VYKONÁVACIE ROZHODNUTIE KOMISIE (EÚ) 2021/1773

z 28. júna 2021

podľa smernice Európskeho parlamentu a Rady (EÚ) 2016/680 o primeranej ochrane osobných údajov Spojeným kráľovstvom

[oznámené pod číslom C(2021) 4801]

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na smernicu Európskeho parlamentu a Rady (EÚ) 2016/680 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií a o voľnom pohybe takýchto údajov a o zrušení rámcového rozhodnutia Rady 2008/977/SVV ([1]), a najmä na jej článok 36 ods. 3,

keďže:

1. **ÚVOD**

(1) Smernica Európskeho parlamentu a Rady (EÚ) 2016/680 stanovuje pravidlá prenosu osobných údajov z príslušných orgánov v Únii do tretích krajín a medzinárodných organizácií v rozsahu, v akom tieto prenosy spadajú do rozsahu jej pôsobnosti. Pravidlá týkajúce sa medzinárodných prenosov údajov príslušnými orgánmi sú stanovené v kapitole V smernice (EÚ) 2016/680, konkrétnejšie v článkoch 35 až 40. Hoci je pre účinnú spoluprácu v oblasti presadzovania práva nevyhnutný tok osobných údajov do krajín mimo Európskej únie a z nich, musí sa zaručiť, že takéto prenosy neohrozia úroveň ochrany, aká sa osobným údajom priznáva v Európskej únii ([2]).

(2) Podľa článku 36 ods. 3 smernice (EÚ) 2016/680 môže Komisia prostredníctvom vykonávacieho aktu rozhodnúť, že tretia krajina, územie alebo jeden či viaceré určené sektory v tretej krajine alebo medzinárodná organizácia zaručujú primeranú úroveň ochrany. Za tejto podmienky sa prenos osobných údajov do tretej krajiny môže uskutočniť bez potreby získať akékoľvek ďalšie povolenie (s výnimkou prípadov, keď iný členský štát, od ktorého sa údaje získali, musí poskytnúť súhlas na prenos), ako sa stanovuje v článku 35 ods. 1 a odôvodnení 66 smernice (EÚ) 2016/680.

(3) Ako sa uvádza v článku 36 ods. 2 smernice (EÚ) 2016/680, prijatie rozhodnutia o primeranosti musí vychádzať z komplexnej analýzy právneho poriadku tretej krajiny. Komisia musí v rámci svojho posúdenia určiť, či dotknutá tretia krajina zaručuje úroveň ochrany, ktorá v „zásade zodpovedá“ úrovni zabezpečenej v rámci Európskej únie [odôvodnenie 67 smernice (EÚ) 2016/680]. Štandard, voči ktorému sa posudzuje „zásadná rovnocennosť“, je štandard stanovený v právnych predpisoch EÚ, najmä v smernici (EÚ) 2016/680, ako aj v judikatúre Súdneho dvora Európskej únie ([3]). V tejto súvislosti má význam aj referenčné kritérium primeranosti Európskeho výboru pre ochranu údajov ([4]).

(4) Ako objasnil Súdny dvor Európskej únie, nie je potrebné, aby bola zaistená rovnaká úroveň ochrany ([5]). Konkrétne prostriedky, ktoré dotknutá tretia krajina využíva na ochranu osobných údajov, sa môžu líšiť od prostriedkov využívaných v Európskej únii, pokiaľ sa v praxi preukáže, že sa nimi účinne zabezpečuje primeraná úroveň ochrany ([6]). V záujme dosiahnutia štandardu primeranosti teda nie je potrebné, aby pravidlá druhej krajiny do detailu zodpovedali pravidlám Únie. Namiesto toho sa skôr overuje, či príslušný zahraničný systém ako celok zabezpečuje prostredníctvom hmotnoprávnej úpravy práv na súkromie a ich účinného uplatňovania, vymáhania, ako aj dohľadu nad nimi, požadovanú úroveň ochrany ([7]).

([1]) Ú. v. EÚ L 119, 4.5.2016, s. 89.
([2]) Pozri odôvodnenie 64 smernice (EÚ) 2016/680.
([3]) Pozri spomedzi najnovších vec C-311/18, Maximilian Schrems/Data Protection Commissioner („Schrems II“), ECLI:EU:C:2020:559.
([4]) Pozri odporúčania č. 01/2021 týkajúce sa referenčného kritéria primeranosti podľa smernice o presadzovaní práva, prijaté vo februári 2021, k dispozícii na tomto odkaze: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_en.
([5]) Vec C-362/14, Maximillian Schrems/Data Protection Commissioner (ďalej len „Schrems“), ECLI:EU:C:2015:650, bod 73.
([6]) Schrems, bod 74.
([7]) Pozri oznámenie Komisie Európskemu parlamentu a Rade s názvom „Výmena a ochrana osobných údajov v globalizovanom svete“, COM(2017) 7 z 10. 1. 2017, oddiel 3.1, s. 6 – 7, k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:52017DC0007&from=SK.

(5) Komisia dôkladne analyzovala príslušné právne predpisy a prax Spojeného kráľovstva (UK). Komisia na základe svojich zistení uvedených ďalej dospela k záveru, že Spojené kráľovstvo zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných príslušnými orgánmi v Únii, ktoré patria do rozsahu pôsobnosti smernice (EÚ) 2016/680, príslušným orgánom v Spojenom kráľovstve, ktoré patria do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018 (DPA 2018) ([8]).

(6) Toto rozhodnutie má za následok, že takéto prenosy sa môžu uskutočňovať bez potreby získať akékoľvek ďalšie povolenie počas obdobia štyroch rokov s výhradou možného obnovenia a bez toho, aby boli dotknuté podmienky stanovené v článku 35 smernice (EÚ) 2016/680.

2. PRAVIDLÁ, KTORÉ SA VZŤAHUJÚ NA SPRACÚVANIE OSOBNÝCH ÚDAJOV PRÍSLUŠNÝMI ORGÁNMI NA ÚČELY PRESADZOVANIA TRESTNÉHO PRÁVA

2.1. Ústavný rámec

(7) Spojené kráľovstvo je parlamentnou demokraciou. Má suverénny parlament, ktorý je nadriadený všetkým ostatným vládnym inštitúciám, orgán výkonnej moci, ktorý je volený z členov parlamentu a ktorý sa tomuto parlamentu zodpovedá, a nezávislé súdnictvo. Výkonná moc vychádza zo spôsobilosti získať vyslovenie dôvery volenej Dolnej snemovne (House of Commons) a zodpovedá sa obom snemovniam parlamentu [Dolnej snemovne (House of Commons) a Snemovne Lordov (House of Lords)], ktoré sú zodpovedné za kontrolu vlády a za prerokúvanie a prijímanie zákonov. Parlament Spojeného kráľovstva preniesol zodpovednosť za prijímanie právnych predpisov o určitých vnútroštátnych záležitostiach v Škótsku, Walese a Severnom Írsku na škótsky parlament, waleský parlament (Senedd Cymru) a Zhromaždenie Severného Írska. Zatiaľ čo ochrana údajov je záležitosťou vyhradenou parlamentu Spojeného kráľovstva, t. j. rovnaké právne predpisy sa uplatňujú v celej krajine, iné oblasti politiky relevantné pre toto rozhodnutie sú prenesené. Napríklad systémy trestnej justície vrátane policajnej činnosti (činnosti policajných zložiek) v Škótsku a Severnom Írsku sú prenesené na škótsky parlament a Zhromaždenie Severného Írska (Northern Ireland Assembly) ([9]).

(8) Hoci Spojené kráľovstvo nemá kodifikovanú ústavu v zmysle zakotveného ústavného dokumentu, jeho ústavné zásady sa ustálili postupne, vychádzajúc z judikatúry a zvyklostí. Ústavná hodnota niektorých zákonov, ako napríklad Magna Carta, Listina práv z roku 1689 a zákon o ľudských právach z roku 1998 sú uznávanými zdrojmi práva. Základné práva jednotlivcov sa formovali ako súčasť ústavy prostredníctvom common law, právnych predpisov a medzinárodných dohovorov, najmä Európskeho dohovoru o ľudských právach (EDĽP), ktorý Spojené kráľovstvo ratifikovalo v roku 1951. Spojené kráľovstvo v roku 1987 ratifikovalo aj Dohovor Rady Európy o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (dohovor č. 108) ([10]).

(9) Zákon o ľudských právach z roku 1998 začleňuje práva obsiahnuté v EDĽP do práva Spojeného kráľovstva. Zákon zaručuje každému jednotlivcovi základné práva a slobody stanovené v článkoch 2 až 12 a 14 EDĽP a v článkoch 1 až 3 jeho prvého protokolu a v článku 1 jeho trinásteho protokolu v spojení s článkami 16 až 18 EDĽP. Patrí sem právo na rešpektovanie súkromného a rodinného života, ktoré zase zahŕňa právo na ochranu údajov a právo na spravodlivý proces ([11]). Najmä v súlade s článkom 8 EDĽP môže štátny orgán do výkonu práva na súkromie zasahovať len v prípadoch, keď je to v súlade so zákonom a nevyhnutné v demokratickej spoločnosti v záujme národnej bezpečnosti, verejnej bezpečnosti, hospodárskeho blahobytu krajiny, predchádzania nepokojom a zločinnosti, ochrany zdravia alebo morálky alebo ochrany práv a slobôd iných.

([8]) Data Protection Act 2018 (zákon o ochrane údajov z roku 2018), k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Vysvetľujúcom rámci Spojeného kráľovstva pre diskusiu o primeranosti, oddiel F s názvom „Presadzovanie práva“, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Zásady dohovoru č. 108 boli pôvodne implementované do právneho poriadku Spojeného kráľovstva prostredníctvom zákona o ochrane údajov z roku 1984 [Data Protection Act (DPA) of 1984], ktorý bol nahradený DPA 1998, a následne DPA 2018 (v spojení so všeobecným nariadením Spojeného kráľovstva o ochrane údajov). Spojené kráľovstvo tiež v roku 2018 podpísalo protokol, ktorým sa mení Dohovor o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov (známy ako „dohovor 108+“), a v súčasnosti pracuje na ratifikácii dohovoru.

([11]) Články 6 a 8 EDĽP (pozri aj prílohu 1 k zákonu o ľudských právach z roku 1998).

(10) V súlade so zákonom o ľudských právach z roku 1998 musí byť každá činnosť orgánov verejnej moci zlučiteľná s právami zaručenými EDĽP ([12]). Okrem toho je potrebné, aby sa primárne a podriadené právne predpisy interpretovali a uplatňovali spôsobom, ktorý je zlučiteľný s týmito právami ([13]). Pokiaľ sa jednotlivec domnieva, že orgány verejnej moci porušili jeho práva vrátane práva na súkromie a ochranu údajov, môže získať nápravu na súdoch Spojeného kráľovstva podľa zákona o ľudských právach z roku 1998 a prípadne po vyčerpaní vnútroštátnych prostriedkov nápravy môže získať nápravu na Európskom súde pre ľudské práva za porušenie práv zaručených podľa EDĽP.

2.2. **Rámec ochrany údajov Spojeného kráľovstva**

(11) Spojené kráľovstvo vystúpilo z Únie 31. januára 2020. Na základe Dohody o vystúpení Spojeného kráľovstva Veľkej Británie a Severného Írska z Európskej únie a z Európskeho spoločenstva pre atómovú energiu ([14]) sa právo Únie naďalej uplatňovalo v Spojenom kráľovstve počas prechodného obdobia do 31. decembra 2020. Pred vystúpením a počas prechodného obdobia právny rámec na ochranu osobných údajov v Spojenom kráľovstve, ktorým sa upravuje spracúvanie osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu, pozostával z príslušných častí zákona o ochrane údajov z roku 2018, ktorým sa transponovala smernica (EÚ) 2016/680.

(12) S cieľom pripraviť sa na vystúpenie z EÚ vláda Spojeného kráľovstva prijala zákon o vystúpení z Európskej únie (ďalej len „zákon o vystúpení“) z roku 2018 ([15]), ktorým sa priamo uplatniteľné právne predpisy Únie začlenili do práva Spojeného kráľovstva a v ktorom sa stanovilo, že takzvané „vnútroštátne právne predpisy odvodené od EÚ“ budú naďalej platiť aj po skončení prechodného obdobia. Časť 3 zákona o ochrane údajov z roku 2018 ([16]), ktorou sa transponuje smernica (EÚ) 2016/680, predstavuje podľa zákona o vystúpení „vnútroštátne právne predpisy odvodené od EÚ“. V súlade so zákonom o vystúpení musia súdy Spojeného kráľovstva vykladať nezmenené „vnútroštátne právne predpisy odvodené od EÚ“ v súlade s príslušnou judikatúrou Súdneho dvora Európskej únie (ďalej len „Súdny dvor“) a všeobecnými zásadami práva Únie tak, ako boli účinné bezprostredne pred skončením prechodného obdobia (ďalej len „ponechaná judikatúra EÚ“, resp. „ponechané všeobecné zásady práva EÚ“) ([17]).

(13) Podľa zákona o vystúpení majú ministri Spojeného kráľovstva právomoc prostredníctvom štatutárnych nástrojov zaviesť sekundárne právne predpisy s cieľom zaviesť potrebné úpravy ponechaného práva EÚ, ktoré vyplývajú z vystúpenia Spojeného kráľovstva z Únie. Výsledkom uplatnenia tejto právomoci sú právne predpisy o ochrane údajov, súkromia a elektronických komunikáciách v dôsledku vystúpenia z EÚ z roku 2019 (právne predpisy DPPEC) ([18]). Menia sa nimi právne predpisy Spojeného kráľovstva o ochrane údajov vrátane zákona o ochrane údajov z roku 2018, aby zodpovedali vnútroštátnym okolnostiam ([19]).

([12]) § 6 zákona o ľudských právach z roku 1998.

([13]) § 3 zákona o ľudských právach z roku 1998.

([14]) Dohoda o vystúpení Spojeného kráľovstva Veľkej Británie a Severného Írska z Európskej únie a z Európskeho spoločenstva pre atómovú energiu 2019/C 384 I/01, XT/21054/2019/INIT, Ú. v. EÚ C 384I, 12. 11. 2019, s. 1 – 177 („dohoda o vystúpení“), k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=SK.

([15]) Zákon o vystúpení z Európskej únie z roku 2018, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([16]) Zákon o ochrane údajov z roku 2018, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([17]) Článok 6 zákona o vystúpení z roku 2018.

([18]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (právne predpisy o ochrane údajov, súkromia a elektronických komunikáciách v dôsledku vystúpenia z EÚ z roku 2019), k dispozícii na tomto odkaze: https://www.legislation.gov.uk/uksi/2019/419/contents/made, zmenené DPPEC 2020, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) V právnych predpisoch o ochrane údajov, súkromia a elektronických komunikáciách v dôsledku vystúpenia z EÚ z roku 2019 sa vykonáva niekoľko zmien časti 3 zákona o ochrane údajov z roku 2018. Mnohé z nich sú technické zmeny, ako napríklad vypustenie odkazov na „členský štát“ alebo „smernicu o presadzovaní práva“ [pozri napríklad § 48 ods. 8 alebo § 73 ods. 5 písm. a) zákona o ochrane údajov z roku 2018, kde sa vložil odkaz na „vnútroštátne právo“], aby sa umožnilo účinné fungovanie časti 3 ako vnútroštátneho právneho predpisu po skončení prechodného obdobia. Na niektorých miestach boli potrebné iné druhy zmien, napríklad v súvislosti s tým, kto je oprávnený na prijímanie „rozhodnutí o primeranosti“ na účely legislatívneho rámca Spojeného kráľovstva v oblasti ochrany údajov (pozri oddiel § 74A zákona o ochrane údajov z roku 2018), t. j. minister namiesto Európskej komisie.

(14) V dôsledku toho sa právne štandardy týkajúce sa spracúvania osobných údajov príslušnými orgánmi na účely predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo na účely výkonu trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti v Spojenom kráľovstve a predchádzania takémuto ohrozeniu po prechodnom období podľa dohody o vystúpení naďalej stanovujú v príslušných častiach zákona o ochrane údajov z roku 2018, ale zmeneného právnymi predpismi DPPEC, najmä v časti 3 uvedeného zákona. Všeobecné nariadenie Spojeného kráľovstva o ochrane údajov sa na tento typ spracúvania nevzťahuje.

(15) V časti 3 zákona o ochrane údajov z roku 2018 sa stanovujú pravidlá spracúvania osobných údajov na účely presadzovania trestného práva vrátane zásad ochrany údajov, právnych dôvodov spracúvania (zákonnosť), práv dotknutých osôb, povinností príslušných orgánov ako prevádzkovateľov a obmedzení následných prenosov. Zároveň sú v častiach 5 a 6 zákona o ochrane údajov z roku 2018 stanovené pravidlá týkajúce sa dohľadu, presadzovania a nápravy uplatniteľné na sektor presadzovania práva.

(16) Okrem toho vzhľadom na dôležitú úlohu, ktorú policajné zložky zohrávajú v oblasti presadzovania práva, by sa mali posúdiť pravidlá upravujúce policajnú činnosť. Keďže policajné právomoci boli prenesené na nižšie celky, policajnú činnosť v a) Anglicku a Walese, b) Škótsku a c) Severnom Írsku upravujú rôzne právne predpisy, ktoré sú však z hľadiska obsahu často podobné ([20]). Ďalšie objasnenia toho, ako by sa mali využívať policajné právomoci, poskytujú ďalej rôzne druhy usmerňovacích dokumentov. Existujú tri hlavné formy policajného usmernenia: 1. zákonné usmernenie, ktoré sa vydáva na základe právnych predpisov, ako je napr. etický kódex (Code of Ethics) ([21]) a kódex praxe správy policajných informácií (Code of Practice on the Management of Police Information) ([22]), ktoré boli vydané na základe policajného zákona z roku 1996 ([23]) alebo tzv. kódexy PACE (PACE codes) ([24]) vydané na základe zákona o polícii a dôkazoch v trestných veciach z roku 1984 ([25]), 2. autorizovaná profesijná prax správy policajných informácií ([26]) vydaná policajnou akadémiou College of Policing a 3. operatívne usmernenie vydané samotnou políciou. Národná rada policajných riaditeľov (The National Police Chiefs Council), ktorá je koordinačným orgánom pre všetky policajné zložky Spojeného kráľovstva, uverejňuje operačné usmernenie, ktoré schválili všetky policajné zložky a ktoré sa preto uplatňuje na celoštátnej úrovni ([27]). Cieľom tohto usmernenia je zabezpečiť medzi policajnými zložkami konzistentnosť v spôsobe správy informácií ([28]).

(17) Kódex praxe správy policajných informácií vydal minister v roku 2005 na základe právomocí stanovených v § 39A zákona o polícii z roku 1996 ([29]). Každý kódex praxe vydaný podľa zákona o polícii musí byť odsúhlasený ministrom a predtým, ako sa predloží parlamentu, musí byť prekonzultovaný s Národnou kriminálnou agentúrou. V § 39A ods. 7 zákona o polícii sa vyžaduje, aby polícia náležite zohľadnila kódexy vydané podľa zákona, a preto sa

([20]) Podrobnejšie vysvetlenie o policajných zložkách a ich právomociach v Spojenom kráľovstve nájdete vo Vysvetľujúcom rámci Spojeného kráľovstva pre diskusiu o primeranosti, oddiel F s názvom „Presadzovanie práva“ (pozri poznámku pod čiarou č. 9).

([21]) Kódex praxe v oblasti zásad a noriem profesionálneho správania pre policajnú profesiu v Anglicku a Walese, k dispozícii na tomto odkaze: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Etický kódex Policajného zboru Severného Írska, k dispozícii na tomto odkaze: https://www.nipolicingboard.org.uk/psni-code-ethics; Etický kódex pre policajnú činnosť v Škótsku, k dispozícii na tomto odkaze: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Kódex praxe správy policajných informácií, k dispozícii na tomto odkaze: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Policajný zákon z roku 1996, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Kódexy PACE vydané na základe zákona o polícii a dôkazoch v trestných veciach z roku 1984 sú k dispozícii na tomto odkaze: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Zákon o polícii a dôkazoch v trestných veciach z roku 1984, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Autorizovaná profesijná prax správy policajných informácií, k dispozícii na tomto odkaze: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Príručka o ochrane údajov pre odborníkov polície pracujúcich v oblasti ochrany údajov, k dispozícii na tomto odkaze: https://www.npcc.police.uk/2019 %20FOI/IMORCC/225 %2019 %20NPCC%20DP%20Manual%20Draft%200.11 %20Mar%202019.pdf.

([28]) Kódex praxe správy policajných informácií (pozri poznámku pod čiarou č. 22) sa napr. uplatňuje na uchovávanie operatívnych informácií polície [pozri odôvodnenie (47) tohto rozhodnutia].

([29]) Podľa informácií, ktoré poskytli orgány Spojeného kráľovstva pracovala policajná akadémia College of Policing v čase rokovaní o primeranosti na príprave Kódexu postupov správy informácií a záznamov, ktorým by sa mal Kódex praxe správy policajných informácií nahradiť. Návrh kódexu bol 25. januára 2021 uverejnený na účely verejnej konzultácie a je k dispozícii na tomto odkaze: https://www.college.police.uk/article/information-records-management-consultation.

od polície očakáva, že ich bude dodržiavať ([30]). Okrem toho usmernenie opierajúce sa o iný základ ako právny predpis (ako napr. autorizovaná profesijná prax správy policajných informácií) musí byť vždy v súlade s Kódexom praxe správy policajných informácií, ktorý je mu nadradený ([31]). V každom prípade, hoci môžu nastať určité operačné situácie, keď sa príslušníci polície musia odchýliť od tohto usmernenia, stále sú povinní dodržiavať požiadavky uvedené v časti 3 zákona o ochrane údajov z roku 2018 ([32]).

(18) Ďalšie usmernenie k právnym predpisom Spojeného kráľovstva o ochrane údajov pri spracúvaní v oblasti presadzovania práva poskytuje Komisár pre informácie (Information Commissioner – ICO) ([33]) (ďalšie podrobnosti o ICO sú uvedené v odôvodneniach (93) až (109)). Hoci nie je právne záväzné, v súdnom prípade by súdy boli povinné zohľadniť akékoľvek porušenie usmernenia, keďže má význam z hľadiska výkladu a ozrejmuje sa v ňom, ako Komisár pre informácie v praxi vykladá a presadzuje právne predpisy o ochrane údajov ([34]).

(19) Napokon, ako sa uvádza v odôvodneniach (8) až (10), orgány Spojeného kráľovstva príslušné na presadzovanie práva musia zabezpečiť súlad s EDĽP a dohovorom č. 108.

(20) Právny rámec upravujúci spracúvanie údajov orgánmi Spojeného kráľovstva príslušnými na presadzovanie trestného práva je preto svojou štruktúrou a hlavnými prvkami veľmi podobný tomu, ktorý sa uplatňuje v EÚ. To zahŕňa aj skutočnosť, že takýto rámec sa neopiera len o povinnosti stanovené vo vnútroštátnom práve, ktoré boli formované právom EÚ, ale aj o povinnosti zakotvené v medzinárodnom práve, najmä prostredníctvom pristúpenia Spojeného kráľovstva k EDĽP a dohovoru č. 108, ako aj o podriadenie tohto rámca pod právomoc Európskeho súdu pre ľudské práva. Tieto povinnosti vyplývajúce z právne záväzných medzinárodných nástrojov, najmä pokiaľ ide o ochranu osobných údajov, sú preto osobitne dôležitým prvkom právneho rámca posudzovaného v tomto rozhodnutí.

2.3. **Vecná a územná pôsobnosť**

(21) Vecná pôsobnosť časti 3 zákona o ochrane údajov z roku 2018 sa zhoduje s rozsahom pôsobnosti smernice (EÚ) 2016/680 v zmysle vymedzenia tohto rozsahu v jej článku 2 ods. 2 Časť 3 sa vzťahuje na spracúvanie osobných údajov zo strany príslušného orgánu vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie zo strany príslušného orgánu inak než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

(22) Okrem toho, aby prevádzkovateľ patril do rozsahu pôsobnosti uvedenej časti 3, musí byť „príslušným orgánom“ a spracúvanie sa musí vykonávať na „účel presadzovania práva“. Z tohto dôvodu režim ochrany údajov, ktorý je predmetom tohto posúdenia v tomto rozhodnutia, sa vzťahuje na všetky činnosti v oblasti presadzovania práva týchto príslušných orgánov.

(23) Pojem „príslušný orgán“ je vymedzený v § 30 zákona o ochrane údajov z roku 2018 ako osoba uvedená v prílohe 7 k zákonu o ochrane údajov z roku 2018, ako aj akákoľvek iná osoba v rozsahu, v akom má zákonné funkcie na ktorýkoľvek z účelov presadzovania práva. Medzi príslušné orgány uvedené v prílohe 7 patria nielen policajné zložky, ale aj všetky ministerské úrady Spojeného kráľovstva, ako aj ďalšie orgány s vyšetrovacími funkciami, napr. komisár daňového a colného úradu jej veličenstva (Commissioner for Her Majesty's Revenue and Customs), waleský daňový úrad (Welsh Revenue Authority), orgán pre hospodársku súťaž a trhy (Competition and Markets Authority), kataster nehnuteľností jej veličenstva (Her Majesty's Land Register) alebo Národná kriminálna agentúra (National

([30]) Vo veci R/Komisariát metropolitnej polície [2014] EWCA Civ 585 bolo potvrdené právne postavenie Kódexu praxe správy policajných informácií a sudca Lord Justice Laws vyhlásil, že metropolitný policajný komisár je podľa § 39A zákona o polícii z roku 1996 povinný dodržiavať tento kódex a autorizovanú profesijnú prax správy policajných informácií.

([31]) Dodržiavanie Kódexu praxe správy policajných informácií zo strany polície kontroluje inšpekčná služba jej veličenstva pre policajný, hasičský a záchranný zbor (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services).

([32]) V tejto súvislosti pozri stanovisko policajnej akadémie College of Policing k dodržiavaniu usmernenia autorizovanej policajnej praxe, pokiaľ ide o všetky prvky policajnej činnosti; v tomto stanovisku sa ozrejmuje, že autorizovanú profesijnú prax schvaľuje profesijná komora pre policajnú činnosť (policajná akadémia College of Policing) ako oficiálny zdroj profesijnej praxe v oblasti policajnej činnosti. Od príslušníkov polície a zamestnancov sa očakáva, že pri plnení svojich povinností budú túto autorizovanú profesijnú prax zohľadňovať. Môžu však existovať okolnosti, za ktorých existuje legitímny operatívny dôvod na to, aby sa policajné zložky odchýlili od autorizovanej profesijnej praxe, za predpokladu, že na to existuje jasný dôvod. V takom prípade by bolo na policajnej zložke, aby niesla zodpovednosť za akékoľvek miestne a celoštátne riziko spojené s pôsobením mimo rámca celoštátne odsúhlasených usmernení a ak v dôsledku toho dôjde k incidentu alebo vyšetrovaniu (napríklad prostredníctvom nezávislého dozorného orgánu Independent Office of Police Conduct), za akékoľvek riziko nesie zodpovednosť policajná zložka. Materiál k dispozícii na tomto odkaze: https://www.app.college.police.uk/faq-page/.

([33]) Usmernenie k spracúvaniu údajov na účely presadzovania práva, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Pozri vec Bridges/The Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), kde síce Vrchný súd (High Court) poukázal na to, že usmernenie Komisára pre informácie nemá zákonnú povahu, zároveň však uviedol, že pri posudzovaní toho, či prevádzkovateľ údajov splnil alebo nesplnil povinnosť podľa § 64 (t. j. povinnosť vykonať pri vysokorizikovom spracúvaní posúdenie vplyvu z hľadiska ochrany údajov), je súd povinný zohľadniť usmernenia, ktoré vydal Komisár pre informácie v súvislosti s posúdeniami vplyvu na ochranu údajov.

Crime Agency), vyšetrovacie orgány, iné orgány s pôsobnosťou v oblasti trestnej justície a ďalšie subjekty alebo organizácie vykonávajúce činnosti v oblasti presadzovania práva ([35]). Časť 3 zákona o ochrane údajov z roku 2018 sa vzťahuje aj na súdy a tribunály pri výkone ich súdnych funkcií, s výnimkou časti týkajúcej sa práv dotknutých osôb a dohľadu Komisára pre informácie ([36]). Zoznam príslušných orgánov uvedený v prílohe 7 nie je konečný a minister ho môže aktualizovať právnym predpisom, aby zohľadnil zmeny v organizácii verejných úradov ([37]).

(24) Príslušné spracúvanie sa okrem toho musí uskutočňovať na „účel presadzovania práva“, ktorý sa vymedzuje ako predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, resp. výkon trestných sankcií vrátane ochrany pred ohrozením verejnej bezpečnosti a predchádzania takémuto ohrozeniu ([38]). Časť 3 zákona o ochrane údajov z roku 2018 neupravuje spracúvanie zo strany príslušného orgánu, ak k nemu nedochádza na účely presadzovania práva. K tomu dochádza napríklad vtedy, keď orgán pre hospodársku súťaž a trhy (Competition and Markets Authority) vyšetruje prípady, ktoré nemajú charakter trestnej činnosti (napr. fúzie spoločností). V takom prípade sa bude uplatňovať všeobecné nariadenie Spojeného kráľovstva o ochrane údajov spolu s časťou 2 zákona o ochrane údajov z roku 2018, keďže spracúvanie osobných údajov príslušnými orgánmi sa vykonáva na iné účely ako na účely presadzovania práva. S cieľom určiť, ktorý režim ochrany údajov (časť 3 či časť 2 zákona o ochrane údajov z roku 2018) sa na príslušné spracúvanie predmetných osobných údajov uplatňuje, musí príslušný orgán (t. j. prevádzkovateľ) zvážiť, či je „primárnym účelom“ takéhoto spracúvania jeden z účelov presadzovania práva podľa zákona o ochrane údajov z roku 2018.

(25) Pokiaľ ide o územnú pôsobnosť časti 3 zákona o ochrane údajov z roku 2018, v § 207 ods. 2 sa stanovuje, že zákon o ochrane údajov z roku 2018 sa vzťahuje na spracúvanie osobných údajov v súvislosti s činnosťami osoby, ktorá je usadená kdekoľvek na území Spojeného kráľovstva. To zahŕňa orgány verejnej moci na území Anglicka, Walesu, Škótska a Severného Írska, ktoré patria do vecnej pôsobnosti časti 3 zákona o ochrane údajov z roku 2018 ([39]).

2.3.1. *Vymedzenie osobných údajov a spracovania*

(26) Kľúčové pojmy osobných údajov a spracúvania sú vymedzené v oddiele 3 zákona o ochrane údajov z roku 2018 a uplatňujú sa v rámci celého tohto právneho predpisu. Toto vymedzenie pojmov sa dôsledne riadi zodpovedajúcimi vymedzeniami pojmov stanovenými v článku 3 smernice (EÚ) 2016/680. Podľa zákona o ochrane údajov z roku 2018 sú osobné údaje akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej žijúcej osoby ([40]). Podľa § 3 ods. 3 zákona o ochrane údajov z roku 2018 je fyzická osoba identifikovateľná, ak ju možno priamo alebo nepriamo identifikovať na základe informácií vrátane odkazu na meno alebo identifikátor, resp. odkazom na jeden alebo viacero faktorov špecifických pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu osoby. Pojem „spracúvanie“ je definovaný ako operácia alebo súbor operácií, ktoré sa vykonávajú v súvislosti s informáciami alebo súbormi informácií, ako je napr. a) získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie alebo uchovávanie; b) prepracúvanie alebo zmena; c) vyhľadávanie, prehliadanie alebo využívanie; d) poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom; e) preskupovanie alebo kombinovanie, alebo f) obmedzenie, vymazanie alebo likvidácia. Okrem toho sa v tomto zákone vymedzuje „citlivé spracovanie“; ako a) spracúvanie osobných údajov odhaľujúcich rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách; b) spracúvanie genetických údajov alebo biometrických údajov na účely jedinečnej identifikácie jednotlivca; c) spracúvanie údajov týkajúcich sa zdravia; d) spracúvanie údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie jednotlivca ([41]). V tejto súvislosti sa v § 205 zákona o ochrane údajov z roku 2018 uvádza vymedzenie pojmov „biometrické údaje“ ([42]), „údaje týkajúce sa zdravia“ ([43]) a „genetické údaje“ ([44]).

([35]) Popri nich sú v prílohe 7 k zákonu o ochrane údajov z roku 2018 uvedení riaditelia prokuratúry, riaditelia prokuratúry pre Severné Írsko, resp. Komisia pre informácie.

([36]) § 43 ods. 3 zákona o ochrane údajov z roku 2018.

([37]) § 30 ods. 3 zákona o ochrane údajov z roku 2018. Spravodajské služby (Secret Intelligence Service, Security Service a Government Communications Headquarters) nie sú príslušnými orgánmi (pozri § 30 ods. 2 zákona o ochrane údajov z roku 2018) a časť 3 zákona o ochrane údajov z roku 2018 sa na žiadnu z ich činností nevzťahuje. Ich činnosti patria do rozsahu pôsobnosti časti 4 zákona o ochrane údajov z roku 2018.

([38]) § 31 zákona o ochrane údajov z roku 2018.

([39]) To znamená, že zákon o ochrane údajov z roku 2018, a teda ani toto rozhodnutie, sa nevzťahuje na korunné dependencie Spojeného kráľovstva ani jeho ostatné zámorské územia, ako sú napríklad Falklandské ostrovy a územie Gibraltáru.

([40]) Osobné údaje týkajúce sa zosnulej osoby nepatria do rozsahu pôsobnosti zákona o ochrane údajov z roku 2018.

([41]) § 35 ods. 8 zákona o ochrane údajov z roku 2018.

([42]) „Biometrické údaje“ sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov jednotlivca a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tohto jednotlivca, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje.

([43]) „Údaje týkajúce sa zdravia“ sú osobné údaje týkajúce sa fyzického alebo duševného zdravia jednotlivca, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jeho zdravotnom stave.

([44]) „Genetické údaje“ sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov jednotlivca, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tohto jednotlivca a ktoré vyplývajú najmä z analýzy biologickej vzorky daného jednotlivca.

(27) V § 32 zákona o ochrane údajov z roku 2018 sa objasňujú vymedzenia pojmov „prevádzkovateľ“ a „sprostredkovateľ“ v súvislosti so spracúvaním osobných údajov na účely presadzovania práva, pričom sa dôsledne dodržiavajú rovnocenné vymedzenia pojmov obsiahnuté v smernici (EÚ) 2016/680. Prevádzkovateľ je príslušný orgán, ktorý určuje účely a prostriedky spracúvania osobných údajov. Ak sa spracúvanie vyžaduje zo zákona, prevádzkovateľom je príslušný orgán, ktorému tento zákon ukladá takúto povinnosť. Sprostredkovateľ sa vymedzuje ako akákoľvek osoba, ktorá spracúva osobné údaje v mene prevádzkovateľa (iná ako osoba, ktorá je zamestnancom prevádzkovateľa).

2.4. **Záruky, práva a povinnosti**

2.4.1. *Zákonnosť a spravodlivosť spracúvania*

(28) Podľa § 35 zákona o ochrane údajov z roku 2018 musí byť spracúvanie osobných údajov zákonné a spravodlivé, podobne ako sa stanovuje v článku 4 ods. 1 písm. a) smernice (EÚ) 2016/680. Podľa § 35 ods. 2 zákona o ochrane údajov z roku 2018 je spracúvanie osobných údajov na ktorýkoľvek z účelov presadzovania práva zákonné len vtedy, ak je založené na zákone a dotknutá osoba vyjadrila súhlas so spracúvaním na tento účel, alebo ak je spracúvanie nevyhnutné na splnenie úlohy, ktorú na tento účel vykonáva príslušný orgán.

2.4.1.1. Spracúvanie na základe zákona

(29) Podobne ako v článku 8 smernice (EÚ) 2016/680, aby sa zabezpečila zákonnosť spracúvania, na ktoré sa vzťahuje časť 3 zákona o ochrane údajov z roku 2018, takéto spracúvanie musí byť „na základe zákona“. „Zákonné“ spracovanie je povolené buď zákonom, common law alebo kráľovskými výsadami ([45]).

(30) Právomoci príslušných orgánov sa vo všeobecnosti riadia právnymi predpismi, čo znamená, že ich funkcie a právomoci sú jasne stanovené v právnych predpisoch prijatých parlamentom ([46]). V určitých prípadoch sa polícia, ako aj iné príslušné orgány uvedené v prílohe 7 k zákonu o ochrane údajov z roku 2018 môžu pri spracúvaní údajov opierať o common law ([47]). Common law sa vytvorilo prostredníctvom precedensov vytvorených rozhodnutiami súdov. Common law je relevantné v súvislosti s právomocami, ktoré má polícia k dispozícii a ktorá z tohto prameňa práva odvodzuje svoju základnú povinnosť chrániť verejnosť odhaľovaním a predchádzaním trestnej činnosti ([48]). Policajné

([45]) Vysvetlivky k zákonu o vystúpení z Európskej únie z roku 2018, bod 181, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Národná kriminálna agentúra napríklad odvodzuje svoje právomoci zo zákona o trestnej činnosti a súdoch z roku 2013, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2013/22/contents. Podobne právomoci agentúry pre potravinové normy (Food Standards Agency) sú stanovené v zákone o potravinových normách z roku 1999k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1999/28/contents. Medzi ďalšie príklady patrí zákon o prokuratúre z roku 1985, ktorým sa zriadila prokuratúra (Crown Prosecution Service) (pozri https://www.legislation.gov.uk/ukpga/1985/23/contents), zákon o komisároch pre dane a clá z roku 2005, ktorým sa zriadili daňové a colné orgány jej veličenstva (pozri https://www.legislation.gov.uk/ukpga/2005/11/contents), zákon o trestnom konaní (Škótsko) z roku 1995, ktorým sa zriadila Škótska komisia pre preskúmanie trestných prípadov (pozri https://www.legislation.gov.uk/ukpga/1995/46/contents), zákon o súdnictve (Severné Írsko) z roku 2002, ktorým sa zriadila prokuratúra v Severnom Írsku (pozri https://www.legislation.gov.uk/ukpga/2002/26/contents) a Úrad pre závažné podvody bol vytvorený a vybavený právomocami podľa zákona o trestnej justícii z roku 1987 (pozri https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Napríklad podľa informácií, ktoré poskytli orgány Spojeného kráľovstva, v rámci Crown Office and Procurator Fiscal Service, ktorý je zodpovedný za stíhanie prípadov v Škótsku, Lord Advocate, ktorý je vedúcim systému trestného stíhania v Škótsku, odvodzuje svoje právomoci vyšetrovať úmrtia a stíhať činy trestné podľa common law, zatiaľ čo niektoré z jeho funkcií sú stanovené zákonom. Okrem toho koruna a v širšom zmysle rôzne vlády, ministerstvá a ministri tiež odvodzujú svoje právomoci z kombinácie právnych predpisov, common law a kráľovskej výsady (ide o právomoci podľa common law zverené korune, ktoré však vykonávajú ministri).

([48]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel F s názvom „Presadzovanie práva“, s. 8 (pozri poznámku pod čiarou č. 9).

zložky však majú na výkon takejto povinnosti tak právomoci vyplývajúce z common law, ako aj zákonné právomoci ([49]). Ak má polícia zákonnú právomoc, nahrádza to akúkoľvek právomoc na základe common law ([50]).

(31) Súdy uznali, že rozsah právomocí a povinností príslušníkov polície podľa common law zahŕňa všetky kroky, ktoré príslušník polície považuje za potrebné na udržanie mieru, predchádzanie trestnej činnosti alebo ochranu majetku pred ujmou vzniknutou v dôsledku trestného činu ([51]). Právomoci na základe common law nie sú neobmedzené právomoci. Vzťahujú sa na ne rôzne obmedzenia vrátane obmedzení stanovených súdmi ([52]) a právnymi predpismi, najmä zákonom o ľudských právach z roku 1998 a zákonom o rovnosti z roku 2010 ([53]). Okrem toho v prípade príslušných orgánov, ktoré spracúvajú údaje podľa časti 3 zákona o ochrane údajov z roku 2018, to zahŕňa uplatňovanie právomocí podľa common law v súlade s požiadavkami stanovenými v zákona o ochrane údajov z roku 2018 ([54]). Ďalej sa pri rozhodovaní o vykonaní akéhokoľvek druhu spracovania údajov musia zohľadniť požiadavky platných usmernení, ako je Kódex praxe správy policajných informácií, ako aj usmernenia špecifické pre príslušnú časť Spojeného kráľovstva ([55]). Vláda a operatívne zložky polície vydávajú viaceré usmerňujúce dokumenty s cieľom zabezpečiť, aby príslušníci polície uplatňovali svoje právomoci v rámci obmedzení stanovených v common law alebo príslušnom zákone ([56]).

(32) Ďalšiu súčasť práva predstavujú kráľovské výsady, ktoré znamenajú určité právomoci zverené korune a uplatniteľné výkonnou mocou, ktoré však nie sú založené na právnom predpise, ale vyplývajú zo suverenity monarchu ([57]). Existuje len veľmi málo príkladov, v ktorých sú právomoci vyplývajúce z výsad relevantné v kontexte presadzovania práva. Zahŕňajú napríklad rámec vzájomnej právnej pomoci, ktorý umožňuje výmenu údajov medzi ministrom

([49]) Kľúčové právne predpisy, ktorými sa stanovuje režim hlavných policajných právomocí (zatknutie, prehliadky, povolenie na pokračovanie zadržiavania, odoberanie odtlačkov prstov, odber intímnych vzoriek, príkaz na zadržanie, prístup ku komunikačným údajom), sú: i), v prípade Anglicka a Walesu zákon o polícii a dôkazoch v trestných veciach z roku 1984 (PACE), k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1984/60/contents [v znení Zákona o ochrane slobôd z roku 2012 (PoFA)], k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2012/9/contents a zákon o vyšetrovacích právomociach z roku 2016 (IPA), k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2016/25/contents, ii) v prípade Škótska, zákon o trestnej justícii (Škótsko) z roku 2016, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/asp/2016/1/contents a trestný poriadok (Škótsko) z roku 1995, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/1995/46/contents a iii) v prípade Severného Írska, nariadenie o polícii a trestných dôkazoch (Severné Írsko) z roku 1989, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Orgány Spojeného kráľovstva vysvetlili, že nadradenosť štatutárneho práva je v Spojenom kráľovstve dávno zakotvená, a to už od rozsudku vo veci Entick/Carrington [1765] EWHC KB J98, v ktorom sa uznalo, že výkon právomocí výkonnej moci je obmedzený a stanovila sa zásada, že právomoci podľa common law a právomoci vyplývajúce z výsad monarchu a vlády sú podriadené právu krajiny.

([51]) Pozri vec Rice/Connolly [1966] 2 QB 414.

([52]) Pozri vec R(Catt)/Association of Chief police Officers [2015] AC 1065, kde sudca Lord Sumption vo vzťahu k právomoci polície získavať a uchovávať informácie o osobe (ktorá spáchala trestný čin) rozhodol, že podľa common law má polícia právomoc získavať a uchovávať informácie na policajné účely, t. j. vo všeobecnosti na zachovanie verejného poriadku a predchádzanie trestnej činnosti a jej odhaľovanie. Týmito právomocami nie sú umožnené rušivé spôsoby získavania informácií, ako napríklad vstup na súkromný majetok alebo konanie (iné ako zatknutie podľa common law), ktoré by predstavovali zásah do práv. Sudca vyjadril názor, že v predmetnej veci boli právomoci podľa common law dostatočne široké, aby umožňovali získanie a uchovávanie verejných informácií, o ktoré išlo v odvolaniach, ktoré boli predmetom konania.

([53]) Zákon o rovnosti z roku 2010, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Príkladom veci, v ktorej sa policajné právomoci vyplývajúce z common law posudzujú v rámci zákona o ochrane údajov z roku 1998, je rozhodnutie Vrchného súdu (High Court) vo veci Bridges/Chief Constable of South Wales Police (pozri poznámku pod čiarou č. 33). Pozri aj veci Vidal-Hall/Google Inc [2015] EWCA Civ 311 a Richard/BBC [2018] EWHC 1837 (Ch).

([55]) Pozri napríklad usmernenie Policajného zboru Severného Írska o pokynoch na správu záznamov, k dispozícii na tomto odkaze: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Dolná snemovňa Spojeného kráľovstva uverejnila informačný dokument, v ktorom sa uvádzajú kľúčové právomoci podľa common law a zákonné právomoci polície v Anglicku a Walese (pozri https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Kým podľa tohto dokumentu napr. právomoc udržiavať „pokoj koruny“, ako aj právo na „použitie sily“, sú založené na common law, „právomoc zastaviť a prehľadávať“ sa vždy opiera o zákonný základ. Škótska vláda okrem toho na svojej webovej stránke poskytuje informácie o policajných právomociach v oblasti zatýkania a zadržania na účely prehliadky (pozri https://www.gov.scot/policies/police/police-powers/).

([57]) Podľa informácií, ktoré poskytli orgány Spojeného kráľovstva, medzi výsadné právomoci, ktoré vykonáva vláda, patrí napríklad uzatváranie a ratifikácia zmlúv, diplomatická činnosť, využívanie ozbrojených síl v Spojenom kráľovstve na udržanie mieru v rámci podpory polície.

a tretími krajinami na účely presadzovania práva, pričom právomoc vymieňať si údaje týmto spôsobom nie je vždy stanovená v zákone ([58]). Kráľovské výsady sú viazané zásadami common law ([59]) a sú podriadené právnym predpisom, a preto podliehajú obmedzeniam stanoveným v zákone o ľudských právach z roku 1998 a zákone o ochrane údajov z roku 2018 ([60]).

(33) Podobne ako v článku 8 smernice (EÚ) 2016/680 sa aj podľa režimu uplatňovaného v Spojenom kráľovstve vyžaduje, aby príslušné orgány v záujme dodržania zásady zákonnosti zabezpečili, že ak je spracúvanie založené na práve, zároveň musí byť „nevyhnutné“ na plnenie úlohy vykonávanej na účely presadzovania práva. Komisár pre informácie v tejto súvislosti poskytuje usmernenie objasňujúce, že musí ísť o cielený a primeraný spôsob dosiahnutia tohto cieľa. Zákonný základ sa neuplatní, ak môžete primerane dosiahnuť tento účel inými, menej rušivými prostriedkami. Nestačí tvrdiť, že spracovanie je nevyhnutné, pretože ste sa rozhodli vykonávať svoju činnosť určitým spôsobom. Otázkou je, či je spracúvanie nutné na uvedený účel ([61]).

2.4.1.2. Spracúvanie na základe súhlasu dotknutej osoby

(34) Ako sa uvádza v odôvodnení (28), v § 35 ods. 2 zákona o ochrane údajov z roku 2018 sa stanovuje možnosť spracúvať osobné údaje na základe súhlasu fyzickej osoby.

(35) Zdá sa však, že súhlas nie je právnym základom relevantným pre operácie spracúvania, ktoré patria do rozsahu pôsobnosti tohto rozhodnutia. Spracovateľské operácie, ktoré sú predmetom tohto rozhodnutia, sa v skutočnosti vždy budú týkať údajov, ktoré príslušný orgán členského štátu preniesol príslušnému orgánu Spojeného kráľovstva podľa smernice (EÚ) 2016/680. Preto zvyčajne nebudú zahŕňať druh priamej interakcie (získavania) medzi orgánom verejnej moci a dotknutými osobami, ktorý môže byť založený na súhlase podľa § 35 ods. 2 písm. a) zákona o ochrane údajov z roku 2018.

(36) Hoci pre vykonanie posúdenia podľa tohto rozhodnutia sa využitie takéhoto súhlasu nepovažuje za relevantné, v záujme úplnosti je potrebné poznamenať, že v kontexte presadzovania práva sa spracúvanie nikdy nezakladá výlučne na súhlase, keďže príslušný orgán musí mať vždy základnú právomoc, ktorá mu umožňuje spracúvať údaje ([62]). Konkrétnejšie a podobne tomu, čo je umožnené v smernici (EÚ) 2016/680 ([63]), to znamená, že súhlas slúži ako dodatočná podmienka na umožnenie určitých obmedzených a špecifických spracovateľských operácií, ktoré by sa inak nemohli vykonať, ako je napr. odber a spracovanie vzorky DNA osoby, ktorá nie je podozrivá. V takom prípade by sa spracovanie nevykonalo, ak sa súhlas neudelí alebo sa odvolá ([64]).

([58]) V tejto súvislosti pozri posúdenie režimu Spojeného kráľovstva uplatňovaného na následný prenos, ktoré je obsiahnuté v odôvodneniach (74) – (87).

([59]) Pozri vec Bancoult/Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, v ktorej súdy rozhodli, že právomoc vyplývajúca z výsad, na základe ktorej je možné prijímať predpisy v mene monarchu Orders in Council, takisto podlieha všeobecným dôvodom súdneho preskúmania.

([60]) Pozri vec Attorney-General/De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, v ktorej súd rozhodol, že právomoci vyplývajúce z výsad nemožno uplatniť v prípade, ak namiesto nich boli stanovené právomoci zákonom, vec Laker Airways Ltd/Department of Trade 1977] QB 643,] v ktorej súd rozhodol, že právomoci vyplývajúce z výsad nemožno využiť na marenie práva vyplývajúceho zo zákonov, vec R/Secretary of State for the Home Department, ex s. Fire Brigades Union [1995] UKHL 3, kde súd rozhodol, že právomoci vyplývajúce z výsad nemožno uplatniť, ak sú v rozpore s prijatými právnymi predpismi, a to aj vtedy, ak tieto prijaté právne predpisy ešte nenadobudli účinnosť, vec R (Miller)/Secretary of State for Exiting the European Union [2017] UKSC 5, v ktorej súd potvrdil, že je možné, aby sa v rámci práva stanovovaného zákonmi upravovali alebo rušili právomoci vyplývajúce z výsad. Všeobecný prehľad vzťahu medzi právomocami vyplývajúcimi z kráľovských výsad a právomocami vyplývajúcimi z prijatých zákonov, resp. z common law, sa nachádza v informačnom dokumente Dolnej snemovne Spojeného kráľovstva, k dispozícii na tomto odkaze: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Čo je obsahom prvej zásady?“, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Uvedené vyplýva z príslušných ustanovení zákona o ochrane údajov z roku 2018, v zmysle ktorých je spracúvanie osobných údajov na ktorýkoľvek z účelov presadzovania práva zákonné len vtedy a v takom rozsahu, pokiaľ je založené na zákone a a) dotknutá osoba vyjadrila súhlas so spracúvaním na tento účel, alebo b) ak je spracúvanie nevyhnutné na splnenie úlohy, ktorú na tento účel vykonáva príslušný orgán.

([63]) Pozri odôvodnenia 35 a 37 smernice (EÚ) 2016/680.

([64]) Orgány Spojeného kráľovstva vysvetlili, že jedným z príkladov, kedy by súhlas mohol byť vhodným základom pre spracovanie, by bol príklad, keď polícia získa vzorku DNA v súvislosti s nezvestnou osobou, aby ju mohla porovnať s telom, v prípade, že bude nájdené. Za takýchto okolností by nebolo vhodné, aby polícia nútila dotknutú osobu, aby poskytla vzorku; namiesto toho môže polícia požiadať o slobodný súhlas jednotlivca, pričom tento súhlas možno kedykoľvek odvolať. Ak sa súhlas odvolá, údaje už nie je možné spracúvať, pokiaľ nebol stanovený nový právny základ na ďalšie spracovanie vzorky (napr. dotknutá osoba sa stala podozrivou osobou). Ďalší príklad by mohol nastať vtedy, keď policajná zložka vyšetruje trestný čin, pri ktorom by obeť (môže ísť o obeť lúpeže, sexuálneho trestného činu, domáceho násilia, príbuzných zavraždeného alebo o inú obeť trestného činu) mohla byť zaradená do programu organizácie Victim Suport na podporu obetí (ide o nezávislú charitatívnu organizáciu na podporu ľudí postihnutých trestnou činnosťou a traumatickými incidentmi). Za takýchto okolností polícia poskytne tejto organizácii osobné informácie, ako je meno a kontaktné údaje, len vtedy, ak má súhlas obete.

(37) V prípadoch, ktoré si vyžadujú súhlas jednotlivca, musí byť takýto súhlas jednoznačný a musí zahŕňať jasný potvrdzujúci úkon ([65]). Policajné zložky sú povinné disponovať oznámením o ochrane osobných údajov, kde sa okrem iného uvádzajú informácie o platnom využití súhlasu. Okrem toho niektoré policajné zložky uverejňujú dodatočné materiály o tom, ako dodržiavajú právne predpisy o ochrane údajov, vrátane toho, ako a kedy použijú súhlas ako právny základ ([66]).

2.4.1.3. Citlivé spracovanie

(38) Na spracúvanie „osobitných kategórií" údajov by sa mali vzťahovať osobitné záruky. V tejto súvislosti sa podobne ako v článku 10 smernice (EÚ) 2016/680 stanovujú v časti 3 zákona o ochrane údajov z roku 2018 silnejšie záruky pre takzvané „citlivé spracovanie" ([67]).

(39) Podľa § 35 ods. 3 zákona o ochrane údajov z roku 1998 môžu príslušné orgány spracúvať citlivé údaje na účely presadzovania práva len v dvoch prípadoch: 1. ak dotknutá osoba vyjadrila súhlas so spracúvaním na účely presadzovania práva a v čase, keď sa spracúvanie uskutočňuje, uplatňuje prevádzkovateľ riadny dokument stanovujúci politiku spracúvania ([68]), alebo 2. ak je spracovanie nevyhnutne potrebné na účely presadzovania práva, spĺňa aspoň jednu z podmienok uvedených v prílohe 8 k zákonu o ochrane údajov z roku 2018 a v čase, keď sa spracúvanie uskutočňuje, uplatňuje prevádzkovateľ riadny dokument stanovujúci politiku spracúvania ([69]).

(40) Pokiaľ ide o prvý prípad a ako je vysvetlené v odôvodnení 38, využitie súhlasu sa pri type prenosu, na ktorý sa vzťahuje toto rozhodnutie, nepovažuje za relevantné ([70]).

(41) Ak sa spracúvanie citlivých údajov neopiera o súhlas, môže sa vykonať na základe jednej z podmienok uvedených v prílohe 8 k zákonu o ochrane údajov z roku 2018. Tieto podmienky sa týkajú spracúvania potrebného na zákonné účely, výkon spravodlivosti, ochranu zásadných záujmov dotknutej osoby či iného jednotlivca, ochranu detí a osôb vystavených riziku, právne nároky, súdne akty, predchádzanie podvodom, archiváciu, v prípadoch, keď ide o osobné údaje, ktoré dotknutá osoba preukázateľne zverejnila. Okrem prípadu, keď sú údaje zjavne zverejnené, podliehajú všetky podmienky stanovené v prílohe 8 k testu, že spracúvanie musí byť „nevyhnutne potrebné". Ako

([65]) Neexistuje žiadne samostatné vymedzenie pojmu „súhlas" na účely spracúvania osobných údajov podľa časti 3 zákona o ochrane údajov z roku 2018. Komisár pre informácie poskytol usmernenie k pojmu „súhlas" podľa časti 3 zákona o ochrane údajov z roku 2018, v ktorom sa objasňuje, že tento pojem má rovnaký význam ako vo všeobecnom nariadení o ochrane údajov a mal by sa s ním zosúladiť, čiže konkrétne, že súhlas musí byť slobodne daný, konkrétny a informovaný a musí existovať skutočná možnosť zvoliť si súhlas so spracovaním údajov [Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Čo je obsahom prvej zásady?", (pozri poznámku pod čiarou č. 64) a Príručka o ochrane údajov a súhlase, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/].

([66]) Pozri napríklad informácie na webovej stránke polície Lincolnshire (pozri https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) alebo na webovej stránke West Yorkshire Police (pozri https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) § 35 ods. 8 zákona o ochrane údajov z roku 2018.

([68]) § 35 ods. 4 zákona o ochrane údajov z roku 2018.

([69]) § 35 ods. 5 zákona o ochrane údajov z roku 2018.

([70]) Pre úplnosť treba poznamenať, že ak sa spracúvanie zakladá na súhlase, musí byť slobodne daný, konkrétny a informovaný a musí existovať skutočná možnosť zvoliť si súhlas so spracovaním údajov. Okrem toho sa od prevádzkovateľa vyžaduje, aby pri spracúvaní na základe súhlasu dotknutej osoby mal k dispozícii riadny dokument stanovujúci politiku spracúvania. V § 42 zákona o ochrane údajov z roku 2018 sa uvádzajú požiadavky, ktoré musí riadny dokument stanovujúci politiku spracúvania spĺňať. Objasňuje sa v ňom, že dokument musí prinajmenšom vysvetliť postupy prevádzkovateľa na zabezpečenie dodržiavania zásad ochrany údajov a ozrejmiť politiky prevádzkovateľa týkajúce sa uchovávania a vymazania osobných údajov. Podľa § 42 zákona o ochrane údajov z roku 2018 to znamená, že prevádzkovateľ musí predložiť dokument, ktorý a) vysvetľuje postupy prevádzkovateľa na zabezpečenie dodržiavania zásad ochrany údajov a b) ozrejmuje politiky prevádzkovateľa týkajúce sa uchovávania a vymazania osobných údajov spracúvaných na základe súhlasu dotknutej osoby, resp. v ktorom sa uvádza, ako dlho sa takéto osobné údaje budú pravdepodobne uchovávať. V takomto dokumente stanovujúcom politiku spracúvania musí byť stanovené, že prevádzkovateľ v rámci dodržiavania svojej povinnosti zaznamenávať spracovateľské činnosti musí vždy zahrnúť prvky uvedené v písmenách a) a b). Komisár pre informácie uverejnil vzorový dokument (Usmernenie k spracúvaniu údajov na účely presadzovania práva. „Podmienky citlivého spracovania", k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) a môže podniknúť kroky na zabezpečenie dodržiavania v prípade, že prevádzkovatelia nesplnia uvedené požiadavky. Z pohľadu možných porušení zákona o ochrane údajov z roku 2018 môžu riadny dokument stanovujúci politiku spracúvania preskúmavať aj súdy. Napríklad v nedávnom prípade R (Bridges)/Chief Constable of South Wales Police súdy preskúmali riadny dokument prevádzkovateľa stanovujúci politiku spracúvania a zistili, že je vyhovujúci, avšak že by bolo prínosom, ak by obsahoval viac podrobnosti. V dôsledku toho polícia Južného Walesu preskúmala svoj riadny dokument stanovujúci politiku spracúvania a aktualizovala ho v súlade s novým usmernením Komisára pre informácie (pozri poznámku pod čiarou č. 33). Okrem toho by prevádzkovateľ mal podľa § 42 ods. 3 zákona o ochrane údajov z roku 2018 svoj riadny dokument stanovujúci politiku spracúvania pravidelne preskúmavať. Dodatočnou zárukou napokon je, že podľa § 42 ods. 4 zákona o ochrane údajov z roku 2018 je prevádzkovateľ povinný viesť rozšírený záznam o spracovateľských činnostiach, ktorý obsahuje dodatočné prvky v porovnaní so všeobecnou povinnosťou prevádzkovateľa viesť záznamy o spracovateľských činnostiach stanovenou v § 61 zákona o ochrane údajov z roku 2018.

ozrejmil Komisár pre informácie, „nevyhnutne potrebné“ v tejto súvislosti znamená, že spracúvanie musí súvisieť s naliehavou spoločenskou potrebou, ktorú nie je možné primerane uspokojiť menej rušivými prostriedkami ([71]). Okrem toho niektoré z týchto podmienok podliehajú dodatočným obmedzeniam. Napríklad na využitie podmienky „zákonných účelov“ a „podmienky ochrany“ (príloha 8, odsek 1 a odsek 4) je potrebné splniť dodatočné kritérium podstatného verejného záujmu. Okrem toho, pokiaľ ide o podmienky týkajúce sa ochrany dieťaťa (príloha 8, odsek 4), dotknutou osobou musí byť zároveň osoba určitého veku a musí sa považovať za ohrozenú osobu. Prevádzkovateľ môže navyše uplatniť podmienku stanovenú v odseku 4 prílohy 8 len v prípade osobitných okolností ([72]). Podobne existujú obmedzenia pre podmienky týkajúce sa „súdnych aktov“ a „predchádzania podvodom“ (príloha 8, odsek 7 a 8). Obe sa vzťahujú len na konkrétnych prevádzkovateľov. V prípade súdnych aktov môže takúto podmienku použiť len súd alebo iný súdny orgán a v prípade predchádzania podvodom sa o túto podmienku môžu oprieť len prevádzkovatelia, ktorí sú organizáciami na boj proti podvodom.

(42) Napokon, ak sa spracúvanie opiera o jednu z podmienok uvedených v prílohe 8 a podľa § 42 ods. 4 zákona o ochrane údajov z roku 2018, musí sa uplatňovať „riadny dokument stanovujúci politiku spracúvania“, v ktorom sa vysvetlia postupy prevádzkovateľa na zabezpečenie dodržiavania zásad ochrany údajov a politiky prevádzkovateľa, pokiaľ ide o uchovávanie a vymazanie osobných údajov, pričom sa uplatňuje povinnosť viesť rozšírený záznam.

2.4.2. *Obmedzenie účelu*

(43) Osobné údaje by sa mali spracúvať na konkrétny účel a následne by sa mali používať len pokiaľ to nie je nezlučiteľné s daným účelom spracúvania. Túto zásadu ochrany údajov zaručuje § 36 zákona o ochrane údajov z roku 2018. V tomto ustanovení sa podobne ako v článku 4 ods. 1 písm. b) smernice (EÚ) 2016/680 vyžaduje, aby a) účel presadzovania práva, na ktorý sa osobné údaje zhromažďujú pri akejkoľvek príležitosti, bol konkrétne určený, výslovne uvedený a legitímny a že b) takto získané osobné údaje sa nesmú spracúvať spôsobom, ktorý nie je zlučiteľný s účelom, na ktorý boli získané.

(44) Ak príslušné orgány spracúvajú údaje na účely presadzovania práva, môže to zahŕňať archiváciu, vedecký alebo historický výskum a štatistické účely ([73]). V týchto prípadoch sa v zákone o ochrane údajov z roku 2018 takisto objasňuje, že archivácia (alebo spracúvanie na účely vedeckého alebo historického výskumu a štatistiky) nie je povolená, ak sa vykonáva v súvislosti s rozhodnutiami prijatými vo vzťahu s konkrétnou dotknutou osobou alebo ak je pravdepodobné, že jej spôsobí značnú škodu alebo ťažkosti ([74]).

2.4.3. *Správnosť a minimalizácia údajov*

(45) Údaje musia byť správne a podľa potreby aktualizované. Zároveň by mali byť primerané, relevantné a nie nadmerné vzhľadom na účely, na ktoré sa spracúvajú. Podobne ako v článku 4 ods. 1 písm. c), d) a e) smernice (EÚ) 2016/680 sú tieto zásady zabezpečené v § 37 a § 38 zákona o ochrane údajov z roku 2018. Musia sa prijať všetky primerané opatrenia na zabezpečenie toho, aby sa nesprávne ([75]) osobné údaje

([71]) Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Podmienky citlivého spracovania“ (pozri poznámku pod čiarou č. 70).

([72]) Spracovanie sa vykoná bez súhlasu dotknutej osoby, ak: a) dotknutá osoba nemôže vyjadriť súhlas so spracovaním; b) nemožno odôvodnene očakávať, že prevádzkovateľ je schopný získať súhlas dotknutej osoby so spracúvaním; c) spracovanie sa musí vykonať bez súhlasu dotknutej osoby, pretože získaním súhlasu dotknutej osoby by bolo ohrozené poskytnutie ochrany uvedenej v odseku 1 písm. a).

([73]) Pozri § 41 ods. 1 zákona o ochrane údajov z roku 2018.

([74]) Pozri § 41 ods. 2 zákona o ochrane údajov z roku 2018.

([75]) V § 205 zákona o ochrane údajov z roku 2018 sa pojem „nesprávne“ osobné údaje vymedzuje ako „chybné alebo zavádzajúce“ osobné údaje. Podľa vysvetlenia orgánov Spojeného kráľovstva je pre údaje súvisiace s vyšetrovaním trestných činov príznačné, že sú často neúplné, napriek tomu však môžu byť správne.

bezodkladne ([76]) vymazali alebo opravili so zreteľom na účel presadzovania práva, na ktorý sa spracúvajú ([77]), a aby sa zabezpečilo, že osobné údaje, ktoré sú nesprávne, neúplné alebo už nie sú aktuálne, sa neprenášajú ani neposkytujú na žiadne z účelov presadzovania práva ([78]).

(46) Okrem toho sa podobne ako v článku 7 smernice (EÚ) 2016/680 aj v rámci režimu ochrany údajov v Spojenom kráľovstve stanovuje, že osobné údaje založené na skutočnostiach musia byť v čo najväčšej možnej miere rozlíšené od osobných údajov založených na osobných hodnoteniach ([79]). Ak je to relevantné a pokiaľ je to možné, treba jasne rozlišovať medzi osobnými údajmi týkajúcimi sa rôznych kategórií dotknutých osôb, ako sú napr. podozrivé osoby, osoby odsúdené za trestný čin, obete trestného činu a svedkovia ([80]).

2.4.4. *Minimalizácia uchovávania*

(47) Podľa článku 5 smernice (EÚ) 2016/680 by sa údaje v zásade nemali uchovávať dlhšie, ako je potrebné na účely, na ktoré sa osobné údaje spracúvajú. Podľa § 39 zákona o ochrane údajov z roku 2018 a podobne ako v článku 5 uvedenej smernice je zakázané uchovávať osobné údaje spracúvané na ktorýkoľvek z účelov presadzovania práva dlhšie, ako je nevyhnutné v súvislosti s účelom, na ktorý sa spracúvajú. V rámci právneho režimu Spojeného kráľovstva sa vyžaduje, aby sa stanovili primerané lehoty na pravidelné preskúmanie potreby ďalšieho uchovávania osobných údajov na akékoľvek účely presadzovania práva. Ďalšie pravidlá týkajúce sa postupov uchovávania osobných údajov a uplatniteľné lehoty boli stanovené v príslušných právnych predpisoch a usmerneniach upravujúcich právomoci a fungovanie polície. Napríklad v Anglicku a Walese vytvára Kódex praxe správy policajných informácií vypracovaný policajnou akadémiou College of Policing spolu s usmernením o autorizovanej profesijnej praxi správy policajných informácií rámec na zabezpečenie konzistentného procesu uchovávania, preskúmania a likvidácie informácií o operačnej policajnej činnosti založeného na riziku ([81]). Tento rámec stanovuje jasné štandardy v rámci celej služby, pokiaľ ide o spôsob, akým by sa v policajných zložkách a iných agentúrach mali informácie vytvárať, vymieňať, používať a spravovať, ako aj v rámci vzťahov medzi týmito zložkami a agentúrami ([82]). Od polície sa očakáva, že bude dodržiavať kódex praxe a toto dodržiavanie kontroluje inšpekčná služba jej veličenstva pre policajný, hasičský a záchranný zbor (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services) ([83]).

(48) Policajný zbor Severného Írska nie je zo zákona povinný dodržiavať Kódex praxe správy policajných informácií. Rámec Kódexu praxe správy policajných informácií prijatý v roku 2011 je však doplnený o príručku Policajného zboru Severného Írska ([84]), v ktorej sa stanovujú politiky a postupy týkajúce sa spôsobu, akým sa tento Kódex uplatňuje v Severnom Írsku.

([76]) § 38 ods. 1 písm. b) zákona o ochrane údajov z roku 2018.

([77]) Podľa Vysvetľujúceho rámca Spojeného kráľovstva pre diskusiu o primeranosti sa uvedeným zabezpečuje uznanie práv dotknutých osôb, ako aj operačných potrieb orgánov presadzovania práva. Uvedený bod bol dôkladne zvážený vo fázach vypracúvania návrhu zákona o ochrane údajov, pretože môžu existovať osobitné a obmedzené operatívne dôvody, prečo údaje nemožno opraviť. Najpravdepodobnejšie k tomu dôjde v prípade, že sa nesprávne osobné údaje musia uchovávať v ich pôvodnej forme na dôkazné účely (pozri vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel F „Presadzovanie práva", s. 21 (pozri poznámku pod čiarou č. 9).

([78]) § 38 ods. 4 zákona o ochrane údajov z roku 2018. Okrem toho podľa § 38 ods. 5 zákona o ochrane údajov z roku 2018 je nutné pred prenosom alebo sprístupnením osobných údajov overiť kvalitu osobných údajov, ďalej pri každom prenose osobných údajov je nutné poskytnúť informácie potrebné na to, aby mohol príjemca posúdiť stupeň správnosti, úplnosti a spoľahlivosti údajov, ako aj ich aktuálnosť, a ak sa po prenose osobných údajov ukáže, že údaje boli nesprávne alebo že prenos bol nezákonný, príjemca musí byť o tom bezodkladne upovedomený.

([79]) § 38 ods. 2 zákona o ochrane údajov z roku 2018.

([80]) § 38 ods. 3 zákona o ochrane údajov z roku 2018.

([81]) Týmto rámcom sa zabezpečuje konzistentnosť pri uplatňovaní pravidiel uchovávania získaných osobných údajov. Lehota na preskúmanie závisí od trestných činov, ktoré sú rozdelené do 4 skupín: 1. určité záležitosti týkajúce sa ochrany verejnosti, 2. iné sexuálne násilné a závažné trestné činy, 3. všetky ostatné trestné činy a 4. rôzne. Podrobnejšie informácie sú k dispozícii v usmernení o autorizovanej profesijnej praxi správy policajných informácií (pozri poznámku pod čiarou č. 26).

([82]) Podľa informácií, ktoré poskytli orgány Spojeného kráľovstva, sa zásadami Kódexu praxe správy policajných informácií môžu riadiť aj iné organizácie, ak si to želajú, pričom napr. daňové a colné orgány jej veličenstva a Národná kriminálna agentúra dobrovoľne prijali mnohé zásady tohto Kódexu s cieľom zabezpečiť konzistentnosť pri presadzovaní práva. Vo všeobecnosti väčšina organizácií poskytne svojim zamestnancom konkrétnu metodiku a usmernenia, ako v rámci plnenia svojich úloh zaobchádzať s osobnými údajmi, ktoré budú prispôsobené potrebám konkrétnej organizácie. To by malo zvyčajne zahŕňať aj povinnú odbornú prípravu.

([83]) Kódex praxe správy policajných informácií bol vydaný na základe právomocí stanovených v zákone o polícii z roku 1996, ktorý umožňuje akadémii College of Policing vydávať kódexy praxe v súvislosti s účinným vykonávaním policajnej činnosti. Každý kódex praxe vydaný podľa tohto zákona o polícii musí byť odsúhlasený ministrom a predtým, ako sa predloží parlamentu, musí byť prekonzultovaný s Národnou kriminálnou agentúrou. V § 39A ods. 7 zákona o polícii z roku 1996 sa vyžaduje, aby polícia náležite zohľadnila kódexy vydané podľa uvedeného zákona.

([84]) Príručka uplatňovania Kódexu praxe správy policajných informácií zo strany Policajného zboru Severného Írska, kapitoly 1 až 6.

(49) V Škótsku policajné zložky vychádzajú zoštandardného operačný postupu uchovávania záznamov (SOP) ([85]), ktorý je podporený politikou riadenia záznamov škótskej polície ([86]). V tomto štandardnom operačnom postupe sa stanovujú osobitné pravidlá uchovávania záznamov, ktorými disponuje škótska polícia.

(50) Okrem zastrešujúcej požiadavky na preskúmanie záznamov, ktorá sa uplatňuje v celom Spojenom kráľovstve, sa v lokálnych pravidlách uvádzajú ďalšie podrobnosti. Ako príklad možno uviesť, že pokiaľ ide o Anglicko a Wales, zákon o polícii a dôkazoch v trestných veciach zmenený zákonom o ochrane slobody z roku 2012 stanovuje uchovávanie odtlačkov prstov a profilov DNA, ako aj osobitný režim pre osoby, ktoré neboli odsúdené ([87]). Zákonom o ochrane slobody z roku 2012 sa okrem iného vytvorila aj funkcia komisára pre uchovávanie a používanie biometrického materiálu (ďalej len „Komisár pre biometriu“) ([88]). Osobitné pravidlá týkajúce sa podôb tváre vyhotovených pri zadržaní sú stanovené v materiáli o preskúmaní uchovávania týchto podôb tváre z roku 2017 ([89]). Pokiaľ ide o Škótsko, trestný poriadok (Škótsko) z roku 1995 stanovuje pravidlá získavania a uchovávania odtlačkov prstov a biologických vzoriek ([90]). Rovnako ako v prípade Anglicka a Walesu, aj v Škótsku právne predpisy upravujú uchovávanie biometrických údajov v rôznych prípadoch ([91]).

2.4.5. *Bezpečnosť údajov*

(51) Osobné údaje sa musia spracúvať spôsobom, ktorým sa zaistí ich bezpečnosť vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením. Na tento účel orgány verejnej moci prijmú vhodné technické alebo organizačné opatrenia na ochranu osobných údajov pred možnými hrozbami. Tieto opatrenia sa musia posudzovať s prihliadnutím na stav techniky a súvisiace náklady.

(52) Tieto zásady sú premietnuté do § 40 zákona o ochrane údajov z roku 2018, podľa ktorého sa podobne, ako sa stanovuje v článku 4 ods. 1 písm. f) smernice (EÚ) 2016/680, osobné údaje spracúvané na akékoľvek účely presadzovania práva musia spracúvať spôsobom, ktorým sa zabezpečí primeraná bezpečnosť osobných údajov, a to prostredníctvom primeraných technických alebo organizačných opatrení. To zahŕňa ochranu údajov pred

([85]) Štandardný operačný postup uchovávania záznamov (SOP), k dispozícii na tomto odkaze: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Viac informácií o správe záznamov sa uvádza v informačnom materiáli o národných záznamoch Škótska, k dispozícii na tomto odkaze: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Obdobie uchovávania sa líši v závislosti od toho, či osoba bola odsúdená (§ 63I – § 63KI zákona o polícii a dôkazoch v trestných veciach z roku 1984). Napríklad v prípade dospelej osoby odsúdenej za trestný čin zapisovaný do registra trestov sa jej odtlačky prstov a profil DNA môžu uchovávať bez obmedzenia (§ 63I ods. 2 zákona o polícii a dôkazoch v trestných veciach z roku 1984), zatiaľ čo uchovávanie je časovo obmedzené, ak je odsúdená osoba mladšia ako 18 rokov, trestný čin je „menej závažným“ trestným činom zapisovaným do registra trestov a osoba nebola predtým odsúdená (§ 63K zákona o polícii a dôkazoch v trestných veciach z roku 1984). Uchovávanie v prípade zatknutej alebo obvinenej osoby, ktorá nebola odsúdená, je časovo obmedzené na tri roky (§ 63F zákona o polícii a dôkazoch v trestných veciach z roku 1984). Predĺženie tohto obdobia uchovávania musí schváliť súdny orgán (§ 63F ods. 7 zákona o polícii a dôkazoch v trestných veciach z roku 1984). V prípade osôb, ktoré boli zatknuté alebo obvinené, ale neboli odsúdené za menej závažný trestný čin, údaje nie je možné uchovávať (§ 63D a § 63H zákona o polícii a dôkazoch v trestných veciach z roku 1984).

([88]) Funkcia komisára pre biometriu je zriadená § 20 zákona o ochrane slobody z roku 2012. Komisár pre biometriu okrem iného rozhoduje o tom, či polícia môže uchovávať záznamy o profiloch DNA a odtlačky prstov získané od osôb, ktoré boli zatknuté, ale neboli obvinené z kvalifikovaného trestného činu (§ 63G zákona o polícii a dôkazoch v trestných veciach z roku 1984). Tento komisár má okrem toho všeobecnú zodpovednosť za to, aby uchovávanie a používanie DNA a odtlačkov prstov a uchovávanie z dôvodov národnej bezpečnosti boli predmetom preskúmania (§ 20 ods. 2 zákona o ochrane slobody z roku 2012). Komisár pre biometriu sa vymenúva na základe kódexu riadenia verejných menovaní (tento kódex je k dispozícii na tomto odkaze: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) a v podmienkach jeho vymenovania sa jasne stanovuje, že ho z funkcie môže odvolať len minister vnútra, a to len na základe úzko vymedzeného súboru okolností, medzi ktoré patrí neplnenie si povinností počas troch mesiacov, odsúdenie za spáchanie trestného činu alebo neplnenie podmienok jeho vymenovania.

([89]) Review of the Use and Retention of Custody Images (Preskúmanie používania a uchovávania podôb tváre vyhotovených pri zadržaní), k dispozícii na tomto odkaze: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) § 18 a nasl. trestného poriadku (Škótsko) z roku 1995.

([91]) Obdobie uchovávania sa líši podľa toho, či bola osoba odsúdená [§ 18 ods. 3 trestného poriadku (Škótsko) z roku 1995], resp. či je táto osoba neplnoletá. V prípade neplnoletej osoby je obdobie uchovávania tri roky od odsúdenia v konaní s detským účastníkom [§ 18E ods. 8 trestného poriadku (Škótsko) z roku 1995]. Údaje osôb, ktoré boli zatknuté, ale neboli odsúdené, nemožno uchovávať [§ 18 ods. 3 trestného poriadku (Škótsko) z roku 1995], s výnimkou osobitných prípadov a v závislosti od závažnosti trestného činu [§ 18A trestného poriadku (Škótsko) z roku 1995]. Zákon o Škótskom komisárovi pre biometriu z roku 2020 (pozri https://www.legislation.gov.uk/asp/2020/8/contents) vytvára pozíciu škótskeho komisára pre biometriu, ktorý musí vypracovať a revidovať kódexy praxe (schvaľované škótskym parlamentom) týkajúce sa získavania, uchovávania, používania a zničenia biometrických údajov na účely trestnej justície a polície (§ 7 zákona o Škótskom komisárovi pre biometriu z roku 2020).

neoprávneným alebo nezákonným spracúvaním a pred náhodnou stratou, zničením alebo poškodením ([92]). V § 66 zákona o ochrane údajov z roku 2018 sa ďalej uvádza, že každý prevádzkovateľ a každý sprostredkovateľ musí prijať primerané technické a organizačné opatrenia na zaistenie úrovne bezpečnosti primeranej rizikám vyplývajúcim zo spracúvania osobných údajov. Podľa dôvodovej správy musí prevádzkovateľ vyhodnotiť riziká a na základe tohto hodnotenia zaviesť vhodné bezpečnostné opatrenia, napríklad šifrovanie alebo osobitné úrovne bezpečnostnej previerky pre zamestnancov, ktorí spracúvajú údaje ([93]). Pri hodnotení sa musí zohľadniť napríklad povaha spracúvaných údajov a akékoľvek iné relevantné faktory alebo okolnosti, ktoré by mohli ovplyvniť bezpečnosť spracúvania.

(53) Režim, ktorým sa riadi dodržiavanie zásad bezpečnosti údajov, je veľmi podobný režimu stanovenému v článkoch 29 až 31 smernice (EÚ) 2016/680. Prevádzkovateľ je predovšetkým v prípade porušenia ochrany osobných údajov, za ktoré je zodpovedný, povinný podľa § 67 ods. 1 zákona o ochrane údajov z roku 2018 bez zbytočného odkladu a podľa možnosti do 72 hodín od zistenia porušenia oznámiť porušenie ochrany osobných údajov Komisárovi pre informácie ([94]). Oznamovacia povinnosť sa neuplatňuje, ak je nepravdepodobné, že porušenie ochrany osobných údajov povedie k ohrozeniu práv a slobôd fyzických osôb ([95]). Prevádzkovateľ musí zdokumentovať skutočnosti týkajúce sa každého porušenia ochrany osobných údajov, jeho účinkov a prijatých nápravných opatrení spôsobom, ktorý umožní Komisárovi pre informácie overiť súlad so zákonom o ochrane údajov z roku 2018 ([96]). Ak sa sprostredkovateľ dozvie o narušení bezpečnosti, musí to bez zbytočného odkladu oznámiť prevádzkovateľovi ([97]).

(54) Podľa § 68 ods. 1 zákona o ochrane údajov z roku 2018, ak porušenie ochrany osobných údajov pravdepodobne predstavuje vysoké riziko pre práva a slobody fyzických osôb, prevádzkovateľ bez zbytočného odkladu informuje dotknutú osobu o porušení ([98]). Oznámenie musí obsahovať rovnaké informácie ako oznámenie Komisárovi pre informácie opísané v odôvodnení(53). Táto povinnosť neplatí, ak prevádzkovateľ zaviedol primerané technické a organizačné ochranné opatrenia, ktoré sa uplatnili na osobné údaje, ktorých sa porušenie týka. Takisto neplatí, ak prevádzkovateľ prijal následné opatrenia, ktorými sa zabezpečí, že vysoké riziko pre práva a slobody dotknutých osôb pravdepodobne už nebude mať dôsledky. Prevádzkovateľ napokon nie je povinný informovať dotknutú osobu, ak by si to vyžadovalo neprimerané úsilie ([99]). V takom prípade musia byť informácie sprístupnené dotknutej osobe iným rovnako účinným spôsobom, napríklad prostredníctvom verejného prenosu ([100]). Ak prevádzkovateľ neinformoval dotknutú osobu o porušení, Komisár pre informácie môže po tom, ako bol informovaný podľa § 67 zákona o ochrane údajov z roku 2018 a po zvážení toho, či je pravdepodobné, že toto porušenie povedie k vysokému riziku , požiadať prevádzkovateľa, aby ju o porušení informoval ([101]).

([92]) Podľa dôvodovej správy k zákonu o ochrane údajov z roku 2018 (pozri poznámku pod čiarou č. 45) musí prevádzkovateľ najmä: navrhovať a organizovať svoju bezpečnosť tak, aby vyhovovala povahe osobných údajov, ktorými disponuje, a škode, ktorá môže vzniknúť v dôsledku narušenia bezpečnosti; jasne vedieť, kto je v jeho organizácii zodpovedný za zaistenie bezpečnosti informácií; zabezpečiť, aby mal správnu fyzickú a technickú bezpečnosť podporenú spoľahlivými politikami a postupmi a spoľahlivým a dobre vyškoleným personálom a byť pripravený rýchlo a účinne reagovať na akékoľvek narušenie bezpečnosti.

([93]) Bod 221 dôvodovej správy k zákonu o ochrane údajov z roku 2018 (pozri poznámku pod čiarou č. 45).

([94]) V § 67 ods. 4 zákona o ochrane údajov z roku 2018 sa stanovuje, že oznámenie musí obsahovať opis povahy porušenia ochrany osobných údajov (podľa možnosti vrátane kategórií a približného počtu dotknutých osôb a ich kategórií a približného počtu dotknutých záznamov o osobných údajoch), meno a kontaktné údaje kontaktného miesta, opis pravdepodobných dôsledkov porušenia ochrany osobných údajov a opis opatrení, ktoré prevádzkovateľ prijal alebo navrhol prijať na riešenie porušenia ochrany osobných údajov (v prípade potreby vrátane opatrení na zmiernenie jeho možných nepriaznivých účinkov).

([95]) § 67 ods. 2 zákona o ochrane údajov z roku 2018.

([96]) § 67 ods. 6 zákona o ochrane údajov z roku 2018.

([97]) § 67 ods. 9 zákona o ochrane údajov z roku 2018.

([98]) Podľa § 68 ods. 7 zákona o ochrane údajov z roku 2018 môže prevádzkovateľ úplne alebo čiastočne obmedziť poskytovanie informácií dotknutej osobe v takom rozsahu a dovtedy, kým obmedzenie predstavuje vzhľadom na základné práva a oprávnené záujmy dotknutej osoby nevyhnutné a primerané opatrenie s cieľom a) zabrániť mareniu úradného alebo súdneho zisťovania, vyšetrovania alebo konania, b) zabrániť ohrozovaniu predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestných sankcií, c) chrániť verejnú bezpečnosť, d) chrániť národnú bezpečnosť, e) chrániť práva a slobody iných.

([99]) § 68 ods. 3 zákona o ochrane údajov z roku 2018.

([100]) § 68 ods. 5 zákona o ochrane údajov z roku 2018.

([101]) § 68 ods. 6 zákona o ochrane údajov z roku 2018, s výhradou obmedzenia stanoveného v § 68 ods. 8 zákona o ochrane údajov z roku 2018.

2.4.6. *Transparentnosť*

(55) Dotknuté osoby musia byť informované o hlavných znakoch spracúvania ich osobných údajov. Táto zásada ochrany údajov sa odráža v § 44 zákona o ochrane údajov z roku 2018, v ktorom sa podobne ako v článku 13 smernice (EÚ) 2016/680 stanovuje, že prevádzkovateľ má všeobecnú povinnosť sprístupniť dotknutým osobám informácie o spracúvaní ich osobných údajov (či už všeobecným sprístupnením informácií verejnosti alebo akýmkoľvek iným spôsobom) ([102]). Informácie, ktoré sa majú sprístupniť, zahŕňajú a) totožnosť a kontaktné údaje prevádzkovateľa, b) v príslušných prípadoch kontaktné údaje zodpovednej osoby, c) účely, na ktoré prevádzkovateľ spracúva osobné údaje, d) informáciu o existencii práv dotknutých osôb požadovať od prevádzkovateľa prístup k osobným údajom, opravu osobných údajov a vymazanie osobných údajov, resp. obmedzenie ich spracúvania a e) informáciu o existencii práva podať sťažnosť Komisárovi pre informácie a kontaktné údaje komisára ([103]).

(56) Prevádzkovateľ musí zároveň v osobitných prípadoch na účely umožnenia výkonu práv dotknutej osoby podľa zákona o ochrane údajov z roku 2018 (napríklad keď sa spracúvané osobné údaje získali bez vedomia dotknutej osoby) poskytnúť dotknutej osobe informácie o a) právnom základe pre spracúvanie; b) informácie o období uchovávania osobných údajov alebo, ak to nie je možné, o kritériách na určenie tohto obdobia; c) prípadne informácie o kategóriách príjemcov osobných údajov (vrátane príjemcov v tretích krajinách alebo medzinárodných organizáciách); d) ďalšie informácie, ktoré sú potrebné na uplatnenie práv dotknutej osoby podľa časti 3 zákona o ochrane údajov z roku 2018 ([104]).

2.4.7. *Individuálne práva*

(57) Dotknutým osobám sa musí poskytnúť niekoľko vymáhateľných práv. V časti 3 kapitoly 3 zákona o ochrane údajov z roku 2018 sa fyzickým osobám poskytujú práva na prístup, opravu, vymazanie a obmedzenie ([105]), ktoré sú porovnateľné s právami stanovenými v kapitole 3 smernice (EÚ) 2016/680.

(58) Právo na prístup je stanovené v § 45 zákona o ochrane údajov z roku 2018. Po prvé, jednotlivec má právo získať od prevádzkovateľa potvrdenie, či sa jeho osobné údaje spracúvajú alebo nie ([106]). Po druhé, ak sa osobné údaje spracúvajú, dotknutá osoba má právo na prístup k týmto údajom a na získanie týchto informácií o spracúvaní: a) účely a právne základy spracúvania; b) kategórie dotknutých údajov; c) príjemca, ktorému boli údaje poskytnuté; d) obdobie, počas ktorého sa osobné údaje budú uchovávať; e) existencia práva dotknutej osoby na opravu a vymazanie osobných údajov; f) právo podať sťažnosť a g) akékoľvek informácie o pôvode príslušných osobných údajov ([107]).

(59) Podľa § 46 zákona o ochrane údajov z roku 2018 má dotknutá osoba právo požadovať od prevádzkovateľa opravu nesprávnych osobných údajov, ktoré sa jej týkajú. Prevádzkovateľ musí údaje bez zbytočného odkladu opraviť (resp. v prípade, že sú nesprávne z dôvodu ich neúplnosti, tieto údaje doplniť). Ak sa osobné údaje musia uchovávať na účely dokazovania, prevádzkovateľ musí (namiesto opravy osobných údajov) obmedziť ich spracovanie ([108]).

([102]) V Usmernení k spracúvaniu údajov na účely presadzovania práva sa uvádza tento príklad: „Na svojom webovom sídle máte všeobecné oznámenie o ochrane osobných údajov, ktoré obsahuje základné informácie o organizácii, účele spracúvania osobných údajov, právach dotknutej osoby a jej práve podať sťažnosť Komisárovi pre informácie. Dostali ste informácie o tom, že osoba bola prítomná v čase spáchania trestného činu. Pri prvom pohovore s touto osobou musíte poskytnúť všeobecné informácie, ako aj ďalšie podporné informácie, aby si mohla uplatniť svoje práva. Informácie o spravodlivom spracovaní, ktoré poskytujete, môžete obmedziť len vtedy, ak by nepriaznivo ovplyvnili vami vedené vyšetrovanie“ [Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Aké informácie by sme mali poskytnúť jednotlivcovi?“, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3].

([103]) V Usmernení k spracúvaniu údajov na účely presadzovania práva sa uvádza, že poskytované informácie o spracovaní osobných údajov musia byť stručné, zrozumiteľné a ľahko dostupné, napísané jasným a jednoduchým jazykom, ktorý je prispôsobený potrebám zraniteľných osôb, ako sú deti, a ich poskytnutie musí byť bezplatné (Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Ako by sme mali poskytnúť tieto informácie?“, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) § 44 ods. 2 zákona o ochrane údajov z roku 2018.

([105]) Podrobná analýza práv dotknutých osôb je uvedená v Usmernení k spracúvaniu údajov na účely presadzovania práva, konkrétne v jej časti venovanej právam jednotlivcov, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) § 45 ods. 1 zákona o ochrane údajov z roku 2018.

([107]) § 45 ods. 2 zákona o ochrane údajov z roku 2018.

([108]) § 46 ods. 4 zákona o ochrane údajov z roku 2018.

(60) V § 47 zákona o ochrane údajov z roku 2018 sa poskytuje fyzickým osobám právo na vymazanie a obmedzenie spracúvania. Prevádzkovateľ musí ([109]) vymazať osobné údaje bez zbytočného odkladu, ak by spracúvanie osobných údajov porušilo niektorú zo zásad ochrany údajov, právne dôvody spracúvania alebo záruky týkajúce sa archivácie a citlivého spracúvania. Prevádzkovateľ musí takisto vymazať údaje, ak má právnu povinnosť tak urobiť. Ak sa osobné údaje musia uchovávať na účely dokazovania, prevádzkovateľ musí (namiesto vymazania osobných údajov) obmedziť ich spracúvanie ([110]). Prevádzkovateľ musí obmedziť spracovanie osobných údajov, ak dotknutá osoba spochybňuje správnosť osobných údajov, ale nie je možné zistiť, či sú tieto údaje správne alebo nie ([111]).

(61) Ak dotknutá osoba požiada o opravu alebo vymazanie osobných údajov alebo obmedzenie ich spracúvania, prevádzkovateľ musí dotknutú osobu písomne informovať o tom, či bola žiadosť schválená, a ak bola zamietnutá, informovať dotknutú osobu o dôvodoch zamietnutia a dostupných prostriedkoch nápravy (právo dotknutej osoby požiadať Komisára pre informácie o preskúmanie, či sa obmedzenie uplatnilo zákonným spôsobom, právo podať sťažnosť Komisárovi pre informácie a právo požiadať súd o príkaz na zabezpečenie súladu) ([112]).

(62) Ak prevádzkovateľ opravuje osobné údaje získané od iného príslušného orgánu, musí to oznámiť druhému orgánu ([113]). Ak prevádzkovateľ opravuje alebo vymazáva osobné údaje alebo obmedzuje spracúvanie osobných údajov, ktoré poskytol, musí to oznámiť príjemcom a príjemcovia musia podobne opraviť alebo vymazať osobné údaje alebo obmedziť spracovanie osobných údajov (pokiaľ za ne nesú zodpovednosť) ([114]).

(63) Okrem toho má dotknutá osoba právo byť bez zbytočného odkladu informovaná prevádzkovateľom o porušení ochrany osobných údajov, ak je pravdepodobné, že to povedie k vysokému riziku pre práva a slobody fyzických osôb ([115]).

(64) V súvislosti so všetkými týmito právami dotknutej osoby a podobne, ako sa stanovuje v článku 12 smernice (EÚ) 2016/680, má prevádzkovateľ povinnosť zabezpečiť, aby sa všetky informácie dotknutej osobe poskytovali v stručnej, zrozumiteľnej a ľahko dostupnej forme ([116]), a ak je to možné, mali by sa poskytovať v rovnakej forme, v akej bola podaná žiadosť ([117]). Prevádzkovateľ musí vyhovieť žiadosti dotknutej osoby bez zbytočného odkladu alebo v každom prípade pred uplynutím lehoty jedného mesiaca od podania žiadosti ([118]). Ak má prevádzkovateľ odôvodnené pochybnosti o totožnosti jednotlivca, môže požiadať o dodatočné informácie a odložiť vybavenie žiadosti dovtedy, kým sa nezistí totožnosť. Prevádzkovateľ môže požadovať primeraný poplatok alebo odmietnuť konať, ak považuje žiadosť za zjavne neopodstatnenú ([119]). Komisár pre informácie poskytol usmernenie o tom, kedy sa žiadosť považuje za zjavne neopodstatnenú alebo neprimeranú a kedy možno požadovať poplatok ([120]).

(65) Okrem toho môže podľa § 53 ods. 4 zákona o ochrane údajov z roku 2018 minister prostredníctvom právnych predpisov stanoviť maximálnu výšku poplatku.

([109]) Dotknutá osoba môže požiadať prevádzkovateľa, aby osobné údaje vymazal alebo obmedzil ich spracúvanie (ale povinnosti prevádzkovateľa vymazať údaje alebo obmedziť ich spracúvanie platia bez ohľadu na to, či sa takáto žiadosť podá).

([110]) § 46 ods. 4 a § 47 ods. 2 zákona o ochrane údajov z roku 2018.

([111]) § 47 ods. 3 zákona o ochrane údajov z roku 2018.

([112]) § 48 ods. 1 zákona o ochrane údajov z roku 2018.

([113]) § 48 ods. 7 zákona o ochrane údajov z roku 2018.

([114]) § 48 ods. 9 zákona o ochrane údajov z roku 2018.

([115]) § 68 zákona o ochrane údajov z roku 2018.

([116]) § 52 ods. 1 zákona o ochrane údajov z roku 2018.

([117]) § 52 ods. 3 zákona o ochrane údajov z roku 2018.

([118]) V § 54 zákona o ochrane údajov z roku 2018 sa vymedzuje pojem „uplatniteľná lehota“, čo znamená obdobie jedného mesiaca alebo dlhšie obdobie, ktoré môže byť uvedené v právnych predpisoch, počnúc príslušným momentom [keď prevádzkovateľ dostane príslušnú žiadosť, keď prevádzkovateľ dostane (prípadné) informácie požadované v súvislosti so žiadosťou podľa § 52 ods. 4 zákona o ochrane údajov z roku 2018, resp. keď je uhradený (prípadný) poplatok účtovaný v súvislosti so žiadosťou podľa § 53 zákona o ochrane údajov z roku 2018].

([119]) § 53 ods. 1 zákona o ochrane údajov z roku 2018.

([120]) Podľa usmernenia Komisára pre informácie môže prevádzkovateľ rozhodnúť o účtovaní poplatku dotknutej osobe v prípade, že je jej žiadosť zjavne neopodstatnená alebo neprimeraná, ale aj tak sa na ňu rozhodne odpovedať. Poplatok musí byť primeraný a musí byť dôvodný vzhľadom na náklady. Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Zjavne neopodstatnené a neprimerané žiadosti“, k dispozícii na tomto odkaze: 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. Obmedzenia práv dotknutej osoby a povinnosti týkajúce sa transparentnosti

(66) Príslušný orgán môže za určitých okolností obmedziť určité práva dotknutej osoby: právo na prístup k informáciám ([121]), právo byť informovaný ([122]), právo byť informovaný o porušení ochrany osobných údajov ([123]) a právo byť informovaný o dôvode zamietnutia žiadosti o opravu alebo vymazanie ([124]). Podobne ako v prípade režimu uvedeného v kapitole III smernice (EÚ) 2016/680 môže príslušný orgán uplatniť obmedzenie len vtedy, ak je toto obmedzenie vzhľadom na základné práva a oprávnené záujmy dotknutej osoby nevyhnutné a primerané s cieľom: a) zabrániť mareniu úradného alebo súdneho zisťovania, vyšetrovania alebo konania; b) zabrániť ohrozovaniu predchádzania trestným činom, ich vyšetrovania, odhaľovania alebo stíhania alebo výkonu trestných sankcií, c) chrániť verejnú bezpečnosť, d) chrániť národnú bezpečnosť, e) chrániť práva a slobody iných.

(67) Komisár pre informácie poskytol usmernenie týkajúce sa uplatňovania týchto obmedzení. Podľa tohto usmernenia musia prevádzkovatelia vykonať analýzu jednotlivých prípadov s cieľom vyvážiť práva jednotlivca a škodu, ktorú by spôsobilo poskytnutie údajov. Predovšetkým musia odôvodniť akékoľvek obmedzenie, ktoré sa uplatňuje ako nevyhnutné a primerané, a môžu obmedziť to, čo sa poskytuje, len ak by to ohrozilo vyššie uvedené účely ([125]).

(68) Existuje aj niekoľko ďalších usmernení vydaných príslušnými orgánmi, ktoré poskytujú podrobné informácie o všetkých aspektoch právnych predpisov o ochrane údajov vrátane uplatňovania obmedzení práv dotknutých osôb ([126]). Napríklad v súvislosti s § 45 ods. 4 sa v Príručke na ochranu údajov Národnej rady policajných riaditeľov uvádza: „Je dôležité poznamenať, že obmedzenia sa môžu uplatňovať len v nevyhnutnom rozsahu a môžu sa uplatňovať len tak dlho, ako je to potrebné. V dôsledku toho nie je povolené paušálne uplatňovanie obmedzenia na všetky osobné údaje žiadateľa ani trvalé uplatňovanie obmedzenia. Pokiaľ ide o druhý bod, často platí, že osobné údaje získané bez vedomia dotknutej osoby, ktorá je podozrivá v rámci vyšetrovania, musia byť spočiatku chránené pred ich sprístupnením tejto podozrivej osobe, aby sa predišlo ohrozeniu vyšetrovania počas jeho realizácie, avšak v neskoršom momente by ich poskytnutím nemalo dôjsť k ujme, ak sa tieto osobné údaje jednotlivcovi poskytnú počas vypočúvania. Policajné zložky musia prijať postupy, ktoré zabezpečia uplatňovanie týchto obmedzení len v požadovanom rozsahu a len na nevyhnutné obdobie“ ([127]). V tomto usmernení sa uvádzajú aj príklady, kedy sa príslušné obmedzenie pravdepodobne uplatní ([128]).

(69) Okrem toho, pokiaľ ide o možnosť obmedziť akékoľvek z uvedených práv v záujme ochrany „národnej bezpečnosti“, prevádzkovateľ môže požiadať o osvedčenie podpísané ministrom vlády alebo generálnym prokurátorom (resp. generálnym advokátom pre Škótsko), v ktorom sa potvrdzuje, že obmedzenie takýchto práv je nevyhnutným a primeraným opatrením na ochranu národnej bezpečnosti ([129]). Vláda Spojeného kráľovstva vydala usmernenie k osvedčeniam o záujme národnej bezpečnosti vydávaným podľa zákona o ochrane údajov z roku 2018, v ktorom sa predovšetkým zdôrazňuje, že akékoľvek obmedzenie práv dotknutých osôb na zaistenie národnej bezpečnosti musí byť primerané a nevyhnutné ([130]) (ďalšie informácie o osvedčeniach o záujme národnej bezpečnosti pozri v odôvodneniach 131 až 134).

([121]) § 45 ods. 4 zákona o ochrane údajov z roku 2018.
([122]) § 44 ods. 4 zákona o ochrane údajov z roku 2018.
([123]) § 68 ods. 7 zákona o ochrane údajov z roku 2018.
([124]) § 48 ods. 3 zákona o ochrane údajov z roku 2018.
([125]) Pozri napríklad Usmernenie k spracúvaniu údajov na účely presadzovania práva, konkrétne jeho časť venovanú právu na prístup, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Pozri napríklad Príručku o ochrane údajov pre odborníkov polície pracujúcich v oblasti ochrany údajov, ktorú vydala Národná rada policajných riaditeľov (pozri poznámku pod čiarou č. 27), alebo usmernenie poskytnuté Úradom pre závažné podvody, k dispozícii na tomto odkaze: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Príručka o ochrane údajov, ktorú vydala Národná rada policajných riaditeľov, strana 140 (pozri poznámku pod čiarou č. 27).
([128]) V Príručke o ochrane údajov, ktorú vydala Národná rada policajných riaditeľov, sa stanovuje, že „zabránenie mareniu úradného alebo právneho skúmania, vyšetrovania alebo konania“ bude pravdepodobne relevantné v prípade, že osobné údaje sú spracúvané na účely skúmania, súdneho konania v rodinných veciach, skúmania v rámci interných disciplinárnych konaní iného ako trestno-právneho charakteru a skúmaní ako je napr. nezávislé skúmanie sexuálneho zneužívania detí, zatiaľ čo „ochrana práv a slobôd iných je relevantná pre osobné údaje, ktoré by sa týkali aj ďalších osôb okrem žiadateľa.“ (Príručka o ochrane údajov, ktorú vydala Národná rada policajných riaditeľov, strana 140, pozri poznámku pod čiarou č. 27).
([129]) § 79 zákona o ochrane údajov z roku 2018.
([130]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Okrem toho, ak sa uplatňuje obmedzenie práva dotknutej osoby, príslušný orgán ju musí bez zbytočného odkladu informovať o tom, že jej práva boli obmedzené, o dôvodoch obmedzenia a o dostupných možnostiach nápravy, okrem prípadov, keď by poskytnutie týchto informácií ohrozilo dôvod na uplatnenie obmedzenia ([131]). V záujme ďalšej ochrany pred zneužitím obmedzení musí prevádzkovateľ zaznamenať dôvody obmedzenia práva na informácie a na požiadanie ho sprístupniť Komisárovi pre informácie ([132]).

(71) Ak prevádzkovateľ odmietne poskytnúť dodatočné informácie v záujme transparentnosti, resp. prístup, alebo zamietne žiadosť o opravu, vymazanie alebo obmedzenie spracúvania, jednotlivec môže požiadať Komisára pre informácie, aby preskúmal, či prevádzkovateľ využil obmedzenie zákonne ([133]). Tento jednotlivec môže Komisárovi pre informácie podať sťažnosť, alebo požiadať súd, aby prevádzkovateľovi nariadil vyhovieť žiadosti ([134]).

2.4.7.2. Automatizované rozhodovanie

(72) Ustanovenia § 49 a § 50 zákona o ochrane údajov z roku 2018 upravujú práva súvisiace s automatizovaným rozhodovaním a záruky, ktoré sa majú uplatňovať ([135]). Podobne ako v článku 11 smernice (EÚ) 2016/680 sa ustanovuje, že prevádzkovateľ môže prijať významné rozhodnutie výlučne na základe automatizovaného spracovania osobných údajov len vtedy, ak ho vyžaduje alebo povoľuje zákon ([136]). Rozhodnutie je významné, ak by malo nepriaznivý právny účinok na dotknutú osobu alebo ak by ju významne ovplyvnilo ([137]).

(73) Ak je prevádzkovateľ podľa zákona povinný alebo oprávnený prijať významné rozhodnutie, v § 50 zákona o ochrane údajov z roku 2018 sa stanovujú záruky, ktoré sa budú uplatňovať na takéto rozhodnutie (ktoré sa vymedzuje ako „kvalifikované významné rozhodnutie“). Prevádzkovateľ musí prijatie takéhoto rozhodnutia čo najskôr oznámiť dotknutej osobe. Dotknutá osoba môže potom do jedného mesiaca požiadať prevádzkovateľa, aby prehodnotil rozhodnutie alebo aby prijal nové rozhodnutie, ktoré nie je založené výlučne na automatizovanom spracovaní. Prevádzkovateľ musí žiadosť posúdiť a informovať dotknutú osobu o výsledku tohto posúdenia. Zákon o ochrane údajov z roku 2018 udeľuje ministrovi právomoc prijať právne predpisy o dodatočných zárukách ([138]). Zatiaľ neboli prijaté žiadne takéto právne predpisy.

2.4.8. *Následné prenosy*

(74) Úroveň ochrany osobných údajov prenášaných orgánom presadzovania práva členského štátu orgánu presadzovania práva Spojeného kráľovstva nesmie byť oslabená ďalším prenosom takýchto údajov príjemcom v tretej krajine. Takéto „následné prenosy“, ktoré z hľadiska orgánu presadzovania práva Spojeného kráľovstva predstavujú medzinárodné prenosy zo Spojeného kráľovstva, by sa mali povoliť len v prípade, že ďalší príjemca mimo Spojeného kráľovstva takisto podlieha pravidlám zabezpečujúcim podobnú úroveň ochrany, aká je zaručená v právnom poriadku Spojeného kráľovstva.

([131]) § 44 ods. 5 a 6, § 45 ods. 5 a 6, a § 48 ods. 4 zákona o ochrane údajov z roku 2018.
([132]) § 44 ods. 7, § 45 ods. 7 a § 48 ods. 6 zákona o ochrane údajov z roku 2018.
([133]) § 51 zákona o ochrane údajov z roku 2018.
([134]) § 167 zákona o ochrane údajov z roku 2018.
([135]) Pokiaľ ide o rozsah automatizovaného spracúvania, v dôvodovej správe k zákonu o ochrane údajov z roku 2018 sa uvádza, že: „tieto ustanovenia sa týkajú plne automatizovaného rozhodovania, a nie automatizovaného spracúvania. K automatizovanému spracovaniu (vrátane profilovania) dochádza vtedy, keď sa operácia vykonáva na údajoch bez toho, aby bol potrebný ľudský zásah. Pravidelne sa používa pri presadzovaní práva, aby sa z veľkých súborov údajov vyfiltrovali zvládnuteľné množstvá, ktoré môže následne ľudský operátor použiť. Automatizované rozhodovanie je formou automatizovaného spracúvania a vyžaduje si, aby sa konečné rozhodnutie prijímalo bez ľudského zásahu“. (Dôvodová správa k zákonu o ochrane údajov z roku 2018, bod 204, pozri poznámku pod čiarou č. 45).
([136]) Popri ochrane stanovenej v zákone o ochrane údajov platia v právnom rámci Spojeného kráľovstva aj iné legislatívne obmedzenia, ktoré sa vzťahujú na orgány presadzovania práv a ktoré bránia automatizovanému spracovaniu (vrátane profilovania), ktoré by mohlo viesť k nezákonnej diskriminácii. Zákonom o ľudských právach z roku 1998 sa do právneho poriadku Spojeného kráľovstva začleňujú práva vyplývajúce z EDĽP, a to aj práva podľa článku 14 EDĽP, čiže zákaz diskriminácie. Podobne sa v Zákone o rovnosti z roku 2010 stanovuje zákaz diskriminácie ľudí s chránenými charakteristikami (čo zahŕňa pohlavie, rasu, zdravotného postihnutie atď.).
([137]) § 49 ods. 2 zákona o ochrane údajov z roku 2018.
([138]) § 50 ods. 4 zákona o ochrane údajov z roku 2018.

(75) Režim Spojeného kráľovstva týkajúci sa medzinárodných prenosov upravuje kapitola 5 časti 3 zákona o ochrane údajov z roku 2018 ([139]) a odráža prístup zaujatý v kapitole V smernice (EÚ) 2016/680. Na prenos osobných údajov do tretej krajiny musí príslušný orgán spĺňať najmä tri podmienky: a) prenos musí byť nevyhnutný na účely presadzovania práva; b) prenos musí byť založený na: i) právnom predpise o primeranosti prijatom v súvislosti s touto treťou krajinou, ii) ak nie je založený na právnom predpise o primeranosti, musia existovať primerané záruky, resp. iii) ak nie je založený na právnom predpise o primeranosti alebo primeraných zárukách, musí byť založený na osobitných okolnostiach a c) príjemca prenosu musí byť: i) príslušný orgán (t. j. orgán rovnocenný príslušnému orgánu) v tretej krajine; ii) „príslušná medzinárodná organizácia“, napr. medzinárodná organizácia, ktorá vykonáva funkcie zodpovedajúce akémukoľvek účelu presadzovania práva, alebo iii) iný subjekt ako príslušný orgán, ale len ak je prenos nevyhnutne potrebný na plnenie niektorého z účelov presadzovania práva, neexistujú žiadne základné práva a slobody dotknutej osoby, ktoré by prevážili nad verejným záujmom, ktorý si vyžaduje prenos, prenos osobných údajov príslušnému orgánu v tretej krajine by bol neúčinný alebo nevhodný a príjemca je informovaný o účeloch, na ktoré sa údaje môžu spracúvať ([140]).

(76) Právne predpisy o primeranosti týkajúce sa tretej krajiny, územia alebo sektora v tretej krajine, medzinárodnej organizácie alebo opis ([141]) takejto krajiny, územia, sektora alebo organizácie prijíma minister. Pokiaľ ide o štandard, ktorý treba dosiahnuť, je na posúdení ministra, či takéto územie, sektor alebo organizácia zabezpečujú primeranú úroveň ochrany osobných údajov. V oddiele 74A ods. 4 zákon o ochrane údajov z roku 2018 sa stanovuje, že minister musí na tento účel zvážiť niekoľko prvkov, ktoré odrážajú prvky uvedené v článku 36 smernice (EÚ) 2016/680 ([142]). V tejto súvislosti treba uviesť, že od skončenia prechodného obdobia predstavuje časť 3 zákona o ochrane údajov z roku 2018 „vnútroštátne právne predpisy odvodené od EÚ“, ktoré, ako už bolo vysvetlené, budú vykladať súdy Spojeného kráľovstva v súlade s príslušnou judikatúrou Súdneho dvora z obdobia pred vystúpením Spojeného kráľovstva z Únie a všeobecnými zásadami práva Únie, keďže mali účinnosť bezprostredne pred skončením prechodného obdobia. To zahŕňa štandard „zásadnej rovnocennosti“, ktorá sa teda bude uplatňovať na posúdenia primeranosti, ktoré vykonávajú orgány Spojeného kráľovstva.

(77) Pokiaľ ide o postup, na právne predpisy sa vzťahujú „všeobecné“ procedurálne požiadavky stanovené v § 182 zákona o ochrane údajov z roku 2018. V rámci tohto postupu musí pri navrhovaní budúcich právnych predpisov Spojeného

([139]) Tento nový rámec začal platiť na konci prechodného obdobia vrátane právomoci ministra prijímať právne predpisy o primeranosti. V právnych predpisoch DPPEC (najmä v odsekoch 10 – 12 prílohy 21, ktoré tieto právne predpisy vkladajú do zákona o ochrane údajov z roku 2018) sa však stanovuje, že s určitými prenosmi osobných údajov na konci prechodného obdobia a po jeho skončení sa zaobchádza tak, ako keby boli založené na právnych predpisoch o primeranosti. Tieto prenosy zahŕňajú prenosy do tretích krajín, na ktoré sa vzťahuje rozhodnutie EÚ o primeranosti na konci prechodného obdobia, a do členských štátov EÚ, štátov EZVO a na územie Gibraltáru na základe toho, že na spracúvanie údajov v oblasti presadzovania práva uplatňujú smernicu o presadzovaní práva [štáty EZVO uplatňujú smernicu (EÚ) 2016/680 v dôsledku svojich povinností podľa schengenského *acquis*]. To znamená, že na konci prechodného obdobia môžu presuny do týchto krajín pokračovať ako pred vystúpením z EÚ. Po skončení prechodného obdobia musí minister do 4 rokov preskúmať zistenia primeranosti.

([140]) § 73 a § 77 zákona o ochrane údajov z roku 2018.

([141]) Orgány Spojeného kráľovstva vysvetlili, že opis krajiny alebo medzinárodnej organizácie sa týka situácie, v ktorej by bolo potrebné vykonať konkrétne a čiastočné určenie primeranosti s cielenými obmedzeniami (napríklad právny predpis o primeranosti len vo vzťahu k určitému typu prenosu údajov).

([142]) Pozri § 74A ods. 4 zákona o ochrane údajov z roku 2018, v ktorom sa stanovuje, že pri posudzovaní primeranosti úrovne ochrany minister musí zohľadniť najmä a) právny štát, dodržiavanie ľudských práv a základných slobôd, príslušné právne predpisy, a to všeobecné aj odvetvové, vrátane predpisov týkajúcich sa verejnej bezpečnosti, obrany, národnej bezpečnosti a trestného práva a prístupu orgánov verejnej moci k osobným údajom, ako aj vykonávanie takýchto právnych predpisov, pravidiel ochrany údajov, profesijných pravidiel a bezpečnostných opatrení vrátane pravidiel pre následný prenos osobných údajov do ďalšej tretej krajiny alebo medzinárodnej organizácii, ktoré sa v danej tretej krajine alebo medzinárodnej organizácii dodržiavajú, judikatúru, ako aj účinné a vymáhateľné práva dotknutej osoby a účinné správne a súdne prostriedky nápravy pre dotknuté osoby, ktorých osobné údaje sa prenášajú; b) existenciu a účinné pôsobenie jedného či viacerých nezávislých dozorných orgánov v predmetnej tretej krajine, alebo ktorému podlieha medzinárodná organizácia, so zodpovednosťou za zabezpečenie a presadzovanie dodržiavania pravidiel ochrany údajov vrátane primeraných právomocí pre presadzovanie práva, za poskytovanie pomoci a poradenstva dotknutým osobám pri výkone ich práv a za spoluprácu s Komisárom a c) medzinárodné záväzky, ktoré dotknutá tretia krajina alebo medzinárodná organizácia prevzala, alebo iné záväzky vyplývajúce z právne záväzných dohovorov alebo nástrojov, ako aj z jej účasti na viacstranných alebo regionálnych systémoch, najmä vo vzťahu k ochrane osobných údajov.

kráľovstva o primeranosti minister konzultovať s Komisárom pre informácie ([143]). Po prijatí ministrom sa tieto právne predpisy predkladajú parlamentu a podliehajú postupu „negatívneho uznesenia“, na základe ktorého môžu obe parlamentné snemovne preskúmať príslušný právny predpis a v rámci 40-dňovej lehoty predložiť návrh na zrušenie príslušného právneho predpisu ([144]).

(78) Podľa § 74B ods. 1 zákona o ochrane údajov z roku 2018 sa právne predpisy o primeranosti musia preskúmavať v intervaloch najviac štyroch rokov a minister musí priebežne monitorovať vývoj v tretích krajinách a medzinárodných organizáciách, ktorý by mohol ovplyvniť rozhodnutia o právnych predpisoch o primeranosti alebo ich zmeniť. Ak minister zistí, že daná krajina alebo organizácia už nezabezpečuje primeranú úroveň ochrany osobných údajov, musí v potrebnom rozsahu zmeniť alebo zrušiť tieto právne predpisy a začať konzultácie s dotknutou treťou krajinou alebo medzinárodnou organizáciou s cieľom napraviť nedostatok primeranej úrovne ochrany.

(79) Podobne ako v článku 37 smernice (EÚ) 2016/680, ak neexistuje právny predpis o primeranosti, prenos osobných údajov v kontexte odvetvia presadzovania práva by bol možný, ak by boli zavedené primerané záruky. Takéto záruky sú zabezpečené buď a) právne záväzným nástrojom obsahujúcim primerané záruky na ochranu osobných údajov, alebo b) posúdením vykonaným prevádzkovateľom, ktorý po posúdení všetkých okolností prenosu dospeje k záveru, že existujú primerané záruky na ochranu údajov ([145]). Okrem toho, ak sa prenosy zakladajú na primeraných zárukách, v zákone o ochrane údajov z roku 2018 sa stanovuje, že okrem toho, že Komisár pre informácie ma zvyčajnú úlohu v oblasti dohľadu, musia mu príslušné orgány poskytnúť špecifické informácie o prenosoch ([146]).

(80) Ak sa prenos nezakladá na rozhodnutí o primeranosti alebo primeraných zárukách, môže sa uskutočniť len za určitých osobitných okolností, ktoré sa označujú ako „osobitné okolnosti“ ([147]). Ide o prípad, keď je prenos nevyhnutný: a) na ochranu životne dôležitých záujmov dotknutej osoby či inej osoby; b) na zabezpečenie oprávnených záujmov dotknutej osoby; c) na zabránenie bezprostrednému a vážnemu ohrozeniu verejnej bezpečnosti tretej krajiny; d) v jednotlivých prípadoch na akékoľvek účely presadzovania práva, alebo e) v jednotlivých prípadoch na právne účely (napríklad v súvislosti so súdnym konaním alebo s cieľom získať právne poradenstvo) ([148]). Možno poznamenať, že písmená d) a e) sa neuplatňujú, ak práva a slobody dotknutej osoby prevažujú nad verejným záujmom na prenose ([149]). Tento súbor okolností zodpovedá špecifickým situáciám a podmienkam kvalifikovaným ako „výnimky“ podľa článku 38 smernice (EÚ) 2016/680.

(81) Za týchto okolností sa dátum, čas a odôvodnenie prenosu, meno a všetky ďalšie relevantné informácie o príjemcovi, ako aj opis prenášaných osobných údajov musia zdokumentovať a na požiadanie poskytnúť Komisárovi pre informácie ([150]).

(82) V § 78 zákona o ochrane údajov z roku 2018 sa upravuje scenár „následných prenosov“, konkrétne prípadov, keď sa osobné údaje, ktoré boli prenesené zo Spojeného kráľovstva do tretej krajiny, následne prenášajú do inej tretej krajiny alebo medzinárodnej organizácii. V zmysle § 78 ods. 1 musí prenášajúci prevádzkovateľ zo Spojeného kráľovstva podmieniť prenos údajov tak, že sa tieto údaje nesmú ďalej prenášať do tretej krajiny bez povolenia prenášajúceho prevádzkovateľa. Okrem toho sa § 78 ods. 3 podobne ako v článku 35 ods. 1 písm. e) smernice (EÚ) 2016/680 stanovuje rad požiadaviek, ktoré platia v prípade, že sa vyžaduje takéto povolenie. Konkrétnejšie možno

([143]) Pozri memorandum o porozumení medzi ministrom ministerstva pre digitálnu oblasť, kultúru, médiá a šport (DCMS) a Úradom Komisára pre informácie o úlohe tohto komisára, pokiaľ ide o nové posúdenia Spojeného kráľovstva z hľadiska primeranosti jeho režimu ochrany údajov, k dispozícii na tomto odkaze: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Počas tohto 40-dňového obdobia môžu mať obe komory parlamentu hlasovať proti nariadeniam, ak si to želajú; ak zahlasujú proti takýmto právnym predpisom, prestanú mať v konečnom dôsledku ďalšie právne účinky.

([145]) § 75 zákona o ochrane údajov z roku 2018.

([146]) Podľa § 75 ods. 3 zákon o ochrane údajov z roku 2018, ak sa prenos údajov uskutočňuje na základe primeraných záruk: a) prenos sa musí zdokumentovať, b) dokumentácia sa musí poskytnúť Komisárovi na požiadanie a c) dokumentácia musí obsahovať najmä i) dátum a čas prenosu, ii) meno príjemcu a akékoľvek ďalšie relevantné informácie o príjemcovi, iii) odôvodnenie prenosu a iv) opis prenášaných osobných údajov.

([147]) Usmernenie k spracúvaniu údajov na účely presadzovania práva, „Existujú nejaké osobitné okolnosti?“, k dispozícii na tomto odkaze: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) § 76 zákona o ochrane údajov z roku 2018.

([149]) § 76 zákona o ochrane údajov z roku 2018.

([150]) § 76 ods. 3 zákona o ochrane údajov z roku 2018.

uviesť, že príslušný orgán sa musí pri rozhodovaní o tom, či povoliť prenos, uistiť, či je ďalší prenos nevyhnutný na účely presadzovania práva, a mal by okrem iných faktorov zohľadniť a) závažnosť okolností vedúcich k žiadosti o povolenie, b) účel, na ktorý boli osobné údaje pôvodne prenesené, a c) normy ochrany osobných údajov, ktoré sa uplatňujú v tretej krajine alebo medzinárodnej organizácii, do ktorej sa osobné údaje prenášajú.

(83) Ďalej možno uviesť, že ak sa zo Spojeného kráľovstva ďalej prenášajú údaje, ktoré boli pôvodne prenesené z Európskej únie, uplatňujú sa dodatočné záruky.

(84) Po prvé, v § 73 ods. 1 písm. b) zákona o ochrane údajov z roku 2018, podobne ako v článku 35 ods. 1 písm. c) smernice (EÚ) 2016/680, sa stanovuje, že v prípade, že osobné údaje pôvodne preniesol alebo iným spôsobom sprístupnil prevádzkovateľovi alebo inému príslušnému orgánu členský štát, musí byť týmto členským štátom alebo akoukoľvek osobou so sídlom v tomto členskom štáte, ktorá je príslušným orgánom na účely smernice (EÚ) 2016/680, prenos povolený v súlade s právom tohto členského štátu.

(85) Podobne ako v článku 35 ods. 2 smernice (EÚ) 2016/680 sa však takéto povolenie nevyžaduje, ak a) je prenos nevyhnutný na zabránenie bezprostrednému a vážnemu ohrozeniu verejnej bezpečnosti členského štátu alebo tretej krajiny alebo základných záujmov členského štátu a ak b) povolenie nie je možné získať včas. V takomto prípade musí byť bezodkladne informovaný orgán členského štátu, ktorý by bol zodpovedný za rozhodnutie o povolení prenosu ([151]).

(86) Po druhé, rovnaký prístup sa uplatňuje v prípade údajov, ktoré boli pôvodne prenesené z Európskej únie do Spojeného kráľovstva, a potom následne prenesené Spojeným kráľovstvom do tretej krajiny, ktorá uskutoční ich následný prenos do nejakej inej tretej krajiny. V takom prípade môže v zmysle § 78 ods. 4 príslušný orgán Spojeného kráľovstva udeliť povolenie len ak „členský štát, [ktorý pôvodne preniesol predmetné údaje], resp. akákoľvek osoba v tomto členskom štáte, ktorá je príslušným orgánom na účely smernice o presadzovaní práva, udelila povolenie na tento prenos v súlade s právom tohto členského štátu“. Tieto záruky sú dôležité, pretože dávajú orgánom členských štátov možnosť zabezpečiť kontinuitu ochrany údajov v súlade s predpismi EÚ na ochranu údajov v rámci „reťazca prenosu“.

(87) Tento nový rámec pre medzinárodné prenosy sa začal uplatňovať na konci prechodného obdobia ([152]). V bodoch 10 až 12 prílohy 21 (zavedenej právnymi predpismi DPPC) sa však stanovuje, že od konca prechodného obdobia sa s určitými prenosmi osobných údajov zaobchádza tak, ako keby boli založené na právnych predpisoch o primeranosti. Medzi takéto prenosy patria prenosy do členského štátu, štátu EZVO, tretej krajiny, na ktorú sa na konci prechodného obdobia vzťahuje rozhodnutie EÚ o primeranosti a na územie Gibraltáru, Prenosy do týchto krajín preto môžu pokračovať rovnako ako pred vystúpením Spojeného kráľovstva z Únie. Po skončení prechodného obdobia musí minister preskúmať zistenia primeranosti do 4 rokov, t. j. do konca decembra 2024. Podľa vysvetlenia, ktoré poskytli orgány Spojeného kráľovstva, hoci minister musí vykonať takéto preskúmanie do konca decembra 2024, prechodné ustanovenia neobsahujú ustanovenie o ukončení platnosti, to znamená, že ak sa preskúmanie neukončí do konca decembra 2024, príslušné prechodné ustanovenia automaticky neprestanú platiť.

2.4.9. *Zodpovednosť*

(88) Podľa zásady zodpovednosti sa od orgánov verejnej moci, ktoré spracúvajú údaje, vyžaduje, aby zaviedli vhodné technické a organizačné opatrenia v záujme účinného dodržiavania svojich povinností v oblasti ochrany údajov a aby vedeli takéto dodržiavanie preukázať, najmä príslušnému dozornému orgánu.

(89) Táto zásada sa odráža v § 56 zákona o ochrane údajov z roku 2018, v ktorom sa pre prevádzkovateľa zavádza všeobecná povinnosť zodpovednosti, t. j. povinnosť prijať primerané technické a organizačné opatrenia s cieľom zabezpečiť a byť schopný preukázať, že spracúvanie osobných údajov je v súlade s požiadavkami časti 3 zákona o ochrane údajov z roku 2018. Prijaté opatrenia sa musia v prípade potreby preskúmať a aktualizovať, a ak je to primerané vzhľadom na spracovanie, musia zahŕňať vhodné politiky ochrany údajov.

([151]) § 73 ods. 5 zákona o ochrane údajov z roku 2018.

([152]) Uplatniteľnosť tohto nového rámca sa musí vykladať so zreteľom na článok 782 Dohody o obchode a spolupráci medzi Európskou úniou a Európskym spoločenstvom pre atómovú energiu na jednej strane a Spojeným kráľovstvom Veľkej Británie a Severného Írska na strane druhej (L 444/14 z 31.12.2020) (ďalej len „Dohoda o obchode a spolupráci medzi Spojeným kráľovstvom a EÚ“), k dispozícii na tomto odkaze: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:22020A1231(01)&from=SK.

(90) V súlade s kapitolou IV smernice (EÚ) 2016/680 sa v § 55 až § 71 zákona o ochrane údajov z roku 2018 stanovujú rôzne mechanizmy na zabezpečenie zodpovednosti, ako aj mechanizmy umožňujúce prevádzkovateľom a sprostredkovateľom preukázať súlad. Od prevádzkovateľov sa predovšetkým vyžaduje, aby špecificky a štandardne vykonávali opatrenia na ochranu údajov, t. j. aby zabezpečili účinné vykonávanie zásad ochrany údajov a aby uchovávali záznamy o všetkých kategóriách spracovateľských činností, za ktoré je prevádzkovateľ zodpovedný (vrátane informácií o totožnosti prevádzkovateľa, kontaktných údajov zodpovednej osoby, účelov spracúvania, kategórií príjemcov zverejnení a opisu kategórií dotknutých osôb a osobných údajov) a aby tieto záznamy uchovávali a na požiadanie ich sprístupnili Komisárovi pre informácie. Prevádzkovateľ a sprostredkovateľ musia takisto viesť záznamy o určitých spracovateľských operáciách a sprístupniť ich Komisárovi pre informácie ([153]). Prevádzkovatelia sú tiež osobitne povinní spolupracovať s Komisárom pre informácie pri plnení jeho úloh.

(91) V zákone o ochrane údajov z roku 2018 sa stanovujú aj dodatočné požiadavky na spracúvanie, ktoré pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb. Patrí medzi ne povinnosť vykonať posúdenia vplyvu na ochranu údajov a konzultovať s Komisárom pre informácie pred spracovaním, ak z takéhoto posúdenia vyplynie, že spracúvanie by viedlo k vysokému riziku pre práva a slobody jednotlivcov (pri absencii opatrení na zmiernenie rizika).

(92) Prevádzkovatelia musia okrem toho vymenovať zodpovednú osobu, pokiaľ prevádzkovateľom nie je súd alebo iný súdny orgán konajúci v rámci svojej súdnej právomoci ([154]). Prevádzkovateľ musí zabezpečiť, aby zodpovedná osoba bola zapojená do všetkých otázok týkajúcich sa ochrany osobných údajov, mala potrebné zdroje a prístup k osobným údajom a spracovateľským operáciám a mohla nezávisle vykonávať svoje úlohy. Úlohy zodpovednej osoby sú stanovené v § 71 zákona o ochrane údajov z roku 2018 vrátane poskytovania informácií a poradenstva, monitorovania dodržiavania predpisov, ako aj spolupráce s Komisárom pre informácie a jeho pôsobenia ako kontaktného miesta. Zodpovedná osoba pri plnení svojich úloh musí zohľadňovať riziká spojené so spracovateľskými operáciami, berúc do úvahy povahu, rozsah, kontext a účely spracúvania.

2.5. **Dohľad a presadzovanie**

2.5.1. *Nezávislý dohľad*

(93) S cieľom zaistiť, aby bola primeraná úroveň ochrany údajov zabezpečená aj v praxi, musí byť zriadený nezávislý dozorný orgán, ktorý bude mať právomoc monitorovať a presadzovať dodržiavanie pravidiel ochrany údajov. Tento orgán musí pri plnení svojich úloh a výkone svojich právomocí konať úplne nezávisle a nestranne.

(94) V Spojenom kráľovstve vykonáva dohľad a presadzovanie dodržiavania všeobecného nariadenia Spojeného kráľovstva o ochrane údajov a zákona o ochrane údajov z roku 2018 Komisár pre informácie ([155]). Komisár pre informácie dozerá aj na spracúvanie osobných údajov príslušnými orgánmi, ktoré patria do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018 ([156]). Komisár pre informácie je „Corporation Sole“, čiže samostatný právny subjekt zložený z jednej osoby. Komisára pre informácie pri jeho práci podporuje jeho úrad. K 31. marcu 2020 mal Úrad Komisára pre informácie 768 stálych zamestnancov ([157]). Hlavným ministerstvom vo vzťahu ku Komisárovi pre informácie je Ministerstvo pre digitálnu oblasť, kultúru, médiá a šport (Department for Digital, Culture, Media and Sport ([158])).

([153]) § 62 zákona o ochrane údajov z roku 2018.
([154]) § 69 zákona o ochrane údajov z roku 2018.
([155]) Článok 36 ods. 2 písm. b) smernice (EÚ) 2016/680.
([156]) § 116 zákona o ochrane údajov z roku 2018.
([157]) Výročná správa a finančné výkazy Komisára pre informácie za roky 2019 – 2020, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.
([158]) Ich vzájomný vzťah upravuje dohoda o riadení. Medzi najdôležitejšie povinnosti Ministerstva pre digitálnu oblasť, kultúru, médiá a šport ako hlavného ministerstva patrí najmä: zabezpečiť, aby Komisár pre informácie bol primerane financovaný a mal primerané zdroje; zastupovať záujmy Komisára pre informácie v parlamente a v rámci vzťahov s ďalšími ministerstvami; zabezpečiť zavedenie spoľahlivého vnútroštátneho rámca na ochranu údajov a poskytovať Komisárovi pre informácie usmernenia a podporu v prevádzkových otázkach, ako sú otázky týkajúce sa nehnuteľností, lízingov a obstarávania (dohoda o riadení na roky 2018 – 2021, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Nezávislosť Komisára je výslovne stanovená v § 52 všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, v ktorom sa odrážajú požiadavky stanovené v článku 52 ods. 1 až 3 nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 ([159]). Komisár musí pri plnení svojich úloh a vykonávaní svojich právomocí podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov konať úplne nezávisle, nesmie byť pod vonkajším vplyvom, či už priamym alebo nepriamym, vo vzťahu k týmto úlohám a právomociam, a nesmie od nikoho žiadať ani prijímať pokyny. Komisár sa tiež musí zdržať akéhokoľvek konania nezlučiteľného so svojimi povinnosťami a počas výkonu funkcie nevykonáva žiadnu platenú ani neplatenú pracovnú činnosť nezlučiteľnú s jeho funkciou.

(96) Podmienky vymenovania a odvolania Komisára pre informácie sú stanovené v prílohe 12 k zákonu o ochrane údajov z roku 2018. Komisára pre informácie vymenúva kráľovná na odporúčanie vlády na základe spravodlivého a otvoreného výberového konania. Uchádzač musí mať primeranú kvalifikáciu, zručnosti a schopnosti. V súlade s kódexom riadenia verejných menovaní ([160]) zostaví poradná hodnotiaca komisia zoznam menovateľných kandidátov. Predtým, ako minister Ministerstva pre digitálnu oblasť, kultúru, médiá a šport dospeje ku konečnému rozhodnutiu, príslušný užší výbor parlamentu musí vykonať kontrolu pred vymenovaním. Stanovisko výboru sa zverejňuje ([161]).

(97) Komisár pre informácie vykonáva svoju funkciu najviac sedem rokov. Z funkcie ho môže odvolať jej veličenstvo na základe jej určenému prejavu vôle oboch snemovní parlamentu (tzv. Address) ([162]). Žiadosť o odvolanie Komisára pre informácie možno predložiť niektorej zo snemovní parlamentu, len ak minister predloží tejto snemovni správu, v ktorej uvedie, že je presvedčený, že Komisár pre informácie sa dopustil závažného pochybenia a/alebo že Komisár už nespĺňa podmienky požadované na výkon svojich funkcií ([163]).

(98) Financovanie Komisára pre informácie pochádza z troch zdrojov: i) poplatky za ochranu údajov, ktoré platia prevádzkovatelia a ktoré sú stanovené právnymi predpismi ministra ([164]); tieto poplatky tvoria 85 – 90 % ročného rozpočtu Úradu Komisára pre informácie ([165]); ii) subvencie, ktoré môže vláda poskytnúť Komisárovi pre informácie a ktoré sa využívajú najmä na financovanie prevádzkových nákladov Komisára pre informácie, pokiaľ ide o úlohy nesúvisiace s ochranou údajov ([166]); iii) poplatky účtované za služby ([167]). V súčasnosti sa neúčtujú žiadne takéto poplatky.

(99) Všeobecné funkcie Komisára pre informácie v súvislosti so spracúvaním osobných údajov, ktoré patrí do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018, sú stanovené v prílohe 13 k zákonu o ochrane údajov z roku 2018. Medzi úlohy patrí monitorovanie a presadzovanie časti 3 zákona o ochrane údajov z roku 2018, podpora informovanosti verejnosti, poradenstvo parlamentu, vláde a iným inštitúciám v oblasti legislatívnych a administratívnych opatrení, podpora informovanosti prevádzkovateľov a sprostredkovateľov o ich povinnostiach,

([159]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (Ú. v. EÚ L 119, 4.5.2016, s. 1).

([160]) Kódex riadenia verejných menovaní, k dispozícii na tomto odkaze: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Druhá správa zo zasadnutia Výboru Dolnej snemovne pre kultúru, médiá a šport 2015 – 2016, k dispozícii na tomto odkaze: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) „Address“ je návrh predložený parlamentu, ktorého cieľom je upovedomiť monarchu o stanoviskách parlamentu k určitej téme.

([163]) Príloha 12 bod 3 k zákonu o ochrane údajov z roku 2018.

([164]) § 137 zákona o ochrane údajov z roku 2018.

([165]) § 137 a 138 zákona o ochrane údajov z roku 2018 obsahujú niekoľko záruk na zabezpečenie toho, aby poplatky boli stanovené na primeranej úrovni. V § 137 ods. 4 zákona o ochrane údajov z roku 2018 sa konkrétne uvádzajú záležitosti, ktoré musí minister zohľadniť pri vydávaní právnych predpisov, v ktorých sa stanovuje suma, ktorú musia zaplatiť rôzne organizácie. V § 138 ods. 1 a § 182 zákona o ochrane údajov z roku 2018 sa tiež stanovuje zákonná požiadavka, že minister je ešte pred prijatím týchto právnych predpisov povinný uskutočniť konzultácie s Komisárom pre informácie a inými zástupcami osôb, na ktoré by sa tieto právne predpisy mohli vzťahovať, a to v záujme zohľadnenia ich názorov. Komisár pre informácie je okrem toho podľa § 138 ods. 2 zákona o ochrane údajov z roku 2018 povinný priebežne preskúmavať fungovanie právnych predpisov o poplatkoch a môže ministrovi predložiť návrhy na ich zmenu. A napokon, s výnimkou prípadov, keď sa právne predpisy prijímajú len s cieľom zohľadniť zvýšenie indexu maloobchodných cien (v takom prípade budú podliehať postupu tzv. negatívneho uznesenia parlamentu), tieto právne predpisy podliehajú postupu kladného uznesenia a môžu sa prijať až po tom, ako ich každá z komôr parlamentu schváli svojim uznesením.

([166]) V dohode o riadení sa ozrejmilo, že minister môže prideliť Komisárovi pre informácie prostriedky z financií, ktoré poskytol parlament podľa prílohy 12 bodu 9 k zákonu o ochrane údajov z roku 2018. Po konzultácii s Komisárom pre informácie poskytne Ministerstvo pre digitálnu oblasť, kultúru, médiá a šport tomuto komisárovi príslušné sumy (subvencie) na pokrytie jeho administratívnych nákladov a plnenie funkcií vo vzťahu k viacerým osobitným úlohám vrátane slobody informácií (dohoda o riadení na roky 2018 – 2021, bod 1.12, pozri poznámku pod čiarou č. 158).

([167]) § 134 zákona o ochrane údajov z roku 2018.

poskytovanie informácií dotknutým osobám o uplatňovaní ich práv a vedenie vyšetrovaní. V záujme zachovania nezávislosti justície nie je Komisár pre informácie oprávnený vykonávať svoje funkcie v súvislosti so spracúvaním osobných údajov jednotlivcom konajúcim v rámci súdnej právomoci, resp. súdom či tribunálom konajúcim v rámci svojej súdnej právomoci. Dohľad nad justíciou však vykonávajú špecializované orgány, o ktorých sa hovorí ďalej.

2.5.1.1. Presadzovanie vrátane sankcií

(100) Komisár pre informácie má všeobecné vyšetrovacie, nápravné, povoľovacie a poradné právomoci v súvislosti so spracúvaním osobných údajov, na ktoré sa vzťahuje časť 3 zákona o ochrane údajov z roku 2018. Komisár pre informácie má právomoc oznámiť prevádzkovateľovi alebo sprostredkovateľovi údajné porušenie časti 3, vydať prevádzkovateľovi alebo sprostredkovateľovi varovanie o tom, že zamýšľané operácie spracovania pravdepodobne porušia ustanovenia časti 3 a vydať prevádzkovateľovi alebo sprostredkovateľovi napomenutie, ak operácie spracúvania porušili ustanovenia časti 3. Okrem toho môže Komisár pre informácie z vlastnej iniciatívy alebo na požiadanie vydávať stanoviská určené parlamentu Spojeného kráľovstva, vláde alebo iným inštitúciám a orgánom, ako aj verejnosti k akejkoľvek otázke týkajúcej sa ochrany osobných údajov ([168]).

(101) Komisár pre informácie má okrem toho právomoc:

— nariadiť prevádzkovateľovi a sprostredkovateľovi (a za určitých okolností akejkoľvek inej osobe), aby poskytli potrebné informácie prostredníctvom oznámenia („informačné oznámenie“) ([169]),

— vykonávať vyšetrovania a audity prostredníctvom oznámenia o posúdení, v ktorom sa môže vyžadovať, aby prevádzkovateľ alebo sprostredkovateľ povolil Komisárovi pre informácie vstúpiť do určených priestorov, skontrolovať alebo preskúmať dokumenty alebo vybavenie, vypočuť osoby, ktoré spracúvajú osobné údaje v mene prevádzkovateľa („oznámenie o posúdení“) ([170]),

— získať iným spôsobom prístup k dokumentom prevádzkovateľov a sprostredkovateľov a prístup do ich priestorov v súlade s § 154 zákona o ochrane údajov z roku 2018 („právomoci na vstup a inšpekciu“),

— vykonávať nápravné právomoci, a to aj prostredníctvom varovaní a napomenutí, alebo vydávať príkazy prostredníctvom oznámenia o presadzovaní, v ktorom sa od prevádzkovateľov, resp. sprostredkovateľov vyžaduje, aby prijali konkrétne kroky alebo aby sa zdržali prijatia konkrétnych krokov („presadzovacie oznámenie“) ([171]) a

— udeľovať správne pokuty vo forme oznámenia o uložení sankcie (ďalej len „oznámenie o uložení sankcie“) ([172]).

(102) Okolnosti, za ktorých Komisára pre informácie vydáva informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie a oznámenie o uložení sankcie sa stanovujú v jeho regulačnej politike ([173]). V presadzovacom oznámení sa môžu stanovovať požiadavky, ktoré Komisár pre informácie považuje za vhodné na účely nápravy nesplnenia povinnosti. V oznámení o uložení sankcie sa vyžaduje, aby príslušná osoba zaplatila Komisárovi pre informácie sumu uvedenú v oznámení. Oznámenie o uložení sankcie možno vydať v prípade nedodržania určitých ustanovení zákona o ochrane údajov z roku 2018 ([174]) alebo sa môže vydať voči prevádzkovateľovi alebo sprostredkovateľovi, ktorí nekonali v súlade s informačným oznámením, oznámením o posúdení alebo presadzovacím oznámením.

(103) Konkrétnejšie, pri určovaní toho, či sa má voči určitému prevádzkovateľovi alebo sprostredkovateľovi vydať oznámenie o uložení sankcie, a pri určovaní výšky sankcie musí Komisár pre informácie zohľadniť skutočnosti uvedené v § 155 ods. 3 zákona o ochrane údajov z roku 2018 vrátane povahy a závažnosti pochybenia, úmyselného alebo nedbanlivého charakteru pochybenia, akýchkoľvek opatrení prijatých prevádzkovateľom alebo

([168]) Bod 2 prílohy 13 k zákonu o ochrane údajov z roku 2018.
([169]) § 142 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 143 zákona o ochrane údajov z roku 2018).
([170]) § 146 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 147 zákona o ochrane údajov z roku 2018).
([171]) § 149 až § 151 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 152 zákona o ochrane údajov z roku 2018).
([172]) § 155 zákona o ochrane údajov z roku 2018 (s výhradou obmedzení stanovených v § 156 zákona o ochrane údajov z roku 2018).
([173]) Regulačná politika, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Komisár pre informácie môže najmä vydať oznámenie o uložení sankcie za nesplnenie povinnosti podľa § 149 ods. 2, 3, 4 alebo 5 zákona o ochrane údajov z roku 2018.

sprostredkovateľom s cieľom zmierniť škodu, ktorú utrpeli dotknuté osoby, stupňa zodpovednosti prevádzkovateľa alebo sprostredkovateľa (so zreteľom na technické a organizačné opatrenia vykonané prevádzkovateľom alebo sprostredkovateľom) a akýchkoľvek relevantných predchádzajúcich pochybení prevádzkovateľa alebo sprostredkovateľa, kategórií osobných údajov, ktorých sa zlyhanie týka, a toho, či by sankcia bola účinná, primeraná a odrádzajúca.

(104) Maximálna výška sankcie, ktorú možno uložiť na základe oznámenia o uložení sankcie, je a) 17 500 000 GBP za nedodržanie zásad ochrany údajov (§ 35, § 36, § 37, § 38 ods. 1, § 39 ods. 1 a § 40 zákona o ochrane údajov z roku 2018), povinnosti transparentnosti a individuálnych práv (§ 44, § 45, § 46, § 47, § 48, § 49, § 52 a § 53 zákona o ochrane údajov z roku 2018) a zásad pre medzinárodné prenosy osobných údajov (§ 73, § 75, § 76, § 77 alebo § 78 zákona o ochrane údajov z roku 2018), inak b) 8 700 000 GBP ([175]). V súvislosti s nedodržaním informačného oznámenia, oznámenia o posúdení alebo presadzovacieho oznámenia je maximálna výška sankcie, ktorú možno uložiť na základe oznámenia o uložení sankcie 17 500 000 GBP.

(105) Podľa posledných výročných správ (2018 – 2019 ([176]), 2019 – 2020 ([177])) Komisár pre informácie uskutočnil niekoľko vyšetrovaní v súvislosti so spracúvaním osobných údajov orgánmi presadzovania práva v trestných veciach. Komisár napríklad viedol vyšetrovanie a v októbri 2019 uverejnil stanovisko týkajúce sa používania technológie rozpoznávania tváre na verejných miestach na účely presadzovania práva. Vyšetrovanie sa zameriavalo najmä na využívanie schopností rozpoznávania tváre v reálnom čase zo strany polície Južného Walesu a Metropolitnej policajnej služby (ďalej len „MPS“). Okrem toho Komisár pre informácie prešetroval matricu MPS na odhaľovanie gangov ([178]) a zistil celý rad závažných porušení právnych predpisov o ochrane údajov, ktoré by mohli narušiť dôveru verejnosti v matricu a používanie údajov.

(106) V novembri 2018 Komisár pre informácie vydal presadzovacie oznámenie a následne MPS podnikla kroky potrebné na zvýšenie bezpečnosti a zodpovednosti a na zabezpečenie primeraného využívania údajov.

(107) Ďalším príkladom nedávneho presadzovacieho opatrenia je pokuta vo výške 325 000 GBP, ktorú Komisára pre informácie uložil v máji 2018 prokuratúre Crown Prosecution Service za stratu nezašifrovaných nosičov DVD obsahujúcich záznamy policajných výsluchov. Komisár pre informácie okrem toho prešetroval širšie témy, napríklad v prvej polovici roka 2020 využívanie extrakcie mobilných telefónov na policajné účely a spracovanie údajov o obetiach zo strany polície.

(108) Okrem toho, že Komisár pre informácie má uvedené právomoci v oblasti presadzovania, určité porušenia právnych predpisov o ochrane údajov predstavujú trestné činy, a preto môžu podliehať trestnoprávnym sankciám (§ 196 zákona o ochrane údajov z roku 2018). Ide napríklad o získanie alebo sprístupnenie osobných údajov bez súhlasu prevádzkovateľa a poskytnutie prístupu k osobným údajom inej osobe bez súhlasu prevádzkovateľa ([179]); opätovnú identifikáciu anonymizovaných osobných údajov bez súhlasu prevádzkovateľa zodpovedného za anonymizáciu týchto osobných údajov ([180]); úmyselné bránenie Komisárovi pre informácie pri výkone jeho právomocí v súvislosti s kontrolou osobných údajov v súlade s medzinárodnými záväzkami ([181]), nepravdivé vyhlásenia o odpovedi na informačné oznámenie, alebo zničenie informácií v súvislosti s informačným oznámením a oznámením o posúdení ([182]).

(109) Komisár pre informácie má tiež podľa § 139 zákona o ochrane údajov z roku 2018 povinnosť predložiť každej zo snemovní parlamentu všeobecnú správu o plnení svojich funkcií podľa zákona ([183]).

([175]) § 157 zákona o ochrane údajov z roku 2018.

([176]) Výročná správa a finančné výkazy Komisára pre informácie za roky 2018 – 2020, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Výročná správa Komisára pre informácie za roky 2019 – 2020 (pozri poznámku pod čiarou č. 157).

([178]) Databáza, ktorá zaznamenávala spravodajské informácie týkajúce sa údajných členov gangov a obetí trestných činov súvisiacich s gangmi.

([179]) § 170 zákona o ochrane údajov z roku 2018.

([180]) § 171 zákona o ochrane údajov z roku 2018.

([181]) § 119 zákona o ochrane údajov z roku 2018.

([182]) § 144 a § 148 zákona o ochrane údajov z roku 2018.

([183]) Ako sa stanovuje v dohode o riadení, výročná správa musí: i) zahŕňať všetky podnikateľské subjekty, dcérske podniky alebo spoločné podniky pod kontrolou Komisára pre informácie; ii) byť v súlade s Manuálom finančného vykazovania (FReM) ministerstva financií; iii) obsahovať vyhlásenie o riadení, v ktorom sa uvádzajú spôsoby, akými účtovník riadil a kontroloval zdroje používané v organizácii v priebehu roka, a preukazuje sa, do akej miery organizácia riadi riziká na dosiahnutie svojich zámerov a cieľov a iv) informovať o hlavných činnostiach a výsledkoch počas predchádzajúceho rozpočtového roka a vymedziť v súhrnnej forme plány budúcich období (dohoda o riadení na roky 2018 – 2021, bod 3.26, pozri poznámku pod čiarou č. 158).

2.5.2. *Dohľad nad justíciou*

(110) Dohľad nad spracúvaním osobných údajov súdmi a justíciou je dvojaký. Ak súdny úradník alebo súd nekoná v rámci súdnej právomoci, dohľad vykonáva Komisár pre informácie. Ak prevádzkovateľ koná v rámci súdnej právomoci, Komisár pre informácie nemôže plniť svoje funkcie dohľadu ([184]) a dohľad vykonávajú osobitné orgány. Uvedené odráža prístup prijatý v článku 32 smernice (EÚ) 2016/680.

(111) Konkrétne v druhom scenári, pokiaľ ide o súdy Anglicka a Walesu a ich tribunály prvého stupňa a vyššie tribunály (First-tier and Upper Tribunals of England and Wales), takýto dohľad vykonáva súdna rada pre ochranu údajov (Judicial Data Protection Panel) ([185]). Okrem toho šéf justície Anglicka a Walesu (Lord Chief Justice) a šéf tribunálov (Senior President of Tribunals) vydali oznámenie o ochrane osobných údajov ([186]), v ktorom sa uvádza, ako súdy v Anglicku a Walese spracúvajú osobné údaje na účely plnenia súdnej funkcie. Podobné oznámenie vydali súdy Severného Írska ([187]) a Škótska ([188]).

(112) Okrem toho v Severnom Írsku vymenoval šéf justície Severného Írska (Lord Chief Justice of Northern Ireland) sudcu Vrchného súdu (High Court) za sudcu pre dohľad nad údajmi (Data Supervisory Judge) ([189]). Vydal tiež usmernenia pre severoírsku justíciu o tom, čo robiť v prípade straty alebo potenciálnej straty údajov a o postupe riešenia akýchkoľvek otázok, ktoré z toho vyplývajú ([190]).

(113) V Škótsku šéf justície Lord President vymenoval sudcu pre dohľad nad údajmi (Data Supervisory Judge), ktorý vyšetruje všetky sťažnosti z dôvodu ochrany údajov. Stanovuje sa tak v pravidlách súdnych sťažností, ktoré odrážajú pravidlá stanovené pre Anglicko a Wales ([191]).

(114) Napokon na najvyššom súde (Supreme Court) je vymenovaný jeden zo sudcov tohto súdu, aby vykonával dohľad nad ochranou údajov.

([184]) § 117 zákona o ochrane údajov z roku 2018.

([185]) Súdna rada pre ochranu údajov je zodpovedná za poskytovanie usmernení a odbornej prípravy pre justíciu. Zaoberá sa aj sťažnosťami dotknutých osôb v súvislosti so spracúvaním osobných údajov súdmi, tribunálmi a jednotlivcami konajúcimi v rámci súdnej právomoci. Cieľom súdnej rady pre ochranu údajov je poskytnúť prostriedky na riešenie akejkoľvek sťažnosti. Ak sťažovateľ nebol spokojný s rozhodnutím tejto rady a poskytol dodatočné dôkazy, rada môže svoje rozhodnutie prehodnotiť. Hoci samotná súdna rada pre ochranu údajov neukladá finančné sankcie, ak sa domnieva, že došlo k dostatočne závažnému porušeniu zákona o ochrane údajov z roku 2018, môže vec postúpiť justičnému vyšetrovaciemu úradu (Judicial Conduct Investigation Office), ktorý sťažnosť vyšetrí. Ak sa sťažnosti vyhovie, je vecou lorda kancelára a šéfa justície Anglicka a Walesu (alebo vyššieho sudcu povereného konať v jeho mene), aby rozhodli, aké kroky by sa mali podniknúť proti dotknutej osobe zastávajúcej príslušný úrad. V poradí závažnosti by to mohlo zahŕňať: formálnu radu, formálne varovanie, napomenutie a v konečnom dôsledku odvolanie z funkcie. Ak je jednotlivec nespokojný so spôsobom, akým justičný vyšetrovací úrad (Judicial Conduct Investigation Office) vyšetroval sťažnosť, svoju sťažnosť môže ďalej predložiť ombudsmanovi pre menovania a správanie sudcov (Judicial Appointments and Conduct Ombudsman) (pozri https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Tento ombudsman má právomoc požiadať justičný vyšetrovací úrad (Judicial Conduct Investigation Office) o opätovné preskúmanie sťažnosti a môže navrhnúť, aby bola sťažovateľovi vyplatená náhrada škody, ak sa domnieva, že utrpel škodu v dôsledku nesprávneho úradného postupu.

([186]) Oznámenie o ochrane osobných údajov šéfa justície Anglicka a Walesu (Lord Chief Justice) a šéfa tribunálov (Senior President of Tribunals) je k dispozícii na tomto odkaze: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Oznámenie o ochrane osobných údajov šéfa justície Severného Írska (Lord Chief Justice of Northern Ireland) je k dispozícii na tomto odkaze: https://judiciaryni.uk/data-privacy.

([188]) Oznámenie o ochrane osobných údajov pre škótske súdy a tribunály je k dispozícii na tomto odkaze: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Sudca pre dohľad nad údajmi poskytuje justícii usmernenie a vyšetruje porušenia a/alebo sťažnosti v súvislosti so spracúvaním osobných údajov súdmi alebo jednotlivcami konajúcimi v rámci súdnej právomoci.

([190]) Ak sa sťažnosť alebo porušenie považujú za závažné, postúpia sa v súlade s kódexom postupov pre sťažnosti (Code of practice on Complaints) vydaným šéfom justície Severného Írska (Lord Chief Justice of Northern Ireland) súdnemu úradníkovi pre sťažnosti (Judicial Complaints Officer) na ďalšie vyšetrovanie. Výsledkom takejto sťažnosti môžu byť: žiadne ďalšie opatrenia, poradenstvo, odborná príprava alebo mentorstvo, neformálne varovanie, formálne varovanie, konečné varovanie, obmedzenie praxe alebo postúpenie správnemu tribunálu. Kódex postupov pre sťažnosti vydaný šéfom justície Severného Írska (Lord Chief Justice of Northern Ireland) je k dispozícii na tomto odkaze: 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]) Sudca pre dohľad nad údajmi (Data Supervisory Judge) vyšetruje každú odôvodnenú sťažnosť, ktorá sa postupuje šéfovi justície Lord President, ktorý má právomoc vydávať rady, formálne varovanie alebo napomenutie, ak to považuje za potrebné (rovnocenné pravidlá existujú pre členov tribunálov a sú k dispozícii na tomto odkaze: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Náprava*

(115) V záujme zabezpečenia primeranej ochrany, a najmä vymáhania individuálnych práv, by dotknutá osoba mala mať k dispozícii účinné správne a súdne prostriedky nápravy vrátane náhrady škôd.

(116) Po prvé, dotknutá osoba má právo podať sťažnosť Komisárovi pre informácie, ak sa domnieva, že v súvislosti s osobnými údajmi, ktoré sa jej týkajú, došlo k porušeniu časti 3 zákona o ochrane údajov z roku 2018 ([192]). Ako sa uvádza v odôvodneniach (100) a (109), Komisár pre informácie má právomoc posúdiť dodržiavanie zákona o ochrane údajov z roku 2018 prevádzkovateľom a sprostredkovateľom a požadovať od nich, aby v prípade nedodržiavania tohto zákona prijali potrebné kroky, resp. aby sa zdržali prijatia potrebných krokov, ako aj uložiť pokuty.

(117) Po druhé, zákon o ochrane údajov z roku 2018 stanovuje právo na nápravu uplatniteľné voči Komisárovi pre informácie. Ak Komisár pre informácie „nepokročil" ([193]) vo veci sťažnosti podanej dotknutou osobou, sťažovateľ má prístup k súdnemu prostriedku nápravy, pretože sa môže obrátiť na tribunál prvého stupňa (First Tier Tribunal) ([194]) s cieľom nariadiť Komisárovi pre informácie, aby v reakcii na sťažnosť prijal vhodné opatrenia, alebo aby informoval sťažovateľa o pokroku v súvislosti so sťažnosťou ([195]). Okrem toho sa každá osoba, ktorá dostane od Komisára pre informácie akékoľvek z uvedených oznámení (informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie alebo oznámenie o uložení sankcie), môže odvolať na tribunál prvého stupňa. Ak sa tribunál domnieva, že rozhodnutie Komisára pre informácie nie je v súlade so zákonom alebo že Komisár pre informácie mal uplatniť svoju voľnú úvahu inak, tribunál musí odvolaniu vyhovieť, resp. musí vydať iné oznámenie alebo prijať iné rozhodnutie, ktoré mohol vydať alebo prijať Komisár pre informácie ([196]).

(118) Po tretie, fyzické osoby môžu získať súdne prostriedky nápravy voči prevádzkovateľom a sprostredkovateľom priamo na súdoch podľa § 167 zákona o ochrane údajov z roku 2018. Ak súd na návrh dotknutej osoby dospeje k záveru, že došlo k porušeniu práv dotknutej osoby v zmysle právnych predpisov o ochrane údajov, môže nariadiť prevádzkovateľovi v súvislosti so spracúvaním alebo sprostredkovateľovi konajúcemu v mene tohto prevádzkovateľa, aby podnikol kroky uvedené v súdnom príkaze alebo aby sa zdržal prijatia krokov uvedených v súdnom príkaze. Okrem toho podľa § 169 zákona o ochrane údajov z roku 2018 akákoľvek osoba, ktorá utrpí škodu v dôsledku porušenia niektorej požiadavky právnych predpisov o ochrane údajov (vrátane časti 3 zákona o ochrane údajov z roku 2018) iných ako všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, má nárok na náhradu tejto škody od prevádzkovateľa alebo sprostredkovateľa s výnimkou prípadu, že prevádzkovateľ alebo sprostredkovateľ dokáže, že prevádzkovateľ alebo sprostredkovateľ nie je žiadnym spôsobom zodpovedný za udalosť, ktorá spôsobila škodu. Škoda zahŕňa tak finančnú ujmu, ako aj škodu, ktorá nezahŕňa finančnú ujmu, ako napríklad nemajetkovú ujmu.

(119) Po štvrté, pokiaľ sa akákoľvek osoba domnieva, že orgány verejnej moci porušili jej práva vrátane práva na súkromie a ochranu údajov, môže získať nápravu na súdoch Spojeného kráľovstva podľa zákona o ľudských právach z roku 1998. Prevádzkovatelia podľa časti 3 zákona o ochrane údajov z roku 2018, t. j. príslušné orgány, sú vždy orgánmi verejnej moci v zmysle zákona o ľudských právach z roku 1998. Jednotlivec, ktorý tvrdí, že orgán verejnej moci konal (alebo navrhuje konať) spôsobom, ktorý je nezlučiteľný s právom vyplývajúcim z dohovoru, a teda protiprávny podľa § 6 ods. 1 zákona o ľudských právach z roku 1998, môže podať návrh na začatie konania proti tomuto orgánu na príslušnom súde alebo tribunáli, resp. sa dovolávať príslušných práv v akomkoľvek súdnom konaní, ak je (alebo by mohol byť) obeťou protiprávneho činu ([197]).

([192]) § 165 zákona o ochrane údajov z roku 2018.

([193]) V § 166 zákona o ochrane údajov z roku 2018 sa konkrétne uvádzajú tieto situácie: a) Komisár pre informácie nepodnikne primerané kroky v reakcii na sťažnosť, b) Komisár pre informácie neposkytne sťažovateľovi informácie o pokroku v súvislosti so sťažnosťou alebo o jej výsledku pred uplynutím 3-mesačnej lehoty, ktorá začína plynúť od prijatia sťažnosti týmto komisárom, alebo c) v prípade, že posúdenie sťažnosti Komisárom pre informácie počas tohto obdobia ešte nie je ukončené, ak neposkytne sťažovateľovi takéto informácie počas nasledujúcich 3 mesiacov.

([194]) Tribunál prvého stupňa je súd príslušný na rozhodovanie o odvolaniach proti rozhodnutiam vládnych regulačných orgánov. V prípade rozhodnutia Komisára pre informácie je príslušnou komorou „Všeobecná regulačná komora", ktorá má právomoc nad celým Spojeným kráľovstvom.

([195]) § 166 zákona o ochrane údajov z roku 2018.

([196]) § 161 a § 162 zákona o ochrane údajov z roku 2018.

([197]) Pozri vec Brown/Commissioner of the Met 2016, v ktorej súd poskytol navrhovateľke nápravu v súvislosti s ochranou údajov v rámci žaloby podanej proti polícii. Súd rozhodol v prospech navrhovateľky tak, že potvrdil jej tvrdenia týkajúce sa porušenia povinností podľa zákona o ochrane údajov z roku 2018, porušenia povinností podľa zákona o ľudských právach z roku 1998 (a súvisiaceho práva podľa článku 8 EDĽP) a konštatoval delikt zneužitia súkromných informácií (žalovaný v konečnom dôsledku pripustil existenciu rozporu s povinnosťami podľa zákona o ochrane údajov z roku 2018 a EDĽP, takže rozsudok bol zameraný na to, aký prostriedok nápravy je primeraný). V dôsledku týchto porušení súd priznal navrhovateľke peňažnú náhradu škody.

(120) Ak súd zistí, že akýkoľvek akt orgánu verejnej moci je nezákonný, môže v rámci svojich právomocí nariadiť akúkoľvek nápravu alebo vydať akýkoľvek príkaz, ktoré považuje za vhodné a primerané ([198]). Súd môže tiež vyhlásiť ustanovenie primárneho práva za nezlučiteľné s právom zaručeným EDĽP.

(121) Jednotlivec môže napokon za porušenie práv zaručených EDĽP po vyčerpaní vnútroštátnych prostriedkov nápravy dosiahnuť nápravu pred Európskym súdom pre ľudské práva.

2.6. **Následné poskytovanie údajov**

(122) V práve Spojeného kráľovstva sa za určitých podmienok povoľuje, aby orgán presadzovania práva poskytol údaje ďalším orgánom Spojeného kráľovstva na iné účely ako tie, na ktoré boli pôvodne získané (tzv. následné poskytnutie).

(123) Podobne ako v článku 4 ods. 2 smernice (EÚ) 2016/680 sa aj § 36 ods. 3 zákona o ochrane údajov z roku 2018 umožňuje, aby sa osobné údaje získané príslušným orgánom na účely presadzovania práva mohli ďalej spracúvať (či už pôvodným prevádzkovateľom alebo iným prevádzkovateľom) na akýkoľvek iný účel presadzovania práva za predpokladu, že prevádzkovateľ je zo zákona oprávnený spracúvať údaje na tento iný účel a predmetné spracovanie je nevyhnutné a primerané ([199]). V takom prípade sa na spracúvanie vykonávané prijímajúcim orgánom uplatnia všetky záruky stanovené v časti 3 zákona o ochrane údajov z roku 2018 a analyzované vyššie.

(124) V právnom poriadku Spojeného kráľovstva výslovne umožňujú následné poskytovanie údajov rôzne právne predpisy. Predovšetkým v i) zákone o digitálnom hospodárstve z roku 2017 sa umožňuje vzájomné poskytovanie údajov medzi orgánmi verejnej moci na viaceré účely, napríklad v prípade akéhokoľvek podvodu voči verejnému sektoru, ktorý by zahŕňal ujmu alebo hrozbu ujmy pre orgán verejnej moci ([200]), resp. v prípade dlhu voči orgánu verejnej moci alebo korune ([201]); v ii) zákone o trestnej činnosti a súdoch z roku 2013 sa umožňuje poskytovanie informácií Národnej kriminálnej agentúre ([202]) na účely boja proti závažnej a organizovanej trestnej činnosti, jej vyšetrovania a stíhania; v iii) zákone o závažnej trestnej činnosti z roku 2007 sa umožňuje orgánom verejnej moci sprístupňovať informácie organizáciám na boj proti podvodom na účely predchádzania podvodom ([203]).

(125) V týchto právnych predpisoch sa výslovne stanovuje, že poskytnutie informácií by sa malo uskutočniť v súlade s pravidlami stanovenými v zákona o ochrane údajov z roku 2018. Okrem toho policajná akadémia College of Policing vydala autorizovanú profesijnú prax poskytovania informácií ([204]) s cieľom pomôcť polícii pri plnení jej povinností v oblasti ochrany údajov podľa všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, zákona o ochrane osobných údajov a zákona o ľudských právach Spojeného kráľovstva z roku 1998. Súlad poskytnutia údajov s uplatniteľným právnym rámcom na ochranu údajov môže samozrejme podliehať súdnemu preskúmaniu ([205]).

(126) Okrem toho, podobne ako v článku 9 smernice (EÚ) 2016/680, sa v zákone o ochrane údajov z roku 2018 stanovuje, že osobné údaje získané na akýkoľvek účel presadzovania práva sa môžu spracúvať na účel, ktorý nie je presadzovaním práva, ak je spracúvanie povolené zákonom ([206]). Tento typ poskytovania zahŕňa dva scenáre: 1. ak orgán presadzovania trestného práva poskytuje údaje orgánu na presadzovanie iného práva, ako je trestné právo, ktorý nie je spravodajskou službou (napr. finančný alebo daňový orgán, orgán na ochranu hospodárskej súťaže, úrad starostlivosti o mládež); 2. ak orgán presadzovania trestného práva poskytuje údaje spravodajskej službe.

([198]) § 8 ods. 1 zákona o ľudských právach z roku 1998.

([199]) § 36 ods. 3 zákona o ochrane údajov z roku 2018.

([200]) § 56 zákona o digitálnom hospodárstve z roku 2017, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) § 48 zákona o digitálnom hospodárstve z roku 2017.

([202]) § 7 zákona o trestnej činnosti a súdoch z roku 2013, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2013/22/contents.

([203]) § 68 zákona o závažnej trestnej činnosti z roku 2007, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([204]) Autorizovaná profesijná prax poskytovania informácií, k dispozícii na tomto odkaze: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

([205]) Pozri napríklad vec M/The Chief Constable of Sussex Police [2019] EWHC 975 (Admin), v ktorej bol Vrchný súd (High Court) požiadaný, aby posúdil výmenu údajov medzi políciou a Partnerstvo na znižovanie kriminality pri podnikaní (Business Crime Reduction Partnership – BCRP), organizáciou poverenou správou systému oznámení o vylúčení z podnikateľských priestorov, ktorými sa zakazuje osobám vstupovať do takýchto priestorov jej členov. Súd preskúmal poskytovanie údajov, ktoré prebiehalo na základe dohody, ktorej cieľom je ochrana verejnosti a predchádzanie trestnej činnosti, a nakoniec dospel k záveru, že väčšina aspektov poskytovania údajov je zákonná, s výnimkou niektorých citlivých informácií, ktoré si vzájomne poskytovali polícia a BCRP. Ďalším príkladom je vec Cooper/NCA [2019] EWCA Civ 16, v ktorej odvolací súd potvrdil vzájomné poskytovanie údajov medzi políciou a Agentúrou pre závažnú organizovanú trestnú činnosť (Serious Organised Crime Agency – SOCA), orgánom presadzovania práva, ktorý je v súčasnosti súčasťou vnútroštátneho orgánu na ochranu hospodárskej súťaže.

([206]) § 36 ods. 4 zákona o ochrane údajov z roku 2018.

V prvom scenári bude spracúvanie osobných údajov patriť do rozsahu pôsobnosti všeobecného nariadenia Spojeného kráľovstva o ochrane údajov, ako aj do časti 2 zákona o ochrane údajov z roku 2018. Ako sa uvádza v rozhodnutí prijatom podľa nariadenia (EÚ) 2016/679, záruky stanovené vo všeobecnom nariadení Spojeného kráľovstva o ochrane údajov a v časti 2 zákona o ochrane údajov z roku 2018 poskytujú úroveň ochrany, ktorá je v zásade rovnocenná úrovni ochrany poskytovanej v rámci Únie ([207]).

(127) V druhom scenári, teda pokiaľ ide o poskytovanie údajov získaných orgánom presadzovania trestného práva spravodajskej službe na účely národnej bezpečnosti, je právnym základom, ktorý umožňuje takéto poskytnutie, zákon o boji proti terorizmu z roku 2008 ([208]). Podľa zákona o boji proti terorizmu z roku 2008 môže každá osoba poskytnúť informácie ktorejkoľvek zo spravodajských služieb na účely plnenia ktorejkoľvek z funkcií tejto služby vrátane „národnej bezpečnosti“.

(128) Pokiaľ ide o podmienky, za ktorých sa údaje môžu poskytovať na účely národnej bezpečnosti, zákon o spravodajských službách a zákon o bezpečnostných službách obmedzujú schopnosť spravodajských služieb získavať údaje na to, čo je nevyhnutné na plnenie ich zákonných funkcií. Príslušné orgány, ktoré patria do rozsahu pôsobnosti časti 3 zákona o ochrane údajov z roku 2018 a ktoré chcú poskytnúť údaje spravodajským službám, musia okrem funkcií týchto služieb, ktoré sú stanovené v zákone o spravodajských službách a v zákone o bezpečnostných službách, zvážiť niekoľko faktorov/obmedzení ([209]). V § 20 zákona o boji proti terorizmu z roku 2008 sa jasne uvádza, že akékoľvek poskytnutie údajov podľa § 19 zákona o boji proti terorizmu z roku 2008 musí byť stále v súlade s právnymi predpismi o ochrane údajov; čo znamená, že sa uplatňujú všetky obmedzenia a požiadavky zákona o ochrane údajov z roku 2018. Orgány presadzovania práva a spravodajské služby sú okrem toho orgánmi verejnej moci v zmysle zákona o ľudských právach z roku 1998, a preto musia zabezpečiť, aby konali v súlade s právami zaručenými podľa EDĽP vrátane jeho článku 8. Povedané inak, tieto požiadavky znamenajú, že každé poskytnutie údajov medzi orgánmi presadzovania práva a spravodajskými službami musí byť v súlade s právnymi predpismi o ochrane údajov a EDĽP.

(129) Spracovanie osobných údajov prijatých alebo získaných od orgánov presadzovania práva na účely národnej bezpečnosti spravodajskými službami podlieha viacerým podmienkam a zárukám ([210]). Časť 4 zákon o ochrane údajov z roku 2018 sa vzťahuje na každé spracúvanie spravodajskými službami alebo v ich mene. Stanovujú sa

([207]) Vykonávacie rozhodnutie Komisie podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o primeranej ochrane osobných údajov Spojeným kráľovstvom, C(2021) 4800.

([208]) § 19 zákona o boji proti terorizmu z roku 2008, k dispozícii na tomto odkaze: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) V § 2 ods. 2 zákona o spravodajských službách z roku 1994 (https://www.legislation.gov.uk/ukpga/1994/13/contents) sa stanovuje, že vedúci spravodajskej služby je zodpovedný za efektívnosť tejto služby a je povinný zabezpečiť – a) aby existovali opatrenia na zabezpečenie toho, aby spravodajská služba získala informácie, len ak sú potrebné na riadne plnenie jej funkcií a že akákoľvek informácia bude zverejnená, len ak je to nevyhnutné – i) na tento účel; ii) v záujme národnej bezpečnosti; iii) na účely predchádzania závažnej trestnej činnosti alebo jej odhaľovania, alebo iv) na účely akéhokoľvek trestného konania a b) že spravodajská služba nepodnikne žiadne kroky na podporu záujmov žiadnej politickej strany Spojeného kráľovstva; zatiaľ čo v § 2 ods. 2 zákona o bezpečnostných službách z roku 1989 (pozri https://www.legislation.gov.uk/ukpga/1989/5/contents) sa stanovuje, že generálny riaditeľ je zodpovedný za efektívnosť tejto služby a je povinný zabezpečiť – a) aby existovali opatrenia na zabezpečenie toho, aby služba získala informácie, len ak sú potrebné na riadne plnenie jej funkcií, resp. že akákoľvek informácia bude zverejnená, len ak je to nevyhnutné na tento účel alebo na účel predchádzania závažnej trestnej činnosti alebo jej odhaľovania alebo na účely akéhokoľvek trestného konania a b) že služba nepodnikne žiadne kroky na podporu záujmov žiadnej politickej strany a zabezpečiť c) aby existovali opatrenia dohodnuté s generálnym riaditeľom Národnej kriminálnej agentúry, ktorých cieľom je koordinácia činností služby podľa § 1 ods. 4 tohto zákona s činnosťou policajných zložiek, Národnej kriminálnej agentúry a iných orgánov presadzovania práva.

([210]) Záruky a obmedzenia právomocí spravodajských služieb sú upravené aj zákonom o vyšetrovacích právomociach z roku 2016, ktorý spolu so zákonom o regulácii vyšetrovacích právomocí pre Anglicko, Wales a Severné Írsko z roku 2000 a zákonom o regulácii vyšetrovacích právomocí (Škótsko) z roku 2000 pre Škótsko poskytuje právny základ pre využívanie takýchto právomocí. Tieto právomoci však nie sú relevantné v kontexte „následného poskytovania údajov“, keďže sa vzťahujú na priame získavanie osobných údajov spravodajskými službami. Pokiaľ ide o posúdenie právomocí udelených spravodajským službám zákonom o vyšetrovacích právomociach, pozri vykonávacie rozhodnutie Komisie podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o primeranej ochrane osobných údajov Spojeným kráľovstvom, C(2021) 4800.

v nej hlavné zásady ochrany údajov (zákonnosť, spravodlivosť a transparentnosť ([211]), obmedzenie účelu ([212]), minimalizácia údajov ([213]), správnosť ([214]), minimalizácia uchovávania ([215]) a bezpečnosť ([216])), a zavádzajú sa v ňom podmienky spracúvania osobitných kategórií údajov ([217]), stanovujú práva dotknutých osôb ([218]), zavádza požiadavka špecificky navrhnutej ochrany údajov ([219]) a upravujú sa v ňom medzinárodné prenosy osobných údajov ([220]).

(130) Zároveň sa v § 110 zákona o ochrane údajov z roku 2018 stanovuje výnimka z osobitných ustanovení v časti 4 zákona o ochrane údajov z roku 2018, ak je táto výnimka potrebná na zabezpečenie národnej bezpečnosti. V § 110 ods. 2 zákona o ochrane údajov z roku 2018 sa uvádzajú ustanovenia, z ktorých je povolená výnimka. Zahŕňa zásady ochrany údajov (okrem zásady zákonnosti), práva dotknutých osôb, povinnosť informovať Komisára pre informácie o porušení ochrany údajov, kontrolné právomoci Komisára pre informácie v súlade s medzinárodnými záväzkami, ako aj jeho niektoré právomoci v oblasti presadzovania práva, ustanovenia, na základe ktorých sa určité porušenia ochrany údajov považujú za trestný čin, a ustanovenia týkajúce sa osobitných účelov spracúvania, ako sú žurnalistické, akademické alebo umelecké účely. Tejto výnimky sa možno dovolávať na základe analýzy jednotlivých prípadov ([221]). Ako vysvetlili orgány Spojeného kráľovstva a potvrdila judikatúra súdov Spojeného kráľovstva, prevádzkovatelia musia zvážiť skutočné dôsledky pre národnú bezpečnosť alebo obranu, ak mali povinnosť dodržiavať konkrétne ustanovenia o ochrane údajov a ak mohli primerane dodržať toto obvyklé pravidlo bez toho, aby to malo vplyv na národnú bezpečnosť alebo obranu“ ([222]). To, či sa výnimka použila primerane, podlieha dohľadu Komisára pre informácie ([223]).

([211]) Podľa § 86 ods. 6 zákona o ochrane údajov z roku 2018 sa pri určovaní spravodlivosti a transparentnosti spracúvania prihliada na spôsob získavania údajov. V tomto zmysle je požiadavka spravodlivosti a transparentnosti splnená, ak sa údaje získajú od osoby, ktorá je zákonne oprávnená alebo od ktorej sa zákonom vyžaduje, aby ich poskytla.

([212]) Podľa § 87 zákona o ochrane údajov z roku 2018 musia byť účely spracúvania konkrétne určené, výslovne uvedené a legitímne. Údaje sa nesmú spracúvať spôsobom, ktorý nie je zlučiteľný s účelom, na ktorý boli získané. Podľa § 87 ods. 3 možno ďalšie zlučiteľné spracovanie osobných údajov povoliť len vtedy, ak je prevádzkovateľ zákonom oprávnený spracúvať údaje na tento účel a spracovanie je nevyhnutné a primerané tomuto inému účelu. Spracúvanie by sa malo považovať za zlučiteľné, ak spracúvanie pozostáva zo spracúvania na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely a podlieha primeraným zárukám (§ 87 ods. 4 zákona o ochrane údajov z roku 2018).

([213]) Osobné údaje musia byť primerané, relevantné a nie nadmerné (§ 88 zákona o ochrane údajov z roku 2018).

([214]) Osobné údaje musia byť presné a aktuálne (§ 89 zákona o ochrane údajov z roku 2018).

([215]) Osobné údaje sa nesmú uchovávať dlhšie, ako je potrebné (§ 90 zákona o ochrane údajov z roku 2018).

([216]) Šiesta zásada ochrany údajov spočíva v tom, že osobné údaje sa musia spracúvať spôsobom, ktorý zahŕňa prijatie primeraných bezpečnostných opatrení, pokiaľ ide o riziká, ktoré vyplývajú zo spracovania osobných údajov. Riziká zahŕňajú (okrem iného) náhodný alebo neoprávnený prístup k osobným údajom alebo ich zničenie, stratu, použitie, zmenu alebo zverejnenie (§ 91 zákona o ochrane údajov z roku 2018). V § 107 sa takisto vyžaduje, aby 1. každý prevádzkovateľ zaviedol primerané bezpečnostné opatrenia zodpovedajúce rizikám vyplývajúcim zo spracúvania osobných údajov a 2. v prípade automatizovaného spracúvania vykonal každý prevádzkovateľ a každý sprostredkovateľ preventívne alebo zmierňujúce opatrenia založené na hodnotení rizika.

([217]) § 86 ods. 2 písm. b) a príloha 10 k zákonu o ochrane údajov z roku 2018.

([218]) Kapitola 3 časti 4 zákona o ochrane údajov z roku 2018, najmä práva: prístupu, opravy a vymazania, ako aj právo namietať proti spracúvaniu a nepodliehať automatizovanému rozhodovaniu, právo zasahovať do automatizovaného rozhodovania a byť informovaný o tomto rozhodovaní. Okrem toho musí prevádzkovateľ dotknutej osobe poskytnúť informácie o spracovaní jej osobných údajov.

([219]) § 103 zákona o ochrane údajov z roku 2018.

([220]) § 109 zákona o ochrane údajov z roku 2018. Prenos osobných údajov medzinárodným organizáciám alebo krajinám mimo Spojeného kráľovstva je možný, ak je prenos nevyhnutným a primeraným opatrením vykonávaným na účely zákonných funkcií prevádzkovateľa alebo na iné účely stanovené v osobitných ustanoveniach zákona o bezpečnostných službách z roku 1989 a zákona o spravodajských službách z roku 1994.

([221]) Pozri vec Baker/Secretary of State for the Home Department [2001] UKIT NSA2 (Baker/Secretary of State).

([222]) Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom „Ochrana údajov v oblasti národnej bezpečnosti a rámec vyšetrovacích právomocí“, s. 15 – 16, k dispozícii na tomto odkaze https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Pozri tiež rozsudok Baker/Secretary of State (pozri poznámku pod čiarou č. 220), v ktorom tribunál zrušil osvedčenie o záujme národnej bezpečnosti vydané ministerstvom vnútra a potvrdil uplatnenie výnimky týkajúcej sa národnej bezpečnosti vzhľadom na to, že neexistoval dôvod stanoviť paušálnu výnimku týkajúcu sa povinnosti odpovedať na žiadosti o prístup a že umožnenie takejto výnimky za každých okolností bez analýzy jednotlivých prípadov presahovalo rámec toho, čo bolo potrebné a primerané na ochranu národnej bezpečnosti.

([223]) Pozri Memorandum o porozumení medzi Komisárom pre informácie a spravodajským spoločenstvom Spojeného kráľovstva, podľa ktorého sa Komisár pre informácie v prípade prijatia sťažnosti od dotknutej osoby bude chcieť uistiť, že v danej otázke sa postupovalo správne a že použitie výnimky bolo v príslušnom prípade náležité (Memorandum o porozumení medzi Úradom Komisára pre informácie a spravodajským spoločenstvom Spojeného kráľovstva, bod 16, k dispozícii na tomto odkaze: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Okrem toho, pokiaľ ide o možnosť obmedziť akékoľvek z uvedených práv v záujme ochrany „národnej bezpečnosti“, v § 79 zákona o ochrane údajov z roku 2018 sa stanovuje, že prevádzkovateľ môže požiadať o osvedčenie podpísané ministrom vlády alebo generálnym prokurátorom, v ktorom sa potvrdzuje, že obmedzenie takýchto práv je (resp. v určitom čase bolo) nevyhnutným a primeraným opatrením na ochranu národnej bezpečnosti ([224]). Vláda Spojeného kráľovstva vydala usmernenie k osvedčeniam o záujme národnej bezpečnosti vydávaným podľa zákona o ochrane údajov z roku 20018, v ktorom sa predovšetkým zdôrazňuje, že akékoľvek obmedzenie práv dotknutých osôb na zaistenie národnej bezpečnosti musí byť primerané a nevyhnutné ([225]). Všetky osvedčenia o záujme národnej bezpečnosti sa musia uverejniť na webovom sídle Komisára pre informácie ([226]).

(132) Osvedčenie by malo mať pevne stanovené obdobie nie dlhšie ako päť rokov, aby ho mohol výkonný orgán pravidelne preskúmavať ([227]). V osvedčení sa uvedú osobné údaje alebo kategórie osobných údajov, na ktoré sa vzťahuje výnimka, ako aj ustanovenia zákona o ochrane údajov z roku 2018, na ktoré sa výnimka vzťahuje ([228]).

(133) Je dôležité poznamenať, že osvedčenia o záujme národnej bezpečnosti nedávajú dodatočný dôvod na to, aby boli obmedzené práva na ochranu údajov z dôvodov národnej bezpečnosti. Inými slovami, prevádzkovateľ alebo sprostredkovateľ sa môžu odvolávať na osvedčenie len vtedy, keď dospeli k záveru, že je potrebné odvolávať sa na výnimku v záujme národnej bezpečnosti, ktorá sa musí uplatňovať od prípadu k prípadu. Aj keď sa na predmetnú vec vzťahuje osvedčenie o záujme národnej bezpečnosti, Komisár pre informácie môže preskúmať, či v konkrétnom prípade bolo uplatnenie výnimky v záujme národnej bezpečnosti odôvodnené ([229]).

(134) Každá osoba, ktorej sa vydanie osvedčenia priamo týka, sa môže proti osvedčeniu ([230]) odvolať na vyšší tribunál (Upper Tribunal) ([231]) alebo, ak sa v osvedčení identifikujú údaje prostredníctvom všeobecného opisu, napadnúť uplatňovanie osvedčenia na konkrétne údaje ([232]).

(135) Tribunál preskúma rozhodnutie o vydaní osvedčenia a rozhodne, či existovali opodstatnené dôvody na vydanie tohto osvedčenia ([233]). Môže zohľadniť širokú škálu otázok vrátane nevyhnutnosti, primeranosti a zákonnosti pri zvažovaní vplyvu na práva dotknutých osôb a vyvažovaní potreby zabezpečiť národnú bezpečnosť. V dôsledku toho môže tribunál rozhodnúť, že osvedčenie sa nevzťahuje na konkrétne osobné údaje, ktoré sú predmetom odvolania ([234]).

([224]) Zákonom o ochrane údajov z roku 2018 bola zrušená možnosť vydať osvedčenie podľa § 28 ods. 2 zákona o ochrane údajov z roku 1998. Možnosť vydania „starých osvedčení“ však stále existuje, a to v rozsahu, v aktom to vyplýva z možnosti, ktorá historicky existuje podľa zákona o ochrane údajov z roku 1998 (pozri bod 17 časti 5 prílohy 20 k zákonu o ochrane údajov z roku 2018). Táto možnosť je však veľmi vzácna a uplatní sa len v obmedzenom počte prípadov, ako napr. keď subjekt údajov napadne uplatnenie výnimky v záujme národnej bezpečnosti vo vzťahu k spracúvaniu zo strany orgánu verejnej moci, ktorý toto spracúvanie uskutočnil na základe zákona o ochrane údajov z roku 1998. Treba poznamenať, že v takýchto prípadoch sa uplatnia všetky ustanovenia § 28 zákona o ochrane údajov z roku 1998, a teda aj ustanovenie umožňujúce subjektu údajov napadnúť príslušné osvedčenie. V súčasnosti neexistujú žiadne osvedčenia o záujme národnej bezpečnosti vydané podľa zákona o ochrane údajov z roku 1998.

([225]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti podľa zákona o ochrane údajov z roku 2018, k dispozícii na tomto odkaze: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) Podľa § 130 zákona o ochrane údajov z roku 2018 môže Komisár pre informácie rozhodnúť, že sa nesmie uverejniť znenie určitého osvedčenia, resp. jeho časť, ak by to bolo v rozpore so záujmom národnej bezpečnosti, alebo ak by to bolo inak v rozpore s verejným záujmom, resp. ak by to mohlo ohroziť bezpečnosť ktorejkoľvek osoby. V takýchto prípadoch však Komisár pre informácie uverejní skutočnosť, že takéto osvedčenie bolo vydané.

([227]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, bod 15, pozri poznámku pod čiarou č. 225.

([228]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, bod 5, pozri poznámku pod čiarou č. 225.

([229]) V § 102 zákona o ochrane údajov z roku 2018 sa stanovuje, že prevádzkovateľ musí byť schopný preukázať, že splnil požiadavky zákona o ochrane údajov z roku 2018. To znamená, že spravodajská služba by musela Komisárovi pre informácie preukázať, že pri odvolávaní sa na výnimku zvážila osobitné okolnosti prípadu. Komisár pre informácie okrem toho uverejňuje aj záznam o osvedčeniach o záujme národnej bezpečnosti, k dispozícii na tomto odkaze: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) § 111 ods. 3 zákona o ochrane údajov z roku 2018.

([231]) Vyšší tribunál (Upper Tribunal) je súd príslušný na rozhodovanie o odvolaniach proti rozhodnutiam nižších správnych súdov a má osobitnú právomoc, pokiaľ ide o priame odvolania proti rozhodnutiam určitých vládnych orgánov.

([232]) § 111 ods. 5 zákona o ochrane údajov z roku 2018.

([233]) Pozri tiež rozsudok Baker/Secretary of State (pozri poznámku pod čiarou č. 221), v ktorom tribunál pre informácie zrušil osvedčenie o záujme národnej bezpečnosti vydané ministerstvom vnútra vzhľadom na to, že neexistoval dôvod stanoviť paušálnu výnimku týkajúcu sa povinnosti odpovedať na žiadosti o prístup a že umožnenie takejto výnimky za každých okolností bez analýzy jednotlivých prípadov presahovalo rámec toho, čo bolo potrebné a primerané na ochranu národnej bezpečnosti.

([234]) Usmernenie vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti, bod 25, pozri poznámku pod čiarou č. 224.

(136) Iný súbor možných obmedzení sa týka obmedzení, ktoré sa podľa prílohy 11 k zákonu o ochrane údajov z roku 2018 uplatňujú na určité ustanovenia časti 4 zákona o ochrane údajov z roku 2018 ([235]) s cieľom chrániť iné dôležité ciele všeobecného verejného záujmu alebo chránené záujmy, ako napríklad parlamentné výsady, dôvernosť komunikácie medzi advokátom a jeho klientom, vedenie súdnych konaní alebo bojovú účinnosť ozbrojených síl. Uplatňovanie týchto ustanovení je buď oslobodené pre určité kategórie informácií („výnimky na základe kategórie"), alebo je oslobodené v rozsahu, v akom by uplatňovanie týchto ustanovení mohlo ohroziť chránený záujem („výnimky na základe ujmy") ([236]). Výnimky na základe ujmy sa môžu uplatniť len vtedy, ak by uplatňovanie uvedených ustanovení o ochrane údajov mohlo byť na ujmu príslušnému osobitnému záujmu. Použitie výnimky musí byť preto vždy odôvodnené odkazom na príslušnú ujmu, ktorá by mohla nastať v konkrétnom prípade. Výnimky na základe kategórie možno uplatniť len v súvislosti so špecifickou, úzko vymedzenou kategóriou informácií, pre ktorú sa výnimka udeľuje. Z hľadiska účelu a účinku sú podobné niekoľkým výnimkám zo všeobecného nariadenia Spojeného kráľovstva o ochrane údajov (podľa prílohy 2 k zákonu o ochrane údajov z roku 2018), ktoré zase odrážajú výnimky stanovené v článku 23 všeobecného nariadenia o ochrane údajov.

(137) Z uvedeného vyplýva, že obmedzenia a podmienky sú zavedené podľa platných právnych predpisov Spojeného kráľovstva, a to aj v zmysle ich výkladu súdmi a Komisie pre informácie, aby sa zabezpečilo, že tieto výnimky a obmedzenia zostanú v medziach toho, čo je nevyhnutné a primerané na ochranu národnej bezpečnosti.

(138) Na spracúvanie osobných údajov spravodajskými službami podľa časti 4 zákona o ochrane údajov z roku 2018 dozerá Komisár pre informácie ([237]).

(139) Všeobecné funkcie Komisára pre informácie v súvislosti so spracúvaním osobných údajov zo strany spravodajských služieb, ktoré patrí do rozsahu pôsobnosti časti 4 zákona o ochrane údajov z roku 2018, sú stanovené v prílohe 13 k zákonu o ochrane údajov z roku 2018. Medzi úlohy patrí (nie však výhradne) monitorovanie a presadzovanie časti 4 zákona o ochrane údajov z roku 2018, podpora informovanosti verejnosti, poradenstvo parlamentu, vláde a iným inštitúciám v oblasti legislatívnych a administratívnych opatrení, podpora informovanosti prevádzkovateľov a sprostredkovateľov o ich povinnostiach, poskytovanie informácií dotknutým osobám o uplatňovaní ich práv a vedenie vyšetrovaní.

(140) Komisár má, podobne ako v časti 3 zákona o ochrane údajov z roku 2018, právomoc informovať prevádzkovateľov o údajnom porušení a vydávať varovania o tom, že spracúvaním môže porušovať pravidlá, ako aj vydávať napomenutia v prípade, že sa porušenie potvrdí. Môže vydávať aj presadzovacie oznámenia a oznámenia o uložení sankcie za porušenie určitých ustanovení tohto zákona ([238]). Na rozdiel od ostatných častí zákona o ochrane údajov z roku 2018 však Komisár nemôže národnému bezpečnostnému orgánu predložiť oznámenie o posúdení ([239]).

(141) Okrem toho sa v § 110 ods. 6 zákona o ochrane údajov z roku 2018 stanovuje výnimka z využívania určitých právomocí Komisára, ak je to potrebné na účely ochrany národnej bezpečnosti. Patrí sem právomoc Komisára vydávať (akýkoľvek druh) oznámení podľa zákona o ochrane údajov (informačné oznámenie, oznámenie o posúdení, presadzovacie oznámenie a oznámenie o uložení sankcie), právomoc vykonávať inšpekcie v súlade

([235]) Patria sem: i) zásady ochrany údajov podľa časti 4 s výnimkou požiadavky zákonnosti spracovania podľa prvej zásady a skutočnosti, že spracúvanie musí spĺňať jednu z príslušných podmienok stanovených v prílohách 9 a 10; ii) práva dotknutých osôb a iii) povinnosti týkajúce sa oznamovania porušení Komisárovi pre informácie.

([236]) Podľa vysvetľujúceho rámca Spojeného kráľovstva medzi „výnimky na základe kategórie" patria: i) informácie o udelení čestných titulov koruny (Crown honours and dignities); ii) dôvernosť komunikácie medzi advokátom a jeho klientom; iii) dôverné údaje o zamestnaní, odbornej príprave alebo vzdelávaní a iv) odpovede v písomných skúškach a známky zo skúšok. „Výnimky na základe ujmy" sa týkajú týchto záležitostí: i) predchádzanie trestnej činnosti alebo jej odhaľovanie, zadržanie a trestné stíhanie páchateľov; ii) parlamentné výsady; iii) súdne konania; iv) bojová účinnosť ozbrojených síl koruny; v) hospodársky blahobyt Spojeného kráľovstva; vi) rokovania s dotknutou osobou; vii) vedecký alebo historický výskum alebo štatistické účely; viii) archivácia vo verejnom záujme. Vysvetľujúci rámec Spojeného kráľovstva pre diskusiu o primeranosti, oddiel H s názvom National Security (Národná bezpečnosť), s. 13 (pozri poznámku pod čiarou č. 222).

([237]) § 116 zákona o ochrane údajov z roku 2018.

([238]) Podľa výkladu § 149 ods. 2 v spojení s § 155 zákona o ochrane údajov z roku 2018 možno prevádzkovateľovi alebo sprostredkovateľovi vydať presadzovacie oznámenie a oznámenie o uložení sankcie v súvislosti s porušením časti 4 kapitoly 2 zákona o ochrane údajov z roku 2018 (zásady spracúvania), ustanovenia časti 4 zákona o ochrane údajov z roku 2018, ktorým sa dotknutej osobe udeľujú práva, požiadavky oznámiť porušenie ochrany osobných údajov Komisárovi podľa § 108 zákona o ochrane údajov z roku 2018, ako aj v súvislosti s porušením zásad prenosu osobných údajov do tretích krajín, krajín, ktoré nie sú zmluvnými stranami dohovoru, a medzinárodným organizáciám podľa § 109 zákona o ochrane údajov z roku 2018. (Pokiaľ ide o ďalšie podrobnosti o presadzovacom oznámení a oznámení o uložení sankcie, pozri odôvodnenia (102) až (103)).

([239]) Podľa § 147 ods. 6 zákona o ochrane údajov z roku 2018 Komisár pre informácie nemôže vydať oznámenie o posúdení orgánu uvedenému v § 23 ods. 3 zákona o slobodnom prístupe k informáciám z roku 2000. Patria sem Bezpečnostná služba (MI5), tajná spravodajská služba (MI6) a vládne komunikačné ústredie Government Communications Headquarter.

s medzinárodnými záväzkami, právomoci na vstup a inšpekciu a pravidlá týkajúce sa trestných činov ([240]). Ako sa vysvetľuje v odôvodnení (136), tieto výnimky sa budú uplatňovať len vtedy, ak sú potrebné a primerané, a od prípadu k prípadu. Uplatnenie týchto výnimiek podlieha súdnemu preskúmaniu ([241]).

(142) Komisár pre informácie a spravodajské služby Spojeného kráľovstva podpísali memorandum o porozumení ([242]), ktorým sa stanovuje rámec pre spoluprácu vo viacerých otázkach vrátane oznámení o porušení ochrany údajov a vybavovania sťažností dotknutých osôb. Konkrétne sa v ňom stanovuje, že po prijatí sťažnosti Komisár pre informácie posúdi, či sa primerane uplatnila nejaká výnimka v záujme národnej bezpečnosti. V zmysle usmernenia vlády Spojeného kráľovstva k osvedčeniam o záujme národnej bezpečnosti podľa zákona o ochrane údajov z roku 2018 musia príslušné subjekty poskytnúť odpovede na otázky, ktoré Komisár pre informácie položil v súvislosti s preskúmaním jednotlivých sťažností, do 20 pracovných dní, pričom sa použijú vhodné bezpečné kanály, ak sa týkajú utajovaných skutočností. Od apríla 2018 ku dnešnému dňu dostal Komisár pre informácie od jednotlivcov 21 sťažností na spravodajské služby. Každá sťažnosť bola posúdená a výsledok bol oznámený dotknutej osobe ([243]).

(143) Parlamentný výbor pre spravodajstvo a bezpečnosť okrem toho vykonáva parlamentný dohľad nad spracúvaním údajov spravodajskými službami. Tento výbor má svoj právny základ v zákone o spravodlivosti a bezpečnosti z roku 2013 ([244]). Týmto zákonom sa v parlamente Spojeného kráľovstva zriaďuje výbor pre spravodajstvo a bezpečnosť. Tento výbor pozostáva z členov oboch snemovní parlamentu, pričom za členov výboru ich vymenúva predseda vlády po konzultácii s lídrom opozície ([245]). Výbor pre spravodajstvo a bezpečnosť je povinný predkladať parlamentu výročnú správu o plnení svojich funkcií a ďalšie správy, ktoré považuje za vhodné ([246]).

(144) Od roku 2013 má výbor pre spravodajstvo a bezpečnosť väčšie právomoci vrátane dohľadu nad operačnými činnosťami bezpečnostných služieb. Podľa § 2 zákona o spravodlivosti a bezpečnosti z roku 2013 má tento výbor za úlohu dohliadať na výdavky, správu, politiku a činnosť služieb v oblasti národnej bezpečnosti. V zákone

([240]) Výnimka sa môže vzťahovať na tieto ustanovenia: § 108 (oznámenie porušenia ochrany osobných údajov Komisárovi), § 119 (inšpekcia v súlade s medzinárodnými záväzkami), § 142 až § 154 a príloha 15 (oznámenia Komisára a právomoci na vstup a inšpekciu) a § 170 až § 173 (trestné činy týkajúce sa osobných údajov). V súvislosti so spracovaním zo strany spravodajských služieb sa môže vzťahovať aj na prílohu 13 (Ďalšie všeobecné funkcie Komisára), odsek 1 písm. a) a g) a odsek 2

([241]) Pozri napr. rozsudok Baker/Secretary of State for the Home Department (pozri poznámku pod čiarou č. 221)

([242]) Memorandum o porozumení medzi Komisárom pre informácie a spravodajskými službami Spojeného kráľovstva, pozri poznámku pod čiarou č. 231.

([243]) V siedmich z týchto prípadov Komisár pre informácie sťažovateľovi odporučil, aby podal podnet prevádzkovateľovi údajov (bolo tomu tak v prípade, že fyzická osoba podala podnet Komisárovi, hoci ho mal najprv podať prevádzkovateľovi), v jednom z týchto prípadov Komisár poskytol prevádzkovateľovi všeobecné poradenstvo (deje sa tak vtedy, keď prevádzkovateľ svojim konaním právne predpisy zrejme neporušil, ale zlepšenie postupov mohlo zabrániť tomu, aby bola Komisárovi podaná sťažnosť) a v zostávajúcich 13 prípadoch nebolo potrebné podniknúť žiadne kroky zo strany prevádzkovateľa (deje sa tak vtedy, ak podnet predložený jednotlivcom nespadá pod zákon o ochrane údajov z roku 2018, pretože sa týka spracúvania osobných údajov, ale na základe poskytnutých informácií sa zdá, že prevádzkovateľ neporušil právne predpisy).

([244]) Ako vysvetlili orgány Spojeného kráľovstva, zákonom o spravodlivosti a bezpečnosti z roku 2013 sa rozšíril rozsah pôsobnosti výboru pre spravodajstvo a bezpečnosť tak, aby zahŕňal úlohu dohľadu nad spravodajskou komunitou nad rámec troch agentúr a umožnil retrospektívny dohľad nad operačnými činnosťami týchto agentúr v otázkach významného národného záujmu.

([245]) § 1 zákona o spravodlivosti a bezpečnosti z roku 2013. Ministri nemôžu byť členmi. Poslanci sú členmi tohto výboru počas funkčného obdobia parlamentu, v rámci ktorého boli vymenovaní. Členstva v tomto výbore môžu byť zbavení uznesením snemovne, ktorá ich vymenovala, resp. ak stratia poslanecký mandát alebo sa stanú ministrami. Člen výboru sa takisto môže svojho členstva vzdať.

([246]) Správy a vyhlásenia výboru sú dostupné online na tomto odkaze: http://isc.independent.gov.uk/committee-reports. V roku 2015 vydal výbor pre spravodajstvo a bezpečnosť správu s názvom „Súkromie a bezpečnosť: moderný a transparentný právny rámec“ (pozri: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), v ktorom posúdil právny rámec techník sledovania, ktoré používajú spravodajské služby a vydal súbor odporúčaní, ktoré boli následne posúdené a začlenené do návrhu zákona o vyšetrovacích právomociach, ktorý sa stal zákonom o vyšetrovacích právomociach z roku 2016. Odpoveď vlády na túto správu je k dispozícii na tomto odkaze: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

o spravodlivosti a bezpečnosti z roku 2013 sa uvádza, že výbor pre spravodajstvo a bezpečnosť môže prešetrovať operačné záležitosti, ak nesúvisia s prebiehajúcimi operáciami ([247]). V memorande o porozumení medzi predsedom vlády a výborom pre spravodajstvo a bezpečnosť ([248]) sa podrobne uvádzajú prvky, ktoré sa majú zohľadniť pri posudzovaní toho, či určitá činnosť nie je súčasťou žiadnej prebiehajúcej operácie ([249]). Výbor pre spravodajstvo a bezpečnosť môže o prešetrenie prebiehajúcich operácií požiadať aj predseda vlády a tento výbor môže preskúmavať aj informácie, ktoré poskytli služby dobrovoľne.

(145) Podľa prílohy 1 k zákonu o spravodlivosti a bezpečnosti z roku 2013 môže výbor pre spravodajstvo a bezpečnosť požiadať vedúcich ktorejkoľvek z troch spravodajských služieb o poskytnutie akýchkoľvek informácií. Daná služba nemusí tieto informácie sprístupniť, len ak príslušný minister neuplatnil právo veta ([250]). Orgány Spojeného kráľovstva ozrejmili, že v praxi bol tomuto výboru zamietnutý prístup len k veľmi málo informáciám ([251]).

(146) Pokiaľ ide o prostriedky nápravy, v súlade s § 165 ods. 2 zákona o ochrane údajov z roku 2018 môže dotknutá osoba podať sťažnosť Komisárovi pre informácie, ak sa domnieva, že v súvislosti s osobnými údajmi, ktoré sa jej týkajú, došlo k porušeniu časti 4 zákona o ochrane údajov z roku 2018 vrátane akéhokoľvek zneužitia výnimiek a obmedzení v záujme národnej bezpečnosti.

(147) Okrem toho podľa časti 4 zákona o ochrane údajov z roku 2018 sú jednotlivci oprávnení podať na Vrchný súd (High Court), resp. v Škótsku na Court of Session, návrh na vydanie príkazu, ktorým sa od prevádzkovateľa vyžaduje, aby dodržiaval právo na prístup k údajom ([252]), právo namietať voči spracúvaniu ([253]) a právo na opravu alebo vymazanie.

(148) Jednotlivci sú tiež oprávnení požadovať od prevádzkovateľa alebo sprostredkovateľa náhradu škody utrpenej v dôsledku porušenia požiadavky časti 4 zákona o ochrane údajov z roku 2018 ([254]). Škoda zahŕňa tak finančnú ujmu, ako aj škodu, ktorá nezahŕňa finančnú ujmu, ako napríklad nemajetkovú ujmu ([255]).

(149) Jednotlivec môže napokon podať sťažnosť na tribunáli pre kontrolu vyšetrovacích právomocí (Investigatory Powers Tribunal) v súvislosti s akýmkoľvek konaním spravodajských služieb Spojeného kráľovstva alebo v ich mene ([256]). Tento tribunál bol zriadený zákonom o regulácii vyšetrovacích právomocí pre Anglicko, Wales a Severné Írsko z roku 2000 a zákonom o regulácii vyšetrovacích právomocí (Škótsko) z roku 2000 pre Škótsko, pričom je nezávislý od výkonnej moci ([257]). V súlade s § 65 zákona o regulácii vyšetrovacích právomocí z roku 2000 členov tribunálu pre kontrolu vyšetrovacích právomocí vymenúva jej veličenstvo na obdobie piatich rokov.

(150) Z funkcie môže člena tribunálu odvolať jej veličenstvo na základe jej určenému prejavu vôle (tzv. Address) ([258]) oboch snemovní parlamentu ([259]).

(151) Keď chce jednotlivec podať návrh na začatie konania na tribunáli pre kontrolu vyšetrovacích právomocí (ďalej len „požiadavka aktívnej legitimácie“), musí byť podľa § 65 zákona o regulácii vyšetrovacích právomocí z roku 2000 presvedčený, že i) spravodajská služba konala vo vzťahu k nemu, k jeho akémukoľvek majetku, k akejkoľvek komunikácii uskutočnenej ním alebo jemu určenej, k jeho využitiu akejkoľvek poštovej služby, telekomunikačnej služby alebo telekomunikačného systému ([260]), a ii) že k tomuto konaniu došlo za

([247]) § 2 zákona o spravodlivosti a bezpečnosti z roku 2013.
([248]) Memorandum o porozumení medzi predsedom vlády a výborom pre spravodajstvo a bezpečnosť, k dispozícii na tomto odkaze: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Memorandum o porozumení medzi predsedom vlády a výborom pre spravodajstvo a bezpečnosť, bod 14, pozri poznámku pod čiarou č 248.
([250]) Minister môže vetovať poskytnutie informácií len z dvoch dôvodov: informácie sú citlivé a nemali by byť výboru pre spravodajstvo a bezpečnosť sprístupnené v záujme národnej bezpečnosti, resp. ide o informácie takej povahy, že ak by bol minister požiadaný, aby ich predložil užšiemu rezortnému výboru Dolnej snemovne, považoval by ich predloženie (z dôvodov neobmedzujúcich sa len na dôvody národnej bezpečnosti) za nevhodné (príloha 1 bod 4 ods. 2 k zákonu o spravodlivosti a bezpečnosti z roku 2013).
([251]) Vysvetľujúci rámec Spojeného kráľovstva oddiel H s názvom National Security (Národná bezpečnosť), s. 43.
([252]) § 94 ods. 11 zákona o ochrane údajov z roku 2018.
([253]) § 99 ods. 4 zákona o ochrane údajov z roku 2018.
([254]) § 169 zákona o ochrane údajov z roku 2018 umožňuje uplatnenie si nároku osobám, ktoré utrpeli škodu v dôsledku porušenia požiadavky právnych predpisov o ochrane údajov.
([255]) § 169 ods. 5 zákona o ochrane údajov z roku 2018.
([256]) Pozri § 65 ods. 2 písm. b) zákona o regulácii vyšetrovacích právomocí z roku 2000.
([257]) Podľa prílohy 3 k zákonu o regulácii vyšetrovacích právomocí z roku 2000 musia členovia tribunálu mať konkrétne skúsenosti v súdnictve a musia byť oprávnení na opätovné vymenovanie.
([258]) Pokiaľ ide o tzv. Address, pozri poznámku pod čiarou č. 183.
([259]) Príloha 3 bod 1 ods. 5 k zákonu o regulácii vyšetrovacích právomocí z roku 2000.
([260]) § 65 ods. 4 zákona o regulácii vyšetrovacích právomocí z roku 2000.

napadnuteľných okolností ([261]) alebo bolo vykonané spravodajskými službami alebo v ich mene ([262]). Keďže najmä tento štandard „presvedčenia“ bol vykladaný pomerne široko ([263]), podanie návrhu na tento tribunál podlieha pomerne nízkym požiadavkám na aktívnu legitimáciu.

(152) Ak sa tribunál pre kontrolu vyšetrovacích právomocí zaoberá sťažnosťou, ktorá mu bola predložená, je jeho povinnosťou preskúmať, či osoby, voči ktorým sťažnosť smeruje, vyvíjali určité aktivity vo vzťahu k sťažovateľovi, ako aj vyšetriť orgán, ktorý sa údajne dopustil porušenia a či k údajnej aktivite došlo ([264]). Tribunál je povinný v rámci svojho konania uplatniť pri rozhodovaní v tomto konaní rovnaké zásady, aké by uplatnil súd v prípade návrhu na súdne preskúmanie ([265]).

(153) Tribunál musí sťažovateľovi oznámiť, či bolo rozhodnuté v jeho prospech ([266]). Podľa § 67 ods. 6 a 7 zákona o regulácii vyšetrovacích právomocí z roku 2000 má tribunál právomoc vydať predbežné uznesenie a vydať akékoľvek rozhodnutie o náhrade škody alebo iné rozhodnutie, ktoré považuje za vhodné ([267]). Podľa § 67A zákona o regulácii vyšetrovacích právomocí z roku 2000 možno proti rozhodnutiu tribunálu podať odvolanie s výhradou povolenia udeleného tribunálom alebo príslušným odvolacím súdom.

(154) Jednotlivci môžu podať žalobu – a dosiahnuť nápravu – na tribunáli pre kontrolu vyšetrovacích právomocí v prípade, že sa domnievajú, že určitý verejný orgán konal (alebo navrhuje konať) spôsobom, ktorý je nezlučiteľný s právami podľa EDĽP vrátane práva na súkromie a ochranu údajov, a takéto konanie je preto nezákonné podľa § 6 ods. 1 zákona o ľudských právach z roku 1998. Tribunálu pre kontrolu vyšetrovacích právomocí bola udelená výlučná právomoc pre všetky žaloby opierajúce sa o zákon o ľudských právach vo vzťahu k spravodajským službám. To znamená, ako uviedol Vrchný súd (High Court), že to, „či došlo k porušeniu zákona o ľudských právach v súvislosti so skutkovými okolnosťami konkrétneho prípadu, je niečo, čo môže v zásade prerokovať a rozhodnúť nezávislý súd, ktorý môže mať prístup ku všetkým relevantným materiálom vrátane tajných materiálov. […] V tejto súvislosti berieme do úvahy aj to, že aj na tribunál pre kontrolu vyšetrovacích právomocí sa teraz vzťahuje možnosť podať odvolanie na príslušný odvolací súd [v Anglicku a Walese by to bol odvolací súd (Court of Appeal)], pričom najvyšší súd (Supreme Court) nedávno rozhodol, že tribunál pre kontrolu vyšetrovacích právomocí v zásade podlieha súdnemu preskúmaniu: pozri R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219“ ([268]). Ak tribunál zistí, že akýkoľvek akt orgánu verejnej moci je nezákonný, môže v rámci svojich právomocí nariadiť akúkoľvek nápravu alebo vydať akýkoľvek príkaz, ktoré považuje za vhodné a primerané ([269]).

([261]) Takéto okolnosti sa týkajú konania orgánov verejnej moci, ku ktorému dochádza pri výkone právomoci (napr. príkaz, povolenie na získanie komunikácie alebo oznámenie s cieľom získať ju atď.), resp. ak sú okolnosti také, že (bez ohľadu na to, či takáto právomoc existuje), by nebolo náležité, ak by sa dané konanie uskutočňovalo bez nej, alebo prinajmenšom bez toho, aby sa náležite zvážilo, či by daný verejný orgán nemal takouto právomocou disponovať. Konanie povolené Komisárom pre justíciu sa považuje za konania uskutočnené za napadnuteľných okolností [§ 65 (7ZA) zákona o regulácii vyšetrovacích právomocí z roku 2000], zatiaľ čo iné konania, ku ktorým dochádza so súhlasom osoby vykonávajúcej sudcovskú funkciu, sa považujú za také, ku ktorým nedošlo za napadnuteľných okolností (§ 65 ods. 7 a 8 zákona o regulácii vyšetrovacích právomocí z roku 2000).

([262]) Podľa informácií, ktoré poskytli orgány Spojeného kráľovstva, nízke požiadavky na podanie sťažnosti vedú k tomu, že nie je nezvyčajné, aby sa po súdnom prešetrovaní dospelo k záveru, že sťažovateľ nebol nikdy predmetom vyšetrovania zo strany orgánu verejnej moci. V najnovšej štatistickej správe tribunálu pre kontrolu vyšetrovacích právomocí sa uvádza, že v roku 2016 dostal tento tribunál 209 sťažností, 52 % z nich bolo považovaných za zjavne neopodstatnené alebo šikanujúce sťažnosti a 25 % bolo uzavretých „bez určenia“. Orgány Spojeného kráľovstva vysvetlili, že to znamená, že vo vzťahu k sťažovateľovi nebola realizovaná žiadna utajená činnosť ani právomoci, resp. že boli použité utajené prostriedky, ale tribunál dospel k záveru, že sa tak stalo v súlade so zákonom. Ďalších 11 % bolo vylúčených z dôvodu chýbajúcej právomoci, stiahnutých alebo neplatných, 5 % bolo vylúčených z dôvodu premeškania lehoty na podanie sťažnosti a 7 % bolo uzavretých v prospech sťažovateľa. Štatistická správa tribunálu pre kontrolu vyšetrovacích právomocí z roku 2016 je k dispozícii na tomto odkaze: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([263]) Pozri vec Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. V tomto prípade tribunál pre kontrolu vyšetrovacích právomocí s odvolaním sa na judikatúru ESĽP rozhodol, že kritériom, pokiaľ ide o overenie existencie presvedčenia, že akékoľvek konanie spadajúce pod § 68 ods. 5 zákona o regulácii vyšetrovacích právomocí z roku 2000 bolo vykonané niektorou zo spravodajských služieb alebo v ich mene, je to, či existuje nejaký základ pre takéto presvedčenie vrátane skutočnosti, že jednotlivec môže tvrdiť, že je obeťou porušenia spôsobeného samotnou existenciou utajovaných opatrení alebo právnych predpisov umožňujúcich utajované opatrenia iba vtedy, ak je tento jednotlivec schopný preukázať, že vzhľadom na jeho osobnú situáciu je potenciálne vystavený riziku, že bude podrobený takýmto opatreniam (pozri rozsudok Human Rights Watch/Secretary of State, bod 41).

([264]) § 67 ods. 3 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([265]) § 67 ods. 2 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([266]) § 68 ods. 4 zákona o regulácii vyšetrovacích právomocí z roku 2000.

([267]) Môže to zahŕňať aj príkaz na zničenie akýchkoľvek záznamov informácií, ktoré má ktorýkoľvek orgán verejnej moci v súvislosti s ktoroukoľvek osobou.

([268]) High Court of Justice, Liberty, [2019] EWHC 2057 (Admin), bod 170.

([269]) § 8 ods. 1 zákona o ľudských právach z roku 1998.

(155) Jednotlivec môže za porušenie práv zaručených EDĽP vrátane práva na súkromie a ochranu údajov po vyčerpaní vnútroštátnych prostriedkov nápravy dosiahnuť nápravu pred Európskym súdom pre ľudské práva.

(156) Z uvedeného vyplýva, že poskytnutie údajov prenášaných podľa tohto rozhodnutia orgánmi Spojeného kráľovstva príslušnými na presadzovanie trestného práva iným orgánom verejnej moci vrátane spravodajských služieb je ohraničené obmedzeniami a podmienkami zabezpečujúcimi, že takéto ďalšie poskytnutie bude potrebné a primerané a bude podliehať osobitným zárukám ochrany údajov podľa zákona o ochrane údajov z roku 2018. Okrem toho na spracúvanie údajov dotknutými orgánmi verejnej moci dohliadajú nezávislé orgány a dotknutí jednotlivci majú prístup k účinným prostriedkom súdnej nápravy.

3. ZÁVER

(157) Komisia sa domnieva, že v časti 3 zákona o ochrane údajov z roku 2018 sa zabezpečuje úroveň ochrany osobných údajov prenášaných príslušnými orgánmi v Únii na účely presadzovania trestného práva príslušným orgánom Spojeného kráľovstva, ktorá je v zásade rovnocenná s úrovňou zaručenou smernicou (EÚ) 2016/680.

(158) Komisia sa okrem toho domnieva, že mechanizmy dohľadu a možnosti získania nápravy v právnom poriadku Spojeného kráľovstva umožňujú ako celok v praxi odhaliť a postihnúť porušovanie a poskytujú dotknutej osobe právne prostriedky nápravy na získanie prístupu k osobným údajom, ktoré sa jej týkajú, a prípadne aj na dosiahnutie opravy alebo vymazania takýchto údajov.

(159) Komisia sa napokon na základe dostupných informácií o právnom poriadku Spojeného kráľovstva domnieva, že akýkoľvek zásah do základných práv jednotlivcov, ktorých osobné údaje do Spojeného kráľovstva prenášajú verejné orgány Spojeného kráľovstva z Európskej únie na účely verejného záujmu, a to aj v súvislosti s výmenou osobných údajov medzi orgánmi presadzovania práva a inými orgánmi verejnej moci, ako sú vnútroštátne bezpečnostné orgány, sa obmedzí na to, čo je nevyhnutne potrebné na dosiahnutie dotknutého legitímneho cieľa, a že existuje účinná právna ochrana proti takémuto zásahu.

(160) Preto by sa malo rozhodnúť, že Spojené kráľovstvo zabezpečuje primeranú úroveň ochrany v zmysle článku 36 ods. 2 smernice (EÚ) 2016/680 vykladaného so zreteľom na Chartu základných práv.

(161) Tento záver vychádza tak z príslušného vnútroštátneho režimu Spojeného kráľovstva, ako aj z jeho medzinárodných záväzkov, najmä z dodržiavania Európskeho dohovoru o ľudských právach a z podriadenia sa právomoci Európskeho súdu pre ľudské práva. Pretrvávajúce dodržiavanie týchto medzinárodných záväzkov je preto mimoriadne dôležitým prvkom posúdenia, na ktorom sa zakladá toto rozhodnutie.

4. ÚČINKY TOHTO ROZHODNUTIA A KONANIE ORGÁNOV PRE OCHRANU ÚDAJOV

(162) Členské štáty a ich orgány sú povinné prijať opatrenia potrebné na dosiahnutie súladu s aktmi inštitúcií Únie, lebo tieto akty požívajú prezumpciu zákonnosti a majú z tohto dôvodu právne účinky dovtedy, kým neuplynie ich platnosť, kým nie sú derogované, zrušené v konaní o žalobe o neplatnosť alebo vyhlásené za neplatné v nadväznosti na návrh na začatie prejudiciálneho konania alebo námietku nezákonnosti.

(163) Rozhodnutie Komisie o primeranosti prijaté podľa článku 36 ods. 3 smernice (EÚ) 2016/680 je preto záväzné pre všetky orgány členských štátov, ktorým je určené, vrátane ich nezávislých dozorných orgánov. Najmä počas obdobia uplatňovania tohto rozhodnutia sa prenosy od prevádzkovateľa alebo sprostredkovateľa v Únii k prevádzkovateľom alebo sprostredkovateľom v Spojenom kráľovstve môžu uskutočniť bez toho, aby bolo potrebné získať akékoľvek ďalšie povolenie.

(164) Zároveň treba pripomenúť, že podľa článku 47 ods. 5 smernice (EÚ) 2016/680 a ako Súdny dvor ozrejmil v rozsudku vo veci Schrems, ak vnútroštátny orgán na ochranu údajov spochybňuje, a to aj na základe sťažnosti, zlučiteľnosť rozhodnutia Komisie o primeranosti so základnými právami jednotlivca na súkromie a ochranu údajov, vnútroštátne právo mu musí poskytnúť právny prostriedok nápravy umožňujúci uplatniť tieto výhrady na vnútroštátnom súde, ktorý môže mať povinnosť podať návrh na začatie prejudiciálneho konania na Súdnom dvore ([270]).

([270]) Schrems, bod 65.

5. MONITOROVANIE, POZASTAVENIE, ZRUŠENIE ALEBO ZMENA TOHTO ROZHODNUTIA

(165) Podľa článku 36 ods. 4 smernice (EÚ) 2016/680 má Komisia po prijatí tohto rozhodnutia priebežne monitorovať príslušný vývoj v Spojenom kráľovstve, s cieľom posúdiť, či Spojené kráľovstvo stále zabezpečuje v zásade rovnocennú úroveň ochrany. Takéto monitorovanie je v tomto prípade osobitne dôležité, keďže Spojené kráľovstvo bude spravovať, uplatňovať a presadzovať nový režim ochrany údajov, ktorý už nepodlieha právu Únie a ktorý sa môže vyvíjať. V tejto súvislosti sa bude osobitná pozornosť venovať praktickému uplatňovaniu pravidiel Spojeného kráľovstva o prenosoch osobných údajov do tretích krajín, a to aj prostredníctvom uzatvárania medzinárodných dohôd, a dosahu, ktorý tento prenos môže mať na úroveň ochrany poskytovanej údajom prenášaným na základe tohto rozhodnutia, ako aj účinnosti uplatňovania individuálnych práv v oblastiach, na ktoré sa vzťahuje toto rozhodnutie. Monitorovanie Komisie bude okrem iných prvkov vychádzať z informácií o vývoji judikatúry a dohľade zo strany Komisára pre informácie a ďalších nezávislých orgánov.

(166) V záujme tohto monitorovania by mali orgány Spojeného kráľovstva bezodkladne a pravidelne informovať Komisiu o každej podstatnej zmene právneho poriadku Spojeného kráľovstva, ktorá má vplyv na právny rámec, ktorý je predmetom tohto rozhodnutia, ako aj o akomkoľvek vývoji postupov týkajúcich sa spracúvania osobných údajov posudzovaných v tomto rozhodnutí, a to najmä pokiaľ ide o prvky uvedené v odôvodnení (165).

(167) Navyše, aby Komisia mohla účinne vykonávať svoju monitorovaciu funkciu, mali by ju členské štáty informovať o všetkých relevantných opatreniach, ktoré prijali vnútroštátne orgány pre ochranu údajov, najmä pokiaľ ide o otázky alebo sťažnosti dotknutých osôb z EÚ týkajúce sa prenosu osobných údajov z Únie príslušným orgánom v Spojenom kráľovstve. Komisia by mala byť informovaná aj o akýchkoľvek známkach toho, že opatrenia orgánov verejnej moci Spojeného kráľovstva zodpovedných za predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie vrátane akýchkoľvek dozorných orgánov nezabezpečujú požadovanú úroveň ochrany.

(168) Ak dostupné informácie, najmä informácie vyplývajúce z monitorovania tohto rozhodnutia alebo poskytnuté orgánmi Spojeného kráľovstva alebo členských štátov, odhalia, že úroveň ochrany poskytovaná Spojeným kráľovstvom už nemusí byť primeraná, Komisia by o tom mala informovať príslušné orgány Spojeného kráľovstva a požiadať o prijatie náležitých opatrení v určenej lehote, ktorá nesmie presiahnuť tri mesiace. Táto lehota sa môže predĺžiť v prípade potreby o určený čas, a to pri zohľadnení povahu príslušnej záležitosti a/alebo opatrenia, ktoré majú byť prijaté.

(169) Ak po uplynutí uvedenej stanovenej lehoty príslušné orgány Spojeného kráľovstva neprijmú takéto opatrenia alebo inak uspokojivo nepreukážu, že toto rozhodnutie sa naďalej zakladá na primeranej úrovni ochrany, Komisia začne postup uvedený v článku 58 ods. 2 smernice (EÚ) 2016/680 s cieľom čiastočne alebo úplne pozastaviť alebo zrušiť toto rozhodnutie.

(170) Alternatívne Komisia začne postup s cieľom zmeniť toto rozhodnutie, najmä podriadením prenosu údajov dodatočným podmienkam alebo obmedzením rozsahu konštatovanej primeranosti len na tie prenosy údajov, pri ktorých je naďalej zabezpečená primeraná úroveň ochrany.

(171) Komisia využije z riadne odôvodnených vážnych a naliehavých dôvodov možnosť prijať v súlade s postupom uvedeným v článku 58 ods. 3 smernice (EÚ) 2016/680 okamžite uplatniteľné vykonávacie akty, ktorými sa pozastaví, zruší alebo zmení toto rozhodnutie.

6. OBDOBIE PLATNOSTI TOHTO ROZHODNUTIA A PREDĹŽENIE JEHO PLATNOSTI

(172) Malo by sa zohľadniť, že po skončení prechodného obdobia stanoveného v dohode o vystúpení a hneď, ako sa prestane uplatňovať dočasné ustanovenie podľa článku 782 Dohody o obchode a spolupráci medzi EÚ a Spojeným kráľovstvom, bude Spojené kráľovstvo v porovnaní s režimom uplatňovaným v čase, keď bolo viazané právom Európskej únie, spravovať, uplatňovať a presadzovať nový režim ochrany údajov. Môže to zahŕňať najmä zmeny rámca ochrany údajov, ktorý bol predmetom posúdenia v tomto rozhodnutí, ako aj ďalší relevantný vývoj.

(173) Preto je vhodné stanoviť, že toto rozhodnutie sa bude uplatňovať počas obdobia štyroch rokov od nadobudnutia jeho účinnosti.

(174) Ak najmä z informácií vyplývajúcich z monitorovania tohto rozhodnutia vyplynie, že zistenia týkajúce sa primeranosti úrovne ochrany zabezpečenej v Spojenom kráľovstve sú stále fakticky a právne odôvodnené, Komisia by mala najneskôr šesť mesiacov pred skončením uplatňovania tohto rozhodnutia začať postup na zmenu tohto rozhodnutia predĺžením jeho časovej pôsobnosti v zásade o ďalšie štyri roky. Akýkoľvek vykonávací akt, ktorým sa mení toto rozhodnutie, sa má prijať v súlade s postupom uvedeným v článku 58 ods. 2 smernice (EÚ) 2016/680.

7. **ZÁVEREČNÉ ÚVAHY**

(175) Európsky výbor pre ochranu údajov zverejnil svoje stanovisko ([271]), ktoré bolo zohľadnené pri príprave tohto rozhodnutia.

(176) Opatrenia stanovené v tomto rozhodnutí sú v súlade so stanoviskom výboru zriadeného podľa článku 58 smernice (EÚ) 2016/680.

(177) V súlade s článkom 6a Protokolu č. 21 o postavení Spojeného kráľovstva a Írska s ohľadom na priestor slobody, bezpečnosti a spravodlivosti, ktorý je pripojený k ZEÚ a ZFEÚ, Írsko nie je viazané pravidlami stanovenými v smernici (EÚ) 2016/680, a teda ani týmto vykonávacím rozhodnutím, ktoré sa týkajú spracúvania osobných údajov členskými štátmi pri vykonávaní činností, ktoré patria do rozsahu pôsobnosti tretej časti hlavy V kapitoly 4 alebo kapitoly 5 ZFEÚ, ak Írsko nie je viazané pravidlami, ktorými sa spravujú formy justičnej spolupráce v trestných veciach alebo policajnej spolupráce, v rámci ktorých sa musia dodržiavať ustanovenia prijaté na základe článku 16 ZFEÚ. Napokon, podľa vykonávacieho rozhodnutia Rady (EÚ) 2020/1745 ([272]), by sa smernica (EÚ) 2016/680 mala v Írsku stať účinnou a uplatňovať na predbežnom základe od 1. januára 2021. Írsko je preto týmto vykonávacím rozhodnutím viazané, a to za rovnakých podmienok, aké sa vzťahujú na uplatňovanie smernice (EÚ) 2016/680 v Írsku, ako sa stanovuje vo vykonávacom rozhodnutí Rady (EÚ) 2020/1745, pokiaľ ide o schengenské *acquis*, na ktorom sa Írsko zúčastňuje.

(178) V súlade s článkami 2 a 2a Protokolu č. 22 o postavení Dánska, ktorý je pripojený k Zmluve o Európskej únii a Zmluve o fungovaní Európskej únie, Dánsko nie je viazané pravidlami stanovenými v smernici (EÚ) 2016/680, a teda ani týmto vykonávacím rozhodnutím, ani nepodlieha ich uplatňovaniu, ktoré sa týkajú spracúvania osobných údajov členskými štátmi pri vykonávaní činností, ktoré patria do rozsahu pôsobnosti tretej časti hlavy V kapitoly 4 alebo kapitoly 5 ZFEÚ. Vzhľadom na to, že smernica (EÚ) 2016/680 je založená na schengenskom *acquis*, Dánsko v súlade s článkom 4 uvedeného protokolu oznámilo 26. októbra 2016 svoje rozhodnutie vykonávať smernicu (EÚ) 2016/680. Dánsko je preto v súlade s medzinárodným právom povinné vykonávať toto vykonávacie rozhodnutie.

(179) Pokiaľ ide o Island a Nórsko, toto vykonávacie rozhodnutie predstavuje vývoj ustanovení schengenského *acquis* v zmysle Dohody uzatvorenej medzi Radou Európskej únie a Islandskou republikou a Nórskym kráľovstvom o pridružení týchto dvoch štátov pri vykonávaní, uplatňovaní a rozvoji schengenského *acquis* ([273]).

(180) Pokiaľ ide o Švajčiarsko, toto vykonávacie rozhodnutie predstavuje vývoj ustanovení schengenského *acquis* v zmysle Dohody medzi Európskou úniou, Európskym spoločenstvom a Švajčiarskou konfederáciou o pridružení Švajčiarskej konfederácie k vykonávaniu, uplatňovaniu a vývoju schengenského *acquis* ([274]).

(181) Pokiaľ ide o Lichtenštajnsko, toto vykonávacie rozhodnutie predstavuje vývoj ustanovení schengenského *acquis* v zmysle Protokolu medzi Európskou úniou, Európskym spoločenstvom, Švajčiarskou konfederáciou a Lichtenštajnským kniežatstvom o pristúpení Lichtenštajnského kniežatstva k Dohode medzi Európskou úniou, Európskym spoločenstvom a Švajčiarskou konfederáciou o pridružení Švajčiarskej konfederácie k vykonávaniu, uplatňovaniu a vývoju schengenského *acquis* ([275]).

([271]) Stanovisko č. 15/2021 k návrhu vykonávacieho rozhodnutia Európskej komisie podľa smernice (EÚ) 2016/680 o primeranej ochrane osobných údajov v Spojenom kráľovstve, k dispozícii na tomto odkaze: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Vykonávacie rozhodnutie Rady (EÚ) 2020/1745 z 18. novembra 2020 o nadobudnutí účinnosti ustanovení schengenského acquis týkajúcich sa ochrany údajov a o predbežnom nadobudnutí účinnosti určitých ustanovení schengenského acquis v Írsku (Ú. v. EÚ L 393, 23.11.2020, s. 3).

([273]) Ú. v. ES L 176, 10.7.1999, s. 36.

([274]) Ú. v. EÚ L 53, 27.2.2008, s. 52.

([275]) Ú. v. EÚ L 160, 18.6.2011, s. 21.

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Na účely článku 36 smernice (EÚ) 2016/680 Spojené kráľovstvo zabezpečuje primeranú úroveň ochrany osobných údajov prenášaných z Európskej únie orgánom verejnej moci Spojeného kráľovstva zodpovedným za predchádzanie trestným činom, ich vyšetrovanie, odhaľovanie alebo stíhanie, resp. na účely výkonu trestných sankcií.

Článok 2

Vždy, keď príslušné dozorné orgány v členských štátoch uplatnia svoje právomoci podľa článku 47 smernice (EÚ) 2016/680, aby ochránili fyzické osoby v súvislosti so spracúvaním ich osobných údajov, pokiaľ ide o prenosy údajov orgánom verejnej moci v Spojenom kráľovstve v rozsahu pôsobnosti stanovenom v článku 1, dotknutý členský štát o tejto skutočnosti bezodkladne informuje Komisiu.

Článok 3

1. Komisia nepretržite monitoruje uplatňovanie právneho rámca, z ktorého vychádza toto rozhodnutie, vrátane podmienok, za ktorých sa uskutočňujú následné prenosy a uplatňujú individuálne práva, s cieľom posúdiť, či Spojené kráľovstvo naďalej zabezpečuje primeranú úroveň ochrany v zmysle článku 1.

2. Členské štáty a Komisia sa vzájomne informujú o prípadoch, v ktorých Komisár pre informácie alebo akýkoľvek iný príslušný orgán Spojeného kráľovstva nezabezpečuje dodržiavanie právneho rámca, na ktorom je založené toto rozhodnutie.

3. Členské štáty a Komisia sa vzájomne informujú o všetkých náznakoch toho, že zásahy orgánov verejnej moci Spojeného kráľovstva do práva fyzických osôb na ochranu ich osobných údajov prekračujú rámec toho, čo je nevyhnutne potrebné, alebo že neexistuje účinná právna ochrana pred takými zásahmi.

4. Ak má Komisia informácie o tom, že primeraná úroveň ochrany už nie je zabezpečená, informuje o tom príslušné orgány Spojeného kráľovstva a môže pozastaviť, zrušiť alebo