadamia on ten drugi organ ([113]). W przypadku sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych, które ujawnił administrator, powiadamia on odbiorców, a odbiorcy podobnie dokonują sprostowania danych osobowych, usuwają je lub ograniczają ich przetwarzanie (w zakresie, w jakim zachowują za nie odpowiedzialność) ([114]).

(63) Ponadto osoba, której dane dotyczą, ma prawo być bez zbędnej zwłoki poinformowana przez administratora o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych ([115]).

(64) W związku z powyższymi prawami osoby, której dane dotyczą, podobnie jak przewidziano w art. 12 dyrektywy (UE) 2016/680, administrator ma obowiązek zapewnić, by wszelkie informacje kierowane do osoby, której dane dotyczą, były przekazywane jej w zwięzłej, zrozumiałej i łatwo dostępnej formie ([116]), a w miarę możliwości należy je przekazywać w takiej samej formie, w jakiej złożono wniosek ([117]). Administrator musi zastosować się do wniosku osoby, której dane dotyczą, bez zbędnej zwłoki, a w każdym razie co do zasady przed upływem jednego miesiąca od złożenia wniosku ([118]). Jeżeli administrator ma zasadne wątpliwości co do tożsamości osoby fizycznej, może on zażądać dodatkowych informacji i opóźnić rozpatrzenie wniosku do czasu ustalenia jej tożsamości. Administrator może zażądać zasadnej opłaty lub odmówić działania, jeżeli uzna żądanie za wyraźnie nieuzasadnione ([119]). Komisarz ds. Informacji wydał wytyczne dotyczące tego, kiedy wniosek uznaje się za wyraźnie nieuzasadniony lub wygórowany i kiedy można żądać opłaty ([120]).

(65) Ponadto, zgodnie z art. 53 ust. 4 DPA 2018, Sekretarz Stanu może w drodze rozporządzeń określić maksymalną wysokość opłaty.

([109]) Osoba, której dane dotyczą, może zwrócić się do administratora z wnioskiem o usunięcie danych osobowych lub ograniczenie ich przetwarzania (ale obowiązki administratora w zakresie usunięcia danych lub ograniczenia ich przetwarzania mają zastosowanie bez względu na to, czy taki wniosek został złożony, czy nie).

([110]) Art. 46 ust. 4 oraz art. 47 ust. 2 DPA 2018.

([111]) Art. 47 ust. 3 DPA 2018.

([112]) Art. 48 ust. 1 DPA 2018.

([113]) Art. 48 ust. 7 DPA 2018.

([114]) Art. 48 ust. 9 DPA 2018.

([115]) Art. 68 DPA 2018.

([116]) Art. 52 ust. 1 DPA 2018.

([117]) Art. 52 ust. 3 DPA 2018.

([118]) W art. 54 DPA 2018 zdefiniowano znaczenie „właściwego okresu", który oznacza okres 1 miesiąca lub okres dłuższy, jaki może wynikać z przepisów, rozpoczynający się odpowiednio w chwili, gdy administrator otrzymuje dany wniosek; gdy administrator otrzymuje informacje (w stosownych przypadkach), o których udzielenie zwrócił się w związku z wnioskiem w sytuacji, o której mowa w art. 52 ust. 4 DPA; lub gdy zostanie uiszczona opłata (w stosownych przypadkach) pobierana w związku z wnioskiem, o którym mowa w art. 53 DPA.

([119]) Art. 53 ust. 1 DPA 2018.

([120]) Zgodnie z wytycznymi Komisarza ds. Informacji administrator może zdecydować o obciążeniu osoby, której dane dotyczą, opłatą, jeżeli wniosek tej osoby jest wyraźnie nieuzasadniony lub wygórowany, ale mimo to administrator postanawia na niego odpowiedzieć. Opłata musi być zasadna i wynikać z poniesionych kosztów. Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „Wyraźnie nieuzasadnione i wygórowane wnioski", dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1. Ograniczenia praw osoby, której dane dotyczą, i obowiązki w zakresie przejrzystości

(66) Właściwy organ może, w określonych okolicznościach, ograniczyć niektóre prawa osoby, której dane dotyczą: prawo dostępu ([121]), prawo do bycia informowanym ([122]), prawo do wiedzy o naruszeniu ochrony danych osobowych ([123]) oraz prawo do informacji o powodzie odrzucenia wniosku o sprostowanie lub usunięcie ([124]). Podobnie jak określono w przepisach rozdziału III dyrektywy (UE) 2016/680, właściwy organ może zastosować ograniczenie wyłącznie wtedy, gdy jest ono – uwzględniając prawa podstawowe i prawnie uzasadnione interesy osoby, której dane dotyczą – niezbędne i proporcjonalne, aby: a) uniemożliwić utrudnianie czynności postępowania urzędowego lub sądowego, postępowania przygotowawczego lub procedury; b) uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar; c) chronić bezpieczeństwo publiczne; d) chronić bezpieczeństwo narodowe; e) chronić prawa i wolności innych osób.

(67) Komisarz ds. Informacji wydał wytyczne dotyczące stosowania tych ograniczeń. Zgodnie z tymi wytycznymi administratorzy są obowiązani przeprowadzać analizę poszczególnych przypadków, aby równoważyć prawa osoby fizycznej ze szkodą, jaką mogłoby spowodować ujawnienie danych. W szczególności powinni oni uzasadniać wszelkie ograniczenia, jakie zastosowali jako niezbędne i proporcjonalne, przy czym mogą ograniczyć zakres praw osoby fizycznej wyłącznie wtedy, gdyby ich wykonanie naruszało powyższe cele ([125]).

(68) Istnieje również szereg innych wytycznych wydanych przez właściwe organy, które zawierają szczegółowe informacje na temat wszystkich aspektów ustawodawstwa w dziedzinie ochrony danych, w tym na temat stosowania ograniczeń praw osób, których dane dotyczą ([126]). Na przykład, w odniesieniu do art. 45 ust. 4, w podręczniku dotyczącym ochrony danych opracowanym przez Krajową Radę Komendantów Policji stwierdzono: „[n]ależy zauważyć, że ograniczenia można stosować wyłącznie w takim zakresie, w jakim jest to konieczne, i można je stosować wyłącznie tak długo, jak jest to niezbędne. W związku z tym nie jest dozwolone powszechne stosowanie ograniczenia do wszystkich danych osobowych wnioskodawcy ani stosowanie ograniczenia w sposób stały. W tej ostatniej kwestii często zdarza się, że dane osobowe zgromadzone bez wiedzy osoby, której dane dotyczą, będącej osobą podejrzaną w postępowaniu przygotowawczym, należy początkowo chronić przed ujawnieniem jej, aby nie zaszkodzić postępowaniu przygotowawczemu w trakcie jego trwania, ale ujawnienie ich w późniejszym czasie nie będzie wiązało się ze szkodą, gdyby te dane osobowe zostały ujawnione danej osobie podczas przesłuchania. Siły policyjne muszą przyjąć procedury zapewniające stosowanie wspomnianych ograniczeń wyłącznie w wymaganym zakresie i tylko przez niezbędny okres" ([127]). Przedmiotowe wytyczne zawierają również przykłady sytuacji, w których prawdopodobnie każde z ograniczeń znajdzie zastosowanie ([128]).

(69) Ponadto jeżeli chodzi o możliwość ograniczenia któregokolwiek z wymienionych powyżej praw ze względu na ochronę „bezpieczeństwa narodowego", administrator może wnieść o podpisanie przez ministra lub Prokuratora Generalnego (lub głównego prawnika ds. Szkocji) poświadczenia potwierdzającego, że ograniczenie takich praw jest niezbędnym i proporcjonalnym środkiem służącym ochronie bezpieczeństwa narodowego ([129]). Rząd Zjednoczonego Królestwa opublikował wytyczne dotyczące poświadczeń bezpieczeństwa narodowego wydawanych na podstawie DPA 2018, w których podkreślono w szczególności, że wszelkie ograniczenia praw osób, których dane dotyczą, służące ochronie bezpieczeństwa narodowego muszą być proporcjonalne i niezbędne ([130]) (aby uzyskać więcej szczegółowych informacji na temat poświadczeń bezpieczeństwa narodowego, zob. motywy 131–134).

([121]) Art. 45 ust. 4 DPA 2018.

([122]) Art. 44 ust. 4 DPA 2018.

([123]) Art. 68 ust. 7 DPA 2018.

([124]) Art. 48 ust. 3 DPA 2018.

([125]) Zob. np. Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw – część dotycząca praw dostępu, dostępna pod adresem:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8

([126]) Zob. np. podręcznik dotyczący ochrony danych opracowany przez Krajową Radę Komendantów Policji (zob. przypis 27) lub wytyczne przedstawione przez Urząd ds. Poważnych Nadużyć Finansowych, dostępne pod adresem: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/

([127]) Podręcznik dotyczący ochrony danych opracowany przez Krajową Radę Komendantów Policji, s. 140 (zob. przypis 27).

([128]) Podręcznik dotyczący ochrony danych opracowany przez Krajową Radę Komendantów Policji stanowi, że „uniemożliwienie utrudniania czynności postępowania urzędowego lub sądowego, postępowania przygotowawczego lub procedury" może mieć znaczenie dla danych osobowych przetwarzanych na potrzeby śledztw, postępowań przed sądem rodzinnym, wewnętrznych postępowań dyscyplinarnych innych niż karne oraz badań takich jak Niezależne badanie dotyczące niegodziwego traktowania dzieci w celach seksualnych; natomiast „ochrona praw i wolności innych osób" ma znaczenie dla danych osobowych, które odnoszą się zarówno do innych osób fizycznych, jak i do wnioskodawcy (Podręcznik dotyczący ochrony danych opracowany przez Krajową Radę Komendantów Policji, s. 140, zob. przypis 27).

([129]) Art. 79 DPA 2018.

([130]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, 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.

(70) Ponadto, w przypadku gdy ograniczenie prawa osoby, której dane dotyczą, ma zastosowanie, właściwy organ musi bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o ograniczeniu jej praw, o przyczynach tego ograniczenia oraz o dostępnych środkach zaskarżenia, chyba że udzielenie tych informacji uniemożliwiałoby osiągnięcie celu, dla którego zastosowano ograniczenie ([131]). W ramach dodatkowego zabezpieczenia przed niewłaściwym wykorzystywaniem ograniczeń administrator musi odnotowywać powody ograniczenia informacji i udostępniać ich rejestr na żądanie Komisarza ds. Informacji ([132]).

(71) Jeżeli administrator odmówi przekazania dodatkowych informacji zapewniających przejrzystość, udzielenia dostępu lub odrzuci wniosek o sprostowanie, usunięcie lub ograniczenie przetwarzania, osoba fizyczna może zwrócić się do Komisarza ds. Informacji o zbadanie, czy administrator zastosował ograniczenie zgodnie z prawem ([133]). Zainteresowana osoba może również złożyć skargę do Komisarza ds. Informacji lub wystąpić do sądu o wydanie nakazu zastosowania się przez administratora do wniosku ([134]).

2.4.7.2. Zautomatyzowane podejmowanie decyzji

(72) Zakres art. 49 i 50 DPA 2018 obejmuje odpowiednio prawa związane ze zautomatyzowanym podejmowaniem decyzji i zabezpieczenia, które należy stosować ([135]). Podobnie jak określono w art. 11 dyrektywy (UE) 2016/680, administrator może podjąć istotną decyzję opartą wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych wyłącznie wówczas, gdy jest to wymagane lub dozwolone przez prawo ([136]). Decyzja jest istotna, jeżeli miałaby niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważny wpływ na tę osobę ([137]).

(73) Jeżeli administrator jest prawnie zobowiązany lub upoważniony do podjęcia istotnej decyzji, w art. 50 DPA 2018 ustanowiono zabezpieczenia, które będą miały zastosowanie do takiej decyzji (którą określono mianem „kwalifikującej się istotnej decyzji"). Administrator musi, w możliwie najkrótszym czasie, powiadomić osobę, której dane dotyczą, o podjęciu takiej decyzji. Osoba, której dane dotyczą, może wówczas w terminie miesiąca zwrócić się do administratora o ponowne rozpatrzenie decyzji lub podjęcie nowej decyzji, która nie będzie oparta wyłącznie na zautomatyzowanym przetwarzaniu. Administrator musi rozpatrzyć wniosek i poinformować osobę, której dane dotyczą, o wyniku tego rozpatrzenia. DPA 2018 uprawnia Sekretarza Stanu do przyjęcia rozporządzeń dotyczących dodatkowych zabezpieczeń ([138]). Dotychczas nie przyjęto takich rozporządzeń.

2.4.8. *Dalsze przekazywanie danych*

(74) Stopień ochrony zapewnianej danym osobowym przekazywanym z organu ścigania państwa członkowskiego do organu ścigania Zjednoczonego Królestwa nie może zostać obniżony wskutek dalszego przekazywania takich danych odbiorcom z państw trzecich. Takie „dalsze przekazywanie danych", które z perspektywy organu ścigania 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.

([131]) Art. 44 ust. 5 i 6; art. 45 ust. 5 i 6; art. 48 ust. 4 DPA 2018.
([132]) Art. 44 ust. 7; art. 45 ust. 7; art. 48 ust. 6 DPA 2018.
([133]) Art. 51 DPA 2018.
([134]) Art. 167 DPA 2018.
([135]) Jeżeli chodzi o zakres zautomatyzowanego przetwarzania, w notach wyjaśniających do DPA 2018 określono, że: „przepisy te odnoszą się do w pełni zautomatyzowanego podejmowania decyzji, a nie do zautomatyzowanego przetwarzania. Zautomatyzowane przetwarzanie (w tym profilowanie) ma miejsce wówczas, gdy operacja jest przeprowadzana na danych bez konieczności interwencji ludzkiej. Jest ono często stosowane na potrzeby ścigania przestępstw do filtrowania i ograniczenia dużych zbiorów danych do ilości możliwych do późniejszego wykorzystania przez człowieka. Zautomatyzowane podejmowanie decyzji jest formą zautomatyzowanego przetwarzania i wymaga podjęcia ostatecznej decyzji bez ingerencji człowieka" (noty wyjaśniające do DPA, pkt 204, zob. przypis 45).
([136]) Oprócz zabezpieczeń przewidzianych w DPA w ramach prawnych Zjednoczonego Królestwa istnieją inne ograniczenia prawne, które mają zastosowanie do organów ścigania i zapobiegają automatycznemu przetwarzaniu (w tym profilowaniu), które prowadzi do niezgodnej z prawem dyskryminacji. Ustawą o prawach człowieka z 1998 r. wprowadzono do prawa Zjednoczonego Królestwa prawa wynikające z EKPC, w tym prawo, o którym mowa w art. 14 konwencji, tj. zakaz dyskryminacji. Podobnie ustawa o równouprawnieniu z 2010 r. zakazuje dyskryminacji osób o cechach podlegających ochronie (które obejmują płeć, rasę, niepełnosprawność itp.).
([137]) Art. 49 ust. 2 DPA 2018.
([138]) Art. 50 ust. 4 DPA 2018.

(75) System międzynarodowego przekazywania danych Zjednoczonego Królestwa został uregulowany w części 3 rozdział 5 DPA 2018 ([139]) i odzwierciedla podejście przyjęte w rozdziale V dyrektywy (UE) 2016/680. W szczególności, aby przekazać dane osobowe do państwa trzeciego, właściwy organ musi spełnić trzy warunki: a) przekazanie musi być niezbędne do celów ścigania przestępstw; b) przekazanie musi opierać się na: (i) rozporządzeniu stwierdzającym odpowiedni stopień ochrony w odniesieniu do państwa trzeciego, (ii) jeżeli nie opiera się na rozporządzeniu stwierdzającym odpowiedni stopień ochrony, na istnieniu odpowiednich zabezpieczeń, lub (iii) jeżeli nie opiera się na decyzji stwierdzającej odpowiedni stopień ochrony ani odpowiednich zabezpieczeniach, musi opierać się na szczególnych okolicznościach; oraz c) odbiorcą przekazania musi być: (i) odpowiedni organ (tj. organ równoważny właściwemu organowi) państwa trzeciego; (ii) „odpowiednia organizacja międzynarodowa", np. organ międzynarodowy pełniący funkcje odpowiadające dowolnemu celowi ścigania przestępstw; lub (iii) osoba inna niż odpowiedni organ, ale wyłącznie wówczas, gdy przekazanie jest absolutnie niezbędne do realizacji jednego z celów ścigania przestępstw; nie istnieją takie podstawowe prawa i wolności osoby, której dane dotyczą, które byłyby nadrzędne wobec interesu publicznego przemawiającego za przekazaniem; przekazanie danych osobowych odpowiedniemu organowi w państwie trzecim byłoby nieskuteczne lub niewłaściwe; odbiorca zostaje poinformowany o celach, w których dane mogą być przetwarzane ([140]).

(76) Rozporządzenia stwierdzające odpowiedni stopień ochrony w odniesieniu do państwa trzeciego, terytorium lub sektora w państwie trzecim, organizacji międzynarodowej lub opisu ([141]) takiego państwa, terytorium, sektora lub takiej organizacji przyjmuje Sekretarz Stanu. Jeżeli chodzi o standard, który ma być zachowany, Sekretarz Stanu musi ocenić, czy takie terytorium/taki sektor/taka organizacja zapewnia odpowiedni stopień ochrony danych osobowych. W art. 74 A ust. 4 DPA 2018 określono, że w tym celu Sekretarz Stanu musi uwzględnić szereg elementów odzwierciedlających elementy wymienione w art. 36 dyrektywy (UE) 2016/680 ([142]). W tym względzie, od czasu zakończenia okresu przejściowego, część 3 DPA 2018 stanowi „ustawodawstwo krajowe wywodzące się z prawa Unii", które, jak wyjaśniono, będzie podlegało wykładni przez sądy Zjednoczonego Królestwa zgodnie ze stosownym orzecznictwem Trybunału Sprawiedliwości sprzed wystąpienia Zjednoczonego Królestwa z Unii i ogólnymi zasadami prawa Unii obowiązującymi bezpośrednio przed zakończeniem okresu przejściowego. Obejmuje to standard „zasadniczej odpowiedniości", który w związku z tym będzie miał zastosowanie do ocen odpowiedniego stopnia ochrony przeprowadzanych przez władze Zjednoczonego Królestwa.

(77) Co się tyczy procedury, rozporządzenia podlegają „ogólnym" wymogom proceduralnym określonym w art. 182 DPA 2018. W ramach wspomnianej procedury Sekretarz Stanu musi przeprowadzić konsultacje z Komisarzem ds.

([139]) Te nowe ramy, w tym uprawnienie Sekretarza Stanu do wydawania rozporządzeń stwierdzających odpowiedni stopień ochrony, zaczęły obowiązywać z końcem okresu przejściowego. Rozporządzenie w sprawie ochrony danych, prywatności i łączności elektronicznej (w szczególności załącznik 21 pkt 10–12, które na mocy tego rozporządzenia wprowadzono do DPA 2018) stanowi jednak, że w okresie przejściowym i po jego zakończeniu określone rodzaje przekazywania danych osobowych są traktowane tak, jakby opierały się na rozporządzeniach stwierdzających odpowiedni stopień ochrony. Te rodzaje przekazywania danych obejmują przekazywanie do państw trzecich objętych unijną decyzją stwierdzającą odpowiedni stopień ochrony na koniec okresu przejściowego oraz do państw członkowskich UE, państw EFTA i terytorium Gibraltaru z racji stosowania przez nie dyrektywy o ochronie danych w sprawach karnych do przetwarzania danych na potrzeby ścigania przestępstw (państwa EFTA stosują dyrektywę (UE) 2016/680 ze względu na swoje zobowiązania wynikające z dorobku Schengen). Oznacza to, że po zakończeniu okresu przejściowego przekazywanie danych do tych państw może nadal odbywać się na takich samych zasadach jak przed wystąpieniem z UE. Po zakończeniu okresu przejściowego Sekretarz Stanu ma obowiązek przeprowadzić przegląd ustaleń dotyczących odpowiedniego stopnia ochrony w ciągu 4 lat.

([140]) Art. 73 i 77 DPA 2018.

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

([142]) Zob. art. 74 A ust. 4 DPA 2018, który stanowi, że oceniając, czy stopień ochrony jest odpowiedni, „Sekretarz Stanu musi uwzględnić w szczególności a) praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie prawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, a także wdrażanie takiego prawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie trzecim lub w organizacji międzynarodowej, orzecznictwo, a także skuteczne i wykonalne prawa osób, których dane dotyczą, oraz prawa osób, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia; b) istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego w państwie trzecim lub organu nadzorującego organizację międzynarodową, mającego obowiązek zapewniać i egzekwować przestrzeganie przepisów o ochronie danych – w tym posiadające odpowiednie uprawnienia do egzekwowania przestrzegania przepisów – pomagać i doradzać osobom, których dane dotyczą, w toku wykonywania przysługujących im praw, a także współpracować z Komisarzem; oraz c) międzynarodowe zobowiązania państwa trzeciego lub organizacji międzynarodowej lub inne obowiązki wynikające z prawnie wiążących konwencji lub aktów prawnych oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych".

Informacji, gdy proponuje przyjęcie przyszłych rozporządzeń Zjednoczonego Królestwa stwierdzających odpowiedni stopień ochrony ([143]). Po przyjęciu przez Sekretarza Stanu rozporządzenia te są przedkładane parlamentowi i podlegają procedurze „milczącej zgody (*negative resolution*)", w ramach której obie izby parlamentu mogą poddać rozporządzenie kontroli i mają możliwość przyjęcia wniosku o jego unieważnienie w ciągu 40 dni ([144]).

(78) Zgodnie z art. 74B 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.

(79) Podobnie do tego, co przewidziano w art. 37 dyrektywy (UE) 2016/680, w przypadku braku rozporządzenia stwierdzającego odpowiedni stopień ochrony przekazanie danych osobowych w kontekście sektora organów ścigania przestępstw byłoby możliwe, gdyby istniały odpowiednie zabezpieczenia. Takie zabezpieczenia zapewnia się w drodze a) prawnie wiążącego aktu zawierającego odpowiednie zabezpieczenia służące ochronie danych osobowych; albo b) oceny przeprowadzonej przez administratora, który po ocenieniu wszystkich okoliczności związanych z przekazaniem stwierdził, że istnieją odpowiednie zabezpieczenia ochrony danych ([145]). Ponadto, w przypadku gdy przekazywanie odbywa się na podstawie odpowiednich zabezpieczeń, DPA 2018 przewiduje, że dodatkowo w stosunku do zwykłego nadzoru pełnionego przez Komisarza ds. Informacji właściwe organy muszą także przekazywać Komisarzowi ds. Informacji szczegółowe informacje na temat przekazywania ([146]).

(80) Jeżeli przekazanie nie opiera się na decyzji stwierdzającej odpowiedni stopień ochrony ani na odpowiednich zabezpieczeniach, może ono nastąpić wyłącznie w niektórych, określonych okolicznościach, zwanych „szczególnymi okolicznościami" ([147]). 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 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) ([148]). 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 ([149]). Ten zbiór okoliczności odpowiada szczególnym sytuacjom i warunkom kwalifikującym się jako „wyjątki" na podstawie art. 38 dyrektywy (UE) 2016/680.

(81) W takich okolicznościach należy udokumentować datę i godzinę przekazania, uzasadnienie, nazwę i wszelkie inne stosowne informacje o odbiorcy oraz opis przekazanych danych osobowych, a dokumentację przekazać Komisarzowi ds. Informacji na jego żądanie ([150]).

(82) Art. 78 DPA 2018 reguluje przypadki „kolejnych przekazań", a mianowicie sytuacji, w których dane osobowe, które zostały przekazane ze Zjednoczonego Królestwa do państwa trzeciego, są następnie przekazywane do innego państwa trzeciego lub organizacji międzynarodowej. Zgodnie z art. 78 ust. 1 administrator ze Zjednoczonego Królestwa przekazujący dane musi uzależnić przekazanie danych od tego, że nie będą one dalej przekazywane do państwa trzeciego bez zgody administratora przekazującego dane. Ponadto zgodnie z art. 78 ust. 3 i podobnie do tego, co przewidziano w art. 35 ust. 1 lit. e) dyrektywy (UE) 2016/680, w przypadku gdy taka zgoda jest wymagana, zastosowanie ma szereg istotnych wymogów. W szczególności, podejmując decyzję o udzieleniu lub odmowie udzielenia

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

([144]) W trakcie tego 40-dniowego okresu obie izby parlamentu mogą, jeśli zechcą, zagłosować przeciwko rozporządzeniom; w przypadku przyjęcia takiego wniosku w drodze głosowania, rozporządzenia ostatecznie przestaną wywoływać jakiekolwiek dalsze skutki prawne.

([145]) Art. 75 DPA 2018.

([146]) Zgodnie z art. 75 ust. 3 DPA 2018, jeżeli przekazanie danych odbywa się w oparciu o odpowiednie zabezpieczenia: a) przekazanie musi być udokumentowane; b) dokumentacja musi zostać przekazana Komisarzowi na jego żądanie oraz c) dokumentacja musi zawierać w szczególności (i) datę i godzinę przekazania, (ii) nazwę odbiorcy i wszelkie inne stosowne informacje na jego temat, (iii) uzasadnienie przekazania oraz (iv) opis przekazanych danych osobowych.

([147]) Przewodnik dotyczący przetwarzania danych do celów ścigania przestępstw, „Czy istnieją jakiekolwiek okoliczności szczególne?", dostępny pod adresem: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

([148]) Art. 76 DPA 2018.

([149]) Art. 76 DPA 2018.

([150]) Art. 76 ust. 3 DPA 2018.

zgody na przekazanie danych, właściwy organ musi upewnić się, że dalsze przekazanie jest niezbędne do celów ścigania przestępstw, i uwzględnić m.in. następujące czynniki a) powagę okoliczności, które doprowadziły do złożenia wniosku o udzielenie zgody, b) cel, w którym dane osobowe zostały pierwotnie przekazane oraz c) standardy ochrony danych osobowych obowiązujące w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe miałyby zostać przekazane.

(83) Ponadto w przypadku gdy dane, które są poddawane dalszemu przekazaniu ze Zjednoczonego Królestwa, zostały pierwotnie przekazane z Unii Europejskiej, zastosowanie mają dodatkowe zabezpieczenia.

(84) Po pierwsze, art. 73 ust. 1 lit. b) DPA 2018 – podobnie jak art. 35 ust. 1 lit. c) dyrektywy (UE) 2016/680 – stanowi, że w przypadku gdy dane osobowe zostały pierwotnie przesłane lub w inny sposób udostępnione administratorowi lub innemu właściwemu organowi przez państwo członkowskie, to państwo członkowskie lub dowolna osoba z siedzibą w tym państwie członkowskim, która jest właściwym organem do celów dyrektywy (UE) 2016/680, musiała wyrazić zgodę na przekazanie zgodnie z prawem państwa członkowskiego.

(85) Podobnie jednak jak określono w art. 35 ust. 2 dyrektywy (UE) 2016/680, zgoda taka nie jest wymagana, jeżeli a) odnośne przekazanie jest niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu dla bezpieczeństwa publicznego w państwie członkowskim albo w państwie trzecim bądź dla ważnych interesów państwa członkowskiego i b) zgody nie da się uzyskać w odpowiednim terminie. W takim przypadku należy bezzwłocznie poinformować organ państwa członkowskiego, który byłby odpowiedzialny za podjęcie decyzji, czy wyrazić zgodę na przekazanie danych ([151]).

(86) Po drugie, to samo podejście ma zastosowanie w przypadku danych pierwotnie przekazanych z Unii Europejskiej do Zjednoczonego Królestwa, a następnie przekazanych przez Zjednoczone Królestwo państwu trzeciemu, które następnie przekazałoby je państwu trzeciemu. W takim przypadku zgodnie z art. 78 ust. 4, właściwy organ Zjednoczonego Królestwa nie może udzielić zgody na to ostatnie przekazanie zgodnie z art. 78 ust. 1, chyba że „państwo członkowskie [które pierwotnie przekazało przedmiotowe dane] lub dowolna osoba z siedzibą w tym państwie członkowskim, która jest właściwym organem do celów dyrektywy o ochronie danych w sprawach karnych, wyraziła zgodę na przekazanie danych zgodnie z prawem państwa członkowskiego". Zabezpieczenia te są ważne, ponieważ umożliwiają organom państw członkowskich zapewnienie ciągłości ochrony, zgodnie z unijnymi przepisami o ochronie danych, w całym „łańcuchu przekazywania danych".

(87) Wspomniane nowe ramy dotyczące międzynarodowego przekazywania danych zaczęły obowiązywać po zakończeniu okresu przejściowego ([152]). Załącznik 21 pkt 10–12 (wprowadzone na mocy rozporządzenia w sprawie ochrony danych, prywatności i łączności elektronicznej) stanowią jednak, że od zakończenia okresu przejściowego określone przekazania danych osobowych będą traktowane tak, jakby opierały się na rozporządzeniach stwierdzających odpowiedni stopień ochrony. Przekazania te obejmują przekazania danych do państwa członkowskiego, państwa EFTA i państwa trzeciego objętego decyzją UE stwierdzającą odpowiedni stopień ochrony na koniec okresu przejściowego oraz do terytorium Gibraltaru. W związku z tym przekazywanie danych do tych państw może nadal odbywać się na takich samych zasadach jak przed wystąpieniem Zjednoczonego Królestwa z Unii. Po zakończeniu 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.

2.4.9. *Rozliczalność*

(88) Zgodnie z zasadą rozliczalności organy publiczne 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.

(89) Zasada ta znajduje odzwierciedlenie w art. 56 DPA 2018, którym wprowadzono ogólny obowiązek rozliczalności administratora, tj. obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się zgodnie z wymogami określonymi w części 3 DPA 2018 i aby administrator był w stanie to wykazać. Wdrożone środki muszą być w razie potrzeby poddawane przeglądom i uaktualniane, a jeżeli jest to proporcjonalne w stosunku do przetwarzania – obejmować odpowiednie polityki ochrony danych.

([151]) Art. 73 ust. 5 DPA 2018.

([152]) 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.

(90) Zgodnie z rozdziałem IV dyrektywy (UE) 2016/680 w art. 55–71 DPA 2018 przewidziano różne mechanizmy mające zapewnić rozliczalność i umożliwić administratorom i podmiotom przetwarzającym wykazanie zgodności. W szczególności administratorzy są zobowiązani do wdrożenia środków ochrony danych w fazie projektowania i domyślnej ochrony danych, tj. do zapewnienia skutecznej realizacji zasad ochrony danych oraz prowadzenia wykazu wszystkich kategorii czynności przetwarzania, za które odpowiada administrator (w tym informacji na temat tożsamości administratora, danych kontaktowych inspektora ochrony danych, celów przetwarzania, kategorii odbiorców ujawnianych informacji oraz opisu kategorii osób, których dane dotyczą, oraz danych osobowych), a także do udostępniania tych wykazów Komisarzowi ds. Informacji na jego żądanie. Administrator i podmiot przetwarzający muszą również ewidencjonować określone operacje przetwarzania i udostępniać ewidencję Komisarzowi ds. Informacji ([153]). Administratorzy są również wyraźnie zobowiązani do współpracy z Komisarzem ds. Informacji przy wykonywaniu jego zadań.

(91) W DPA 2018 określono również dodatkowe wymogi dotyczące sytuacji, gdy przetwarzanie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Obejmują one obowiązek przeprowadzenia oceny skutków dla ochrony danych oraz konsultacji z Komisarzem ds. Informacji przed przetwarzaniem, jeżeli taka ocena wskaże, że przetwarzanie powodowałoby wysokie ryzyko dla praw i wolności osób fizycznych (w przypadku braku zastosowania środków w celu zminimalizowania tego ryzyka).

(92) Administratorzy muszą ponadto wyznaczyć inspektora ochrony danych, chyba że administratorem jest sąd lub inny organ sądowy, działający w zakresie sprawowania wymiaru sprawiedliwości ([154]). Administrator musi zapewnić, aby inspektor ochrony danych był włączany we wszystkie sprawy dotyczące ochrony danych osobowych, posiadał niezbędne zasoby i dostęp do danych osobowych i operacji przetwarzania oraz mógł niezależnie wykonywać swoje zadania. Zadania inspektora ochrony danych określono w art. 71 DPA 2018 i obejmują one udzielanie informacji i porad, monitorowanie przestrzegania przepisów, a także współpracę z Komisarzem ds. Informacji i pełnienie funkcji punktu kontaktowego dla Komisarza ds. Informacji. Podczas wykonywania swoich zadań inspektor ochrony danych musi uwzględniać ryzyko związane z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

2.5. **Nadzór i egzekwowanie przepisów**

2.5.1. *Niezależny nadzór*

(93) Aby zagwarantować również 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 musi być całkowicie niezależny i bezstronny.

(94) W Zjednoczonym Królestwie za nadzór i egzekwowanie zgodności z przepisami RODO UK i DPA 2018 odpowiada Komisarz ds. Informacji ([155]). Komisarz ds. Informacji nadzoruje również przetwarzanie danych osobowych przez właściwe organy wchodzące w zakres części 3 DPA 2018 ([156]). 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 ([157]). Departamentem finansującym Komisarza ds. Informacji jest Departament Cyfryzacji, Kultury, Mediów i Sportu ([158]).

([153]) Art. 62 DPA 2018.
([154]) Art. 69 DPA 2018.
([155]) Art. 36 ust. 2 lit. b) dyrektywy (UE) 2016/680.
([156]) Art. 116 DPA 2018.
([157]) 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
([158]) 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 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

(95) Kwestię niezależności Komisarza wyraźnie uregulowano w art. 52 RODO UK, który odpowiada wymogom określonym w art. 52 ust. 1–3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([159]). 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 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.

(96) Warunki powoływania i odwoływania Komisarza ds. Informacji określono w załączniku 12 do DPA 2018. Komisarz ds. Informacji jest powoływany przez Królową 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 ([160]) 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 ([161]).

(97) Kadencja Komisarza ds. Informacji trwa maksymalnie siedem lat. Jej Królewska Mość może odwołać Komisarza ds. Informacji ze stanowiska na podstawie oświadczenia obu izb parlamentu ([162]). Wniosek o odwołanie Komisarza ds. Informacji może zostać przedstawiony jednej z izb parlamentu jedynie w wypadku, gdy minister przedstawi tej izbie sprawozdanie, w którym wyrazi przekonanie, że Komisarz ds. Informacji jest winny poważnego uchybienia lub nie spełnia już warunków wymaganych do sprawowania funkcji Komisarza ([163]).

(98) 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 ([164]) i wynoszą 85–90 % rocznego budżetu Biura ([165]); (ii) subwencji, które mogą być wypłacane przez rząd na rzecz Komisarza ds. Informacji i są wykorzystywane głównie do finansowania kosztów operacyjnych Komisarza ds. Informacji w odniesieniu do zadań niezwiązanych z ochroną danych ([166]); (iii) opłat pobieranych z tytułu świadczenia usług ([167]). Obecnie nie pobiera się takich opłat.

(99) Ogólne funkcje Komisarza ds. Informacji w odniesieniu do przetwarzania danych osobowych wchodzącego w zakres części 3 DPA 2018 zostały określone w załączniku 13 do tej ustawy. Jego zadania obejmują: monitorowanie i egzekwowanie części 3 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 postępowań. Aby utrzymać niezależność sądów, Komisarz ds.

([159]) 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) (Dz.U. L 119 z 4.5.2016, s. 1).

([160]) Kodeks zarządzania w zakresie nominacji publicznych, dostępny pod adresem: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) 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.

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

([163]) Pkt 3 załącznika 12 do DPA 2018.

([164]) Art. 137 DPA 2018.

([165]) Art. 137 i 138 DPA 2018 zawiera szereg zabezpieczeń służących zapewnieniu ustalenia opłat na odpowiednim poziomie. W szczególności w art. 137 ust. 4 DPA 2018 wymieniono kwestie, jakie Sekretarz Stanu musi uwzględnić przy tworzeniu przepisów określających kwotę, którą muszą zapłacić różne organizacje. 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.

([166]) 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 158).

([167]) Art. 134 DPA 2018.

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 jednak omówione poniżej wyspecjalizowane organy.

2.5.1.1. Egzekwowanie przepisów, w tym sankcje

(100) Komisarz posiada ogólne uprawnienia dochodzeniowo-śledcze, uprawnienia w zakresie korekt i upoważnień oraz uprawnienia doradcze w odniesieniu do przetwarzania danych osobowych, do których zastosowanie ma część 3 DPA 2018. Komisarz posiada uprawnienia do zawiadomienia administratora lub podmiotu przetwarzającego o domniemanym naruszeniu przepisów części 3, do udzielania ostrzeżeń administratorowi lub podmiotowi przetwarzającemu, że planowane operacje przetwarzania prawdopodobnie naruszą przepisy części 3, a także do udzielania upomnień administratorowi lub podmiotowi przetwarzającemu, jeżeli operacje przetwarzania naruszyły przepisy części 3. Ponadto Komisarz może wydawać z urzędu lub na wniosek opinie dla parlamentu, rządu lub innych instytucji i organów Zjednoczonego Królestwa, a także opinii publicznej w sprawie dowolnej kwestii związanej z ochroną danych osobowych ([168]).

(101) Ponadto Komisarz posiada uprawnienia w zakresie:

— nakazania administratorowi i podmiotowi przetwarzającemu (a w określonych okolicznościach każdej innej osobie) udzielenia niezbędnych informacji poprzez wydanie zawiadomienia informacyjnego („zawiadomienie informacyjne") ([169]);

— 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 („zawiadomienie oceniające") ([170]);

— uzyskania w inny sposób dostępu do dokumentów administratorów i podmiotów przetwarzających oraz dostępu do ich pomieszczeń zgodnie z art. 154 DPA 2018 („uprawnienia do wstępu i inspekcji");

— 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 podejmowania określonych kroków („zawiadomienie egzekucyjne") ([171]); oraz

— nakładania administracyjnych kar pieniężnych w drodze zawiadomienia w sprawie sankcji („zawiadomienie w sprawie sankcji") ([172]).

(102) W polityce działań regulacyjnych Komisarza ds. Informacji określono okoliczności, w których wydaje on, odpowiednio, zawiadomienie informacyjne, oceniające, egzekucyjne i zawiadomienie w sprawie sankcji ([173]). W ramach zawiadomienia egzekucyjnego możliwe jest nałożenie tych wymogów, które Komisarz uzna za właściwe w celu zaradzenia uchybieniu. W ramach zawiadomienia w sprawie sankcji zobowiązuje się daną osobę do wpłacenia na rzecz Komisarza ds. Informacji kwoty określonej w zawiadomieniu. Zawiadomienie w sprawie sankcji można wydać w następstwie uchybienia określonym przepisom DPA 2018 ([174]) lub można je wydać w odniesieniu do administratora lub podmiotu przetwarzającego, który nie zastosował się do zawiadomienia informacyjnego, oceniającego lub egzekucyjnego.

(103) W szczególności podczas podejmowania decyzji, czy należy wydać zawiadomienie w sprawie sankcji w odniesieniu do danego administratora lub podmiotu przetwarzającego, oraz podczas ustalania wysokości sankcji Komisarz ds. Informacji musi uwzględnić kwestie wymienione w art. 155 ust. 3 DPA 2018, w tym charakter i wagę uchybienia, umyślny lub nieumyślny charakter uchybienia, wszelkie działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przed osoby, których dane dotyczą, stopień odpowiedzial-

([168]) Pkt 2 załącznika 13 do DPA 2018.
([169]) Art. 142 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 143 DPA 2018).
([170]) Art. 146 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 147 DPA 2018).
([171]) Art. 149–151 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 152 DPA 2018).
([172]) Art. 155 DPA 2018 (z zastrzeżeniem ograniczeń określonych w art. 156 DPA 2018).
([173]) Polityka działań regulacyjnych, dostępna pod adresem: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) W szczególności Komisarz ds. Informacji może wydać zawiadomienie w sprawie sankcji w następstwie uchybienia przepisom, o którym mowa w art. 149 ust. 2, 3, 4 lub 5 DPA 2018.

ności administratora lub podmiotu przetwarzającego (z uwzględnieniem wdrożonych przez nich środków technicznych i organizacyjnych), wszelkie istotne wcześniejsze uchybienia ze strony administratora lub podmiotu przetwarzającego; kategorie danych osobowych, których dotyczyło uchybienie, oraz to, czy sankcja byłaby skuteczna, proporcjonalna i odstraszająca.

(104) Maksymalna kwota sankcji, jaką można nałożyć w drodze zawiadomienia w sprawie sankcji, wynosi a) 17 500 000 GBP w odniesieniu do niezastosowania się do zasad ochrony danych (art. 35, 36, 37, 38 ust. 1, 39 ust. 1 i 40 DPA 2018), obowiązków w zakresie przejrzystości i praw indywidualnych (art. 44, 45, 46, 47, 48, 49, 52 i 53 DPA 2018) oraz zasad dotyczących międzynarodowego przekazywania danych osobowych (art. 73, 75, 76, 77 i 78 DPA 2018); oraz b) 8 700 000 GBP w innych przypadkach ([175]). W odniesieniu do niezastosowania się do zawiadomienia informacyjnego, oceniającego lub egzekucyjnego maksymalna kwota sankcji, jaką można nałożyć w ramach zawiadomienia w sprawie sankcji, wynosi 17 500 000 GBP.

(105) Zgodnie z ostatnimi sprawozdaniami rocznymi (2018–2019 ([176]), 2019–2020 ([177])) Komisarz ds. Informacji przeprowadził szereg postępowań w odniesieniu do przetwarzania danych osobowych 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" ([178]) i stwierdził szereg poważnych naruszeń przepisów o ochronie danych, które mogły podważyć zaufanie publiczne w kwestii stosowania matrycy i sposobu wykorzystywania danych.

(106) 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.

(107) Innym przykładem niedawnych działań egzekucyjnych jest grzywna w wysokości 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.

(108) Ponadto należy zauważyć, że poza powyższymi możliwościami egzekwowania przestrzegania przepisów przez Komisarza ds. Informacji niektóre naruszenia ustawodawstwa w dziedzinie ochrony danych stanowią przestępstwo, wobec czego mogą podlegać sankcjom karnym (art. 196 DPA 2018). Dotyczy to na przykład uzyskania lub ujawnienia danych osobowych bez zgody administratora oraz doprowadzenia do ujawnienia danych osobowych innej osobie bez zgody administratora ([179]); deanonimizacji informacji będących zanonimizowanymi danymi osobowymi bez zgody administratora odpowiedzialnego za anonimizację danych osobowych ([180]); umyślnego utrudniania Komisarzowi wykonywania jego uprawnień w zakresie kontroli danych osobowych zgodnie z zobowiązaniami międzynarodowymi ([181]), składania fałszywych oświadczeń w odpowiedzi na zawiadomienie informacyjne lub niszczenia informacji w związku z zawiadomieniem informacyjnym i oceniającym ([182]).

(109) Komisarz ds. Informacji jest również zobowiązany na podstawie art. 139 DPA 2018 do składania przed każdą z izb parlamentu ogólnego sprawozdania z wykonywania swoich funkcji wynikających z ustawy ([183]).

([175]) Art. 157 DPA 2018.

([176]) 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.

([177]) Sprawozdanie roczne Komisarza ds. Informacji za okres 2019–2020 (zob. przypis 157).

([178]) Baza danych, w której zapisywano dane wywiadowcze dotyczące domniemanych członków gangów i poszkodowanych w przestępstwach związanych z gangami.

([179]) Art. 170 DPA 2018.

([180]) Art. 171 DPA 2018.

([181]) Art. 119 DPA 2018.

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

([183]) Jak określono w umowie o zarządzanie, sprawozdanie roczne musi: (i) uwzględniać wszystkie przedsiębiorstwa, spółki zależne lub spółki joint venture objęte kontrolą Komisarza ds. Informacji; (ii) być zgodne z Podręcznikiem dotyczącym sprawozdawczości finansowej opublikowanym przez Ministerstwo Skarbu (Financial Reporting Manual – FReM); (iii) zawierać oświadczenie dotyczące zarządzania, określające metody stosowane przez księgowego do zarządzania zasobami wykorzystywanymi w organizacji i ich kontroli w ciągu roku i ilustrujące sprawność organizacji w zarządzaniu ryzykiem związanym z realizacją jej celów i zadań oraz (iv) nakreślać główne działania i wyniki w poprzednim roku budżetowym oraz przedstawiać w skróconej formie plany na przyszłość (umowa o zarządzanie na lata 2018–2021, pkt 3.26, zob. przypis 158).

2.5.2. *Nadzór nad wymiarem sprawiedliwości*

(110) Nadzór nad przetwarzaniem danych osobowych przez sądy i wymiar sprawiedliwości ma dwojaki charakter. W przypadku gdy osoba zajmująca 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 ([184]), a nadzór sprawują organy specjalne. Odzwierciedla to podejście przyjęte w art. 32 dyrektywy (UE) 2016/680.

(111) W szczególności w tej drugiej sytuacji w przypadku sądów Anglii i Walii oraz trybunału pierwszej instancji i wyższych trybunałów Anglii i Walii taki nadzór sprawuje panel sądowy ds. ochrony danych [Judicial Data Protection Panel] ([185]). Ponadto Lord Chief Justice (zwierzchnik sądownictwa Anglii i Walii) i Senior President of Tribunals (zwierzchnik trybunałów pozasądowych) wydali oświadczenie o ochronie prywatności ([186]), w którym określili sposób, w jaki sądy w Anglii i Walii przetwarzają dane osobowe w związku z pełnieniem funkcji sądowych. Podobne oświadczenia wydano w systemach sądownictwa Irlandii Północnej ([187]) i Szkocji ([188]).

(112) Ponadto w Irlandii Północnej Lord Chief Justice (zwierzchnik sądownictwa) Irlandii Północnej mianował sędziego Wysokiego Trybunału na stanowisko sędziego sprawującego nadzór nad ochroną danych osobowych ([189]). 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 ([190]).

(113) W Szkocji Lord President 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 ([191]).

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

([184]) Art. 117 DPA 2018.

([185]) 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 każdej skargi. Jeżeli skarżący nie jest zadowolony z decyzji podjętej przez panel i dostarcza dodatkowy materiał dowodowy, panel może ponownie rozpatrzyć swoją decyzję. Chociaż sam panel nie nakłada sankcji finansowych, to 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 starszy rangą 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 załatwienia sprawy.

([186]) 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

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

([188]) 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.

([189]) 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.

([190]) 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.

([191]) 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 trybunału i są dostępne pod adresem: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Środki zaskarżenia*

(115) 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.

(116) Po pierwsze, 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 ([192]). Jak opisano w motywach 100 i 109 powyżej, Komisarz ds. Informacji jest uprawniony do oceny przestrzegania DPA 2018 przez administratora i podmiot przetwarzający, wezwania ich do podjęcia lub zaniechania koniecznych kroków w przypadku nieprzestrzegania przepisów oraz do nałożenia kar.

(117) Po drugie, DPA 2018 zapewnia prawo do środka ochrony prawnej przeciwko Komisarzowi ds. Informacji. Jeżeli Komisarz nie „czyni postępów" ([193]) w rozpatrywaniu skargi złożonej przez osobę, której dane dotyczą, skarżący ma dostęp do środka ochrony prawnej przed sądem, ponieważ może zwrócić się do trybunału pierwszej instancji ([194]) o nakazanie Komisarzowi podjęcia odpowiednich kroków w celu udzielenia odpowiedzi na skargę lub poinformowania skarżącego o postępach w rozpatrywaniu skargi ([195]). Ponadto każda osoba, wobec której Komisarz wydał którekolwiek z powyższych 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 ([196]).

(118) Po trzecie, osoby fizyczne mogą wnieść środki zaskarżenia przeciwko administratorom i podmiotom przetwarzającym bezpośrednio do sądu na podstawie 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. Ponadto, zgodnie z art. 169 DPA 2018, każdy, kto poniósł szkodę z powodu naruszenia wymogu określonego w ustawodawstwie w dziedzinie ochrony danych (w tym w części 3 DPA 2018), innym niż RODO UK, ma prawo do odszkodowania z tytułu poniesienia tej szkody od administratora lub podmiotu przetwarzającego, chyba że administrator lub podmiot przetwarzający udowodni, że nie ponosi w żaden sposób odpowiedzialności za zdarzenie wywołujące szkodę. Szkoda obejmuje zarówno stratę finansową, jak i szkodę niezwiązaną ze stratą finansową, taką jak cierpienie.

(119) Po czwarte, jeżeli ktokolwiek uważa, że jego 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. Administratorzy w rozumieniu części 3 DPA 2018, tj. właściwe organy, są zawsze organami publicznymi w rozumieniu ustawy o prawach człowieka z 1998 r. 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 ([197]).

([192]) Art. 165 DPA 2018.

([193]) Art. 166 DPA 2018 odnosi się w szczególności do następujących sytuacji: a) Komisarz nie podejmuje odpowiednich kroków w celu udzielenia odpowiedzi na skargę; b) Komisarz nie przekazuje 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 informuje o tym skarżącego w okresie kolejnych trzech miesięcy.

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

([195]) Art. 166 DPA 2018.

([196]) Art. 161 i 162 DPA 2018.

([197]) Zob. sprawa Brown przeciwko Commissioner of the Met 2016, w której sąd zasądził rekompensatę powódce w kontekście ochrony danych w powództwie przeciwko policji. Sąd orzekł na korzyść powódki, przychylając się do jej pozwu dotyczącego naruszenia obowiązków wynikających z DPA 1998, naruszenia ustawy o prawach człowieka z 1998 r. (i powiązanego prawa określonego w art. 8 EKPC) oraz popełnienia czynu niedozwolonego polegającego na niewłaściwym wykorzystaniu informacji prywatnych (pozwany ostatecznie przyznał, że naruszył DPA i EKPC, więc sąd skupił się w wyroku na określeniu odpowiedniego środka zaradczego). W związku z tymi naruszeniami sąd zasądził na rzecz powódki odszkodowanie pieniężne.

(120) Jeśli sąd stwierdzi, że jakiekolwiek działanie organu publicznego jest niezgodne z prawem, może – w ramach swojej właściwości – zastosować taki środek zabezpieczający lub inny środek prawny lub wydać taki nakaz, jaki uzna za sprawiedliwy i właściwy ([198]). Sąd może również orzec, że przepis ustawodawczy jest niezgodny z prawem gwarantowanym na mocy EKPC.

(121) Ponadto po wyczerpaniu krajowych środków ochrony prawnej osobie fizycznej przysługuje środek zaskarżenia przed Europejskim Trybunałem Praw Człowieka z tytułu naruszenia praw gwarantowanych na mocy EKPC.

2.6. **Dalsze przekazywanie**

(122) Prawo Zjednoczonego Królestwa dopuszcza udostępnianie danych przez organ ścigania innym organom Zjednoczonego Królestwa do celów innych niż te, dla których pierwotnie je zebrano (tzw. „dalsze przekazywanie"), pod pewnymi warunkami.

(123) 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), o ile dalsze przetwarzanie odbywa się 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 ([199]). W takim przypadku wszystkie zabezpieczenia przewidziane w części 3 DPA 2018 i przeanalizowane powyżej mają zastosowanie do przetwarzania prowadzonego przez organ otrzymujący.

(124) W porządku prawnym Zjednoczonego Królestwa różne ustawy wyraźnie dopuszczają 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 organu publicznego ([200]), lub w przypadku długu należnego na rzecz organu publicznego lub Korony ([201]); (ii) ustawa o przestępczości i sądach z 2013 r. zezwala na udostępnianie danych Krajowej Agencji ds. Zwalczania Przestępczości ([202]) 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 ([203]).

(125) 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 ([204]), aby pomóc policji w wypełnianiu obowiązków w zakresie ochrony danych wynikających z RODO UK, DPA oraz ustawy o prawach człowieka z 1998 r. Zgodność udostępniania informacji z obowiązującymi ramami prawnymi w zakresie ochrony danych może oczywiście podlegać kontroli sądowej ([205]).

(126) 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 ([206]). Ten rodzaj udostępniania danych obejmuje dwa scenariusze: 1) gdy organ ścigania przekazuje dane organowi niebędącemu

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

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

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

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

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

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

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

([205]) Zob. np. sprawa M 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 programem 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), organem ścigania będącym obecnie częścią Krajowej Agencji ds. Zwalczania Przestępczości.

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

organem ścigania ani agencją wywiadowczą (np. organowi ds. regulacji finansowej, organowi podatkowemu, organowi ochrony konkurencji, urzędowi ds. młodzieży itp.); 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. Jak określono w decyzji przyjętej na mocy rozporządzenia (UE) 2016/679, zabezpieczenia przewidziane w RODO UK i części 2 DPA 2018 zapewniają stopień ochrony zasadniczo odpowiadający stopniowi zapewnionemu w Unii ([207]).

(127) 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 ustawa o zwalczaniu terroryzmu z 2008 r. (CTA 2008) ([208]). Zgodnie z ustawą o zwalczaniu terroryzmu z 2008 r. każdy może przekazać informacje którejkolwiek ze służb wywiadowczych na potrzeby wykonywania którejkolwiek z funkcji tej służby, w tym dotyczącej „bezpieczeństwa narodowego".

(128) Jeśli chodzi o warunki, na jakich dane można udostępniać do celów bezpieczeństwa narodowego, ustawa o służbach wywiadowczych oraz ustawa o Służbie Bezpieczeństwa ograniczają możliwości służb wywiadowczych w zakresie uzyskiwania danych do tego, co jest niezbędne do wykonywania ich funkcji ustawowych. Właściwe organy, wchodzące w zakres części 3 DPA 2018, które zamierzają 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 ([209]). W art. 20 ustawy o zwalczaniu terroryzmu z 2008 r. wyraźnie wskazano, że wszelkie udostępnianie danych na podstawie art. 19 tej ustawy musi być również zgodne z ustawodawstwem w dziedzinie ochrony danych; oznacza to, że mają zastosowanie wszystkie ograniczenia i wymogi określone w DPA 2018. Ponadto organy ścigania i służby wywiadowcze są organami publicznymi w rozumieniu ustawy o prawach człowieka z 1998 r., a zatem muszą zagwarantować, że działają zgodnie z prawami gwarantowanymi na mocy EKPC, w tym jej art. 8. Innymi słowy, wymogi te oznaczają, że wszelkie udostępnianie danych między organami ścigania a służbami wywiadowczymi musi być zgodne z ustawodawstwem w dziedzinie ochrony danych i EKPC.

(129) Przetwarzanie przez służby wywiadowcze danych osobowych otrzymanych lub uzyskanych od organów ścigania do celów bezpieczeństwa narodowego podlega szeregowi warunków i zabezpieczeń ([210]). Część 4 DPA 2018 ma zastosowanie do wszelkiego przetwarzania danych przez służby wywiadowcze lub w ich imieniu. Określono

([207]) Decyzja wykonawcza Komisji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo C(2021) 4800.

([208]) Art. 19 ustawy o zwalczaniu terroryzmu z 2008 r., dostępnej pod adresem: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) Art. 2 ust. 2 ustawy o służbach wywiadowczych z 1994 r. (zob. https://www.legislation.gov.uk/ukpga/1994/13/contents) stanowi, że „Dyrektor służby wywiadowczej jest odpowiedzialny za skuteczne działanie tej służby i jego obowiązkiem jest zapewnienie, aby: a) wprowadzono rozwiązania mające na celu zagwarantowanie, że służba wywiadowcza nie uzyskuje żadnych informacji z wyjątkiem tych, które są konieczne do właściwego wykonywania jej funkcji, i że nie zostaną ujawnione żadne informacje poza to, co konieczne – (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. (zob. https://www.legislation.gov.uk/ukpga/1989/5/contents) stanowi, że „Dyrektor generalny jest odpowiedzialny za skuteczne działanie Służby i jego obowiązkiem jest zapewnienie, aby: a) wprowadzono rozwiązania mające na celu zagwarantowanie, że Służba nie uzyskuje żadnych informacji z wyjątkiem tych, które są konieczne do właściwego wykonywania jej funkcji, i że nie zostaną ujawnione żadne informacje poza to, co konieczne do tego celu lub do celów zapobiegania poważnej przestępczości lub jej wykrywania lub do celów jakichkolwiek postępowań karnych; b) Służba nie podejmowała żadnych działań na rzecz interesów jakiejkolwiek partii politycznej; oraz 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".

([210]) Zabezpieczenia i ograniczenia uprawnień służb wywiadowczych uregulowano również ustawą o uprawnieniach dochodzeniowo-śledczych z 2016 r., która wraz z ustawą regulującą uprawnienia dochodzeniowo-śledcze z 2000 r. w przypadku Anglii, Walii i Irlandii Północnej oraz ustawą regulującą uprawnienia dochodzeniowo-śledcze w Szkocji z 2000 r., w przypadku Szkocji, zapewnia podstawę prawną do korzystania z takich uprawnień. Uprawnienia te nie są jednak istotne w kontekście „dalszego przekazywania", ponieważ obejmują one bezpośrednie gromadzenie danych osobowych przez agencje wywiadowcze. Ocenę uprawnień przyznanych agencjom wywiadowczym na mocy ustawy o uprawnieniach dochodzeniowo-śledczych zawarto w decyzji wykonawczej Komisji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzającej odpowiedni stopień ochrony danych osobowych przez Zjednoczone Królestwo C(2021) 4800.

w niej główne zasady ochrony danych (zgodność z prawem, rzetelność i przejrzystość ([211]); ograniczenie celu ([212]); minimalizacja danych ([213]); prawidłowość ([214]); ograniczenie przechowywania ([215]) i bezpieczeństwo ([216])), określono warunki dotyczące przetwarzania szczególnych kategorii danych ([217]), zapewniono prawa osób, których dane dotyczą, ([218]) określono obowiązek uwzględniania ochrony danych w fazie projektowania ([219]) i uregulowano międzynarodowe przekazywanie danych osobowych ([220]).

(130) Jednocześnie w art. 110 DPA 2018 przewidziano wyłączenie stosowania określonych przepisów zawartych w części 4 tej ustawy, gdy takie wyłączenie jest wymagane do ochrony bezpieczeństwa narodowego. 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. Na wyłączenie to można się powołać na podstawie analizy poszczególnych przypadków ([221]). Jak wyjaśniły władze Zjednoczonego Królestwa i jak potwierdzono w orzecznictwie sądów Zjednoczonego Królestwa, „administrator musi uwzględnić faktyczne konsekwencje dla bezpieczeństwa narodowego lub obrony, gdyby musiał zastosować się do konkretnego przepisu dotyczącego ochrony danych i gdyby istniały racjonalne przesłanki, że mógłby przestrzegać zwykłej zasady bez wpływu na bezpieczeństwo narodowe lub obronę" ([222]). Nad prawidłowym stosowaniem wyłączeń nadzór sprawuje Komisarz ds. Informacji ([223]).

([211]) 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.

([212]) 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 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).

([213]) Dane osobowe muszą być adekwatne, stosowne i nienadmierne w stosunku do celów, dla których są przetwarzane (art. 88 DPA 2018).

([214]) Dane osobowe muszą być prawidłowe i aktualne (art. 89 DPA 2018).

([215]) Danych osobowych nie wolno przechowywać dłużej niż jest to niezbędne (art. 90 DPA 2018).

([216]) 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 zawarto również wymóg, 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.

([217]) Art. 86 ust. 2 lit. b) i załącznik 10 do DPA 2018.

([218]) Część 4 rozdział 3 DPA 2018, a 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.

([219]) Art. 103 DPA 2018.

([220]) 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.

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

([222]) 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, dostępne pod adresem: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Zob. również sprawa Baker przeciwko Secretary of State (zob. przypis 220 powyżej), w której trybunał 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.

([223]) 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).

(131) Ponadto jeżeli chodzi o możliwość ograniczenia któregokolwiek z wymienionych powyżej praw ze względu na ochronę „bezpieczeństwa narodowego", w art. 79 DPA 2018 określono, że administrator może ubiegać się o podpisane przez ministra lub Prokuratora Generalnego poświadczenie potwierdzające, że ograniczenie takich praw jest, lub było w dowolnym momencie, niezbędnym i proporcjonalnym środkiem służącym ochronie bezpieczeństwa narodowego ([224]). Rząd Zjednoczonego Królestwa opublikował wytyczne dotyczące poświadczeń bezpieczeństwa narodowego wydawanych na podstawie DPA 2018, w których podkreślono w szczególności, że wszelkie ograniczenia praw osób, których dane dotyczą, służące do ochrony bezpieczeństwa narodowego muszą być proporcjonalne i niezbędne ([225]). Wszelkie poświadczenia bezpieczeństwa narodowego muszą zostać opublikowane na stronie internetowej Komisarza ds. Informacji ([226]).

(132) Poświadczenie powinno być wydawane na czas określony, nie dłuższy niż pięć lat, tak aby podlegało regularnej ocenie przez władzę wykonawczą ([227]). W poświadczeniu określa się dane osobowe lub kategorie danych osobowych podlegające wyłączeniu, a także przepisy DPA 2018, do których wyłączenie ma zastosowanie ([228]).

(133) Należy zauważyć, że poświadczenia 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 stwierdził, że konieczne jest powołanie się na wyłączenie dotyczące bezpieczeństwa narodowego, co jest możliwe wyłącznie na podstawie oceny każdego przypadku z osobna. Nawet jeżeli do danej sprawy zastosowanie ma poświadczenie bezpieczeństwa narodowego, Komisarz ds. Informacji może zbadać, czy w tym konkretnym przypadku powołanie się na wyłączenie dotyczące bezpieczeństwa narodowego było uzasadnione ([229]).

(134) Każdy, na kogo wydanie poświadczenia wywarło bezpośredni wpływ, może odwołać się od wydania poświadczenia ([230]) do Wyższego Trybunału ([231]) lub, gdy w poświadczeniu dane określono za pomocą ogólnego opisu, zaskarżyć stosowanie poświadczenia w odniesieniu do konkretnych danych ([232]).

(135) W takiej sytuacji Trybunał bada decyzję o wydaniu poświadczenia i orzeka, czy istniały uzasadnione podstawy do jego wydania ([233]). Może rozważyć wiele różnych aspektów, takich jak 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 ([234]).

([224]) 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 DPA 1998 będzie miał zastosowanie w całości, włączając w to możliwość zaskarżenia poświadczenia przez osobę, której dane dotyczą. W chwili obecnej brak jest poświadczeń bezpieczeństwa narodowego wydanych na mocy DPA 1998.

([225]) 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.

([226]) Zgodnie z art. 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.

([227]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, pkt 15, zob. przypis 225.

([228]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, pkt 5, przypis 225.

([229]) 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 powołując się na wyłączenie, uwzględniła szczególne okoliczności sprawy. Komisarz ds. Informacji publikuje również rejestr poświadczeń bezpieczeństwa narodowego, który jest dostępny pod adresem: jest dostępny pod adresem: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

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

([231]) 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.

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

([233]) W sprawie Baker przeciwko Secretary of State (zob. przypis 221) 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.

([234]) Wytyczne rządu Zjednoczonego Królestwa dotyczące poświadczeń bezpieczeństwa narodowego, pkt 25, przypis 224.

(136) Inny zbiór możliwych ograniczeń dotyczy wyłączeń, które stosuje się na podstawie załącznika 11 do DPA 2018 do określonych przepisów zawartych w części 4 DPA 2018 ([235]) 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. 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") ([236]). Na wyłączenia ze względu na szkodę można się powoływać tylko w takim zakresie, 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.

(137) Z powyższego wynika, że – w rozumieniu obowiązujących w Zjednoczonym Królestwie przepisów 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.

(138) Przetwarzanie danych osobowych prowadzone przez służby wywiadowcze na podstawie części 4 DPA 2018 nadzoruje Komisarz ds. Informacji ([237]).

(139) 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 w szczególności 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 postępowań.

(140) 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 ([238]). W odróżnieniu jednak od uprawnień określonych w innych częściach DPA 2018 Komisarz nie może wydać zawiadomienia oceniającego organowi bezpieczeństwa narodowego ([239]).

(141) 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

([235]) Obejmują one: (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.

([236]) 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. Ramy wyjaśniające Zjednoczonego Królestwa dotyczące dyskusji na temat odpowiedniego stopnia ochrony, sekcja H: Bezpieczeństwo narodowe, s. 13, zob. przypis 222.

([237]) Art. 116 DPA 2018.

([238]) Zgodnie z art. 149 ust. 2 w związku z art. 155 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 określono w art. 109 DPA 2018. (Aby uzyskać bardziej szczegółowe informacje na temat zawiadomień egzekucyjnych i zawiadomień w sprawie sankcji, zob. motywy 102–103).

([239]) 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.

informacyjnych, oceniających, egzekucyjnych i w sprawie sankcji), uprawnienie do przeprowadzania inspekcji zgodnie z zobowiązaniami międzynarodowymi, uprawnienia do wstępu i inspekcji oraz przepisy dotyczące przestępstw ([240]). Jak wyjaśniono w motywie 136, wyjątki te będą miały zastosowanie tylko wtedy, gdy jest to niezbędne i proporcjonalne, oraz po przeprowadzeniu oceny każdego przypadku z osobna. Stosowanie tych wyjątków może podlegać kontroli sądowej ([241]).

(142) Komisarz ds. Informacji i służby wywiadowcze Zjednoczonego Królestwa podpisały protokół ustaleń ([242]), który ustanawia ramy współpracy w wielu kwestiach, w tym w zakresie powiadamiania o naruszeniu ochrony danych i rozpatrywania skarg osób, których dane dotyczą. W protokole tym uzgodniono w szczególności, że po otrzymaniu skargi Komisarz ds. Informacji będzie zobowiązany ocenić prawidłowość wszelkich wyłączeń zastosowanych w związku z wystąpieniem zagrożenia dla bezpieczeństwa narodowego. Odpowiednia agencja wskazana w wytycznych rządu Zjednoczonego Królestwa dotyczących poświadczeń bezpieczeństwa narodowego przyjętych na podstawie ustawy o ochronie danych jest zobowiązana odpowiadać na pytania zadawane przez Komisarza ds. Informacji w toku rozpatrywania skarg osób fizycznych w terminie 20 dni roboczych, korzystając w tym celu z odpowiednich bezpiecznych kanałów, jeżeli wspomniane pytania 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 ([243]).

(143) Ponadto nad przetwarzaniem danych osobowych przez agencje wywiadowcze nadzór parlamentarny sprawuje Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa (ISC). Podstawą ustawową regulującą działalność komisji jest ustawa o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. ([244]) Na mocy tej ustawy powołano Komisję ds. Agencji Wywiadowczych i Bezpieczeństwa, która stanowi jedną z komisji parlamentu Zjednoczonego Królestwa. W skład Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa wchodzą członkowie izb parlamentu powołani przez premiera po zasięgnięciu opinii lidera opozycji ([245]). Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa jest zobowiązana przedstawić parlamentowi sprawozdanie roczne ze swojej działalności, a w stosownych przypadkach również inne sprawozdania ([246]).

(144) 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 admini-

([240]) 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 załącznika 13 (inne ogólne funkcje Komisarza).

([241]) Zob. np. sprawa Baker przeciwko Secretary of State for the Home Department (zob. przypis 221).

([242]) Protokół ustaleń między Komisarzem ds. Informacji a wspólnotą wywiadowczą Zjednoczonego Królestwa (UKIC), zob. przypis 231.

([243]) 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 zgłaszane 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).

([244]) Zgodnie z wyjaśnieniami udzielonymi przez władze Zjednoczonego Królestwa w ustawie o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r. 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.

([245]) 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.

([246]) Sprawozdania i opinie komisji są dostępne online pod adresem: http://isc.independent.gov.uk/committee-reports. W 2015 r. Komisja ds. Agencji Wywiadowczych i Bezpieczeństwa opublikowała sprawozdanie pt. „Prywatność i bezpieczeństwo: nowoczesne i przejrzyste ramy prawne" (zob.: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.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.

stracją, 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 ([247]). W protokole ustaleń uzgodnionym między premierem a Komisją ds. Agencji Wywiadowczych i Bezpieczeństwa ([248]) wyszczególniono elementy, które należy wziąć pod uwagę przy ustalaniu, czy dana czynność jest częścią operacji będącej w toku, czy też nie ([249]). 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.

(145) 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 sprzeciwi się temu Sekretarz Stanu ([250]). Władze Zjednoczonego Królestwa wyjaśniły, że w praktyce przypadki odmowy udostępnienia Komisji ds. Agencji Wywiadowczych i Bezpieczeństwa żądanych przez nią informacji zdarzają się niezwykle rzadko ([251]).

(146) Jeżeli chodzi o środki zaskarżenia, to – przede wszystkim – zgodnie z art. 165 ust. 2 DPA 2018 osoba, której dane dotyczą, może wnieść skargę do Komisarza ds. Informacji, jeżeli uważa, że w odniesieniu do danych osobowych, które jej dotyczą, doszło do naruszenia przepisów części 4 DPA 2018, uwzględniając wszelkie nadużycia w zakresie stosowania odstępstw i ograniczeń z tytułu zagrożenia dla bezpieczeństwa narodowego.

(147) 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 ([252]), prawa do wyrażenia sprzeciwu wobec przetwarzania danych ([253]) lub prawa do sprostowania danych bądź ich usunięcia.

(148) 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 ([254]). Szkoda obejmuje zarówno stratę finansową, jak i szkodę niezwiązaną ze stratą finansową, taką jak cierpienie ([255]).

(149) Osoba fizyczna może również wnieść skargę do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych (Investigatory Powers Tribunal) w związku z jakimikolwiek działaniami agencji wywiadowczych Zjednoczonego Królestwa lub jakimikolwiek działaniami podejmowanymi w imieniu tych agencji ([256]). Trybunał ds. Uprawnień Dochodzeniowo-Śledczych ustanowiono na mocy ustawy regulującej uprawnienia dochodzeniowo-śledcze w Anglii, Walii i Irlandii Północnej z 2000 r. oraz na mocy ustawy regulującej uprawnienia dochodzeniowo-śledcze w Szkocji z 2000 r. (RIPA 2000) – jest on niezależny od organów władzy wykonawczej ([257]). Zgodnie z art. 65 RIPA 2000 Jej Królewska Mość powołuje członków Trybunału ds. Uprawnień Dochodzeniowo-Śledczych na pięcioletnią kadencję.

(150) Jej Królewska Mość może odwołać członka Trybunału na podstawie oświadczenia ([258]) obydwu izb parlamentu ([259]).

(151) 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, że (i) 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 ([260]) i że (ii)

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

([248]) 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.

([249]) Protokół ustaleń między premierem a Komisją ds. Agencji Wywiadowczych i Bezpieczeństwa, pkt 14, zob. przypis 248.

([250]) 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 załącznika 1 do ustawy o wymiarze sprawiedliwości i bezpieczeństwie z 2013 r.).

([251]) Ramy wyjaśniające Zjednoczonego Królestwa – sekcja H: Bezpieczeństwo narodowe, s. 43.

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

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

([254]) Art. 169 DPA 2018, który zapewnia możliwość wystąpienia z roszczeniem „osobie, która doznała szkody wskutek niespełnienia wymogu ustanowionego w ustawodawstwie w dziedzinie ochrony danych".

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

([256]) Zob. art. 65 ust. 2 lit. b) RIPA.

([257]) 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.

([258]) Aby uzyskać dodatkowe informacje na temat „oświadczenia", zob. przypis 183.

([259]) Pkt 1 ppkt 5 załącznika 3 do RIPA 2000.

([260]) Art. 65 ust. 4 RIPA 2000.

działania te były podejmowane w „okolicznościach budzących wątpliwości" ([261]) lub „przez służby wywiadowcze bądź w imieniu tych służb" ([262]). Ponieważ do owego „przekonania" stosuje się dość szeroką wykładnię ([263]), wniesienie sprawy do Trybunału podlega stosunkowo łagodnym wymogom w zakresie legitymacji procesowej.

(152) W przypadku gdy Trybunał rozpoznaje 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 ([264]). We wszelkich tego rodzaju postępowaniach przy wydawaniu orzeczeń Trybunał musi stosować te same zasady, które zastosowałby sąd w przypadku wniosku o kontrolę sądową ([265]).

(153) Trybunał ds. Uprawnień Dochodzeniowo-Śledczych musi powiadomić skarżącego o tym, czy wydał orzeczenie na jego korzyść, czy nie ([266]). 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 ([267]). Zgodnie z art. 67 A RIPA 2000 orzeczenie Trybunału można zaskarżyć pod warunkiem uzyskania zgody Trybunału lub właściwego sądu apelacyjnego.

(154) Osoby fizyczne mogą wystąpić z roszczeniem do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych – i uzyskać odszkodowanie – w szczególności w przypadku gdy organ publiczny działał (lub zamierza działać) w sposób naruszający prawa zagwarantowane w EKPC, w tym prawo do prywatności i ochrony danych, a w rezultacie niezgodny z prawem w rozumieniu art. 6 ust. 1 ustawy o prawach człowieka z 1998 r. Trybunał ds. Uprawnień Dochodzeniowo-Śledczych dysponuje właściwością wyłączną do rozpoznawania wszystkich roszczeń przeciwko agencjom wywiadowczym wnoszonych na podstawie ustawy o prawach człowieka. 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 ds. Uprawnień Dochodzeniowo-Śledczych 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 ds. Uprawnień Dochodzeniowo-Śledczych może co do zasady podlegać kontroli sądowej: zob. Korona (Privacy International) przeciwko Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219" ([268]). Jeśli Trybunał ds. Uprawnień Dochodzeniowo-Śledczych stwierdzi, że jakiekolwiek działanie organu publicznego jest niezgodne z prawem, może – w ramach swojej właściwości – zastosować taki środek zabezpieczający lub środek prawny bądź wydać taki nakaz, jaki uzna za sprawiedliwy i właściwy ([269]).

([261]) 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).

([262]) 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%20Statistical%20Report%202016.pdf.

([263]) 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).

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

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

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

([267]) Takim nakazem może być nakaz zniszczenia wszelkich zapisów informacji przechowywanych przez dowolny organ publiczny w odniesieniu do jakiejkolwiek osoby.

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

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

(155) Po wyczerpaniu krajowych środków ochrony prawnej osobie fizycznej przysługuje środek zaskarżenia przed Europejskim Trybunałem Praw Człowieka z tytułu naruszenia praw gwarantowanych na mocy EKPC, w tym prawa do prywatności i ochrony danych.

(156) Z powyższego wynika, że udostępnianie danych przekazanych na podstawie niniejszej decyzji przez organy ścigania Zjednoczonego Królestwa innym organom publicznym, w tym agencjom wywiadowczym, podlega ograniczeniom i warunkom zapewniającym, aby takie dalsze przekazanie było niezbędne i proporcjonalne, a także szczególnym zabezpieczeniom służącym ochronie danych przewidzianym w DPA 2018. Ponadto przetwarzanie danych przez organy publiczne podlega nadzorowi niezależnych organów, a osoby, na które ma ono wpływ, mają dostęp do skutecznych środków ochrony prawnej przed sądem.

3. **WNIOSEK**

(157) Komisja uważa, że część 3 DPA 2018 zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych do celów ścigania przestępstw z właściwych organów w Unii do właściwych organów w Zjednoczonym Królestwie, który zasadniczo odpowiada stopniowi ochrony zagwarantowanemu w dyrektywie (UE) 2016/680.

(158) Ponadto Komisja stwierdza, że mechanizmy nadzoru i możliwości dochodzenia roszczeń przewidziane w prawie Zjednoczonego Królestwa – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia przepisów i w praktyce nakładania za te naruszenia sankcji oraz oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych, a także – ostatecznie – sprostowania lub usunięcia takich danych.

(159) 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 w kontekście udostępniania danych osobowych między organami ścigania i innymi organami publicznymi, takimi jak organy bezpieczeństwa narodowego, będą ograniczać się do tego, co jest ściśle niezbędne do osiągnięcia tego uzasadnionego celu, oraz że ustanowiono skuteczną ochronę prawną przed takimi ingerencjami.

(160) Należy zatem uznać, że Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony w rozumieniu art. 36 ust. 2 dyrektywy (UE) 2016/680, interpretowanego w świetle Karty praw podstawowych.

(161) 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.

4. **SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH**

(162) 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.

(163) Decyzja stwierdzająca odpowiedni stopień ochrony danych osobowych przyjęta przez Komisję na podstawie art. 36 ust. 3 dyrektywy (UE) 2016/680 jest zatem wiążąca dla wszystkich organów państw członkowskich, do których jest skierowana, w tym ich niezależnych organów nadzorczych. W szczególności w okresie stosowania niniejszej decyzji przekazywanie danych przez administratora lub podmiot przetwarzający w Unii administratorom lub podmiotom przetwarzającym w Zjednoczonym Królestwie może odbywać się bez konieczności uzyskania jakiegokolwiek dodatkowego zezwolenia.

(164) Należy przypomnieć, że zgodnie z art. 47 ust. 5 dyrektywy (UE) 2016/680 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems, jeżeli krajowy organ ochrony danych kwestionuje, również na podstawie skargi, zgodność wydanej przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony z podstawowymi prawami osoby do prywatności i ochrony danych, należy zapewnić w prawie krajowym drogę prawną umożliwiającą jej podniesienie tych zarzutów przed sądem krajowym, który może być zobowiązany do wystąpienia z odesłaniem prejudycjalnym do Trybunału Sprawiedliwości ([270]).

([270]) Schrems, pkt 65.

5. MONITOROWANIE, ZAWIESZENIE, UCHYLENIE LUB ZMIANA NINIEJSZEJ DECYZJI

(165) Zgodnie z art. 36 ust. 4 dyrektywy (UE) 2016/680 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, w tym poprzez zawieranie umów międzynarodowych, oraz na wpływ, jaki może to mieć na stopień ochrony zapewnianej danym przekazywanym na mocy niniejszej decyzji; a także na skuteczność wykonywania praw indywidualnych w dziedzinach objętych niniejszą decyzją. W ramach monitorowania Komisja uwzględni m.in. zmiany w orzecznictwie i nadzór ze strony Komisarza ds. Informacji i innych niezależnych organów.

(166) Aby ułatwić to monitorowanie, władze Zjednoczonego Królestwa powinny niezwłocznie i regularnie informować Komisję o wszelkich istotnych zmianach w porządku prawnym Zjednoczonego Królestwa, które mają wpływ na ramy prawne będące przedmiotem niniejszej decyzji, a także o wszelkich zmianach praktyk związanych z przetwarzaniem danych osobowych poddanych ocenie w niniejszej decyzji, w szczególności w odniesieniu do elementów, o których mowa w motywie 165.

(167) Ponadto, aby Komisja mogła skutecznie realizować funkcję monitorowania, państwa członkowskie powinny informować ją o wszelkich istotnych działaniach podejmowanych przez organy ochrony danych państw członkowskich, zwłaszcza w odniesieniu do zapytań lub skarg osób z UE, których dane dotyczą, dotyczących przekazywania danych osobowych z Unii właściwym organom w Zjednoczonym Królestwie. Komisja powinna być również informowana o wszelkich sygnałach świadczących o tym, że działania organów publicznych Zjednoczonego Królestwa odpowiedzialnych za zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych, w tym wszelkich organów nadzoru, nie gwarantują wymaganego stopnia ochrony.

(168) 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.

(169) Jeżeli 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. 58 ust. 2 dyrektywy (UE) 2016/680, w celu częściowego lub całkowitego zawieszenia lub uchylenia niniejszej decyzji.

(170) 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.

(171) W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja skorzysta z możliwości przyjęcia zgodnie z procedurą, o której mowa w art. 58 ust. 3 dyrektywy (UE) 2016/680, mających natychmiastowe zastosowanie aktów wykonawczych zawieszających, uchylających lub zmieniających decyzję.

6. OKRES OBOWIĄZYWANIA I PRZEDŁUŻENIE OBOWIĄZYWANIA NINIEJSZEJ DECYZJI

(172) Należy 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.

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

(174) 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. 58 ust. 2 dyrektywy (UE) 2016/680.

7. **UWAGI KOŃCOWE**

(175) Europejska Rada Ochrony Danych opublikowała swoją opinię ([271]), która została uwzględniona podczas przygotowywania niniejszej decyzji.

(176) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na mocy art. 58 dyrektywy (UE) 2016/680.

(177) Zgodnie z art. 6a Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, który jest załączony do TUE i TFUE, Irlandia nie jest związana przepisami ustanowionymi w dyrektywie (UE) 2016/680, a zatem również w niniejszej decyzji wykonawczej, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, jeżeli Irlandia nie jest związana zasadami regulującymi formy współpracy wymiarów sprawiedliwości w sprawach karnych lub współpracy policyjnej, w ramach której należy przestrzegać przepisów ustanowionych na podstawie art. 16 TFUE. Ponadto zgodnie z decyzją wykonawczą Rady (UE) 2020/1745 ([272]) dyrektywę (UE) 2016/680 należy wprowadzić w życie i stosować tymczasowo w Irlandii od dnia 1 stycznia 2021 r. Irlandia jest zatem związana niniejszą decyzją wykonawczą na takich samych zasadach, jakie mają zastosowanie do stosowania dyrektywy (UE) 2016/680 w Irlandii, jak przewidziano w decyzji wykonawczej (UE) 2020/1745, jeżeli chodzi o dorobek Schengen, w którym uczestniczy.

(178) Zgodnie z art. 2 i 2a Protokołu nr 22 w sprawie stanowiska Danii, który jest załączony do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie jest związana przepisami ustanowionymi w dyrektywie (UE) 2016/680, a zatem również w niniejszej decyzji wykonawczej, dotyczącymi przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres zastosowania części trzeciej tytuł V rozdział 4 lub rozdział 5 TFUE, ani nie podlega stosowaniu tych przepisów. Biorąc jednak pod uwagę fakt, że dyrektywa (UE) 2016/680 opiera się na dorobku Schengen, zgodnie z art. 4 tego Protokołu w dniu 26 października 2016 r. Dania poinformowała o swojej decyzji dotyczącej wdrożenia dyrektywy (UE) 2016/680. W związku z powyższym na mocy prawa międzynarodowego Dania ma obowiązek wprowadzenia w życie przepisów niniejszej decyzji wykonawczej.

(179) W odniesieniu do Norwegii i Islandii niniejsza decyzja wykonawcza stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy zawartej przez Radę Unii Europejskiej i Republikę Islandii oraz Królestwo Norwegii dotyczącej włączenia tych dwóch państw we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([273]).

(180) W odniesieniu do Szwajcarii niniejsza decyzja wykonawcza stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Umowy między Unią Europejską, Wspólnotą Europejską a Konfederacją Szwajcarską w sprawie włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([274]).

(181) W odniesieniu do Liechtensteinu niniejsza decyzja wykonawcza stanowi rozwinięcie przepisów dorobku Schengen w rozumieniu Protokołu między Unią Europejską, Wspólnotą Europejską, Konfederacją Szwajcarską i Księstwem Liechtensteinu w sprawie przystąpienia Księstwa Liechtensteinu do Umowy między Unią Europejską, Wspólnotą Europejską i Konfederacją Szwajcarską dotyczącej włączenia Konfederacji Szwajcarskiej we wprowadzanie w życie, stosowanie i rozwój dorobku Schengen ([275]),

---

([271]) Opinia 15/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej przyjętej na podstawie dyrektywy (UE) 2016/680 w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie, dostępna pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Decyzja wykonawcza Rady (UE) 2020/1745 z dnia 18 listopada 2020 r. w sprawie wprowadzenia w życie przepisów dorobku Schengen dotyczących ochrony danych oraz tymczasowego wprowadzenia w życie niektórych przepisów dorobku Schengen w Irlandii (Dz.U. L 393 z 23.11.2020, s. 3).

([273]) Dz.U. L 176 z 10.7.1999, s. 36.

([274]) Dz.U. L 53 z 27.2.2008, s. 52.

([275]) Dz.U. L 160 z 18.6.2011, s. 21.

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Do celów art. 36 dyrektywy (UE) 2016/680 Zjednoczone Królestwo zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej organom publicznym Zjednoczonego Królestwa odpowiedzialnym za zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych oraz wykonywanie kar.

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. 47 dyrektywy (UE) 2016/680 w odniesieniu do przekazywania danych organom publicznym w Zjednoczonym Królestwie 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 i wykonywanie praw indywidualnych, 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. Jeżeli 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.

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.

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. 58 ust. 2 dyrektywy (UE) 2016/680.

Artykuł 5

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 28 czerwca 2021 r.

W imieniu Komisji
Didier REYNDERS
Członek Komisji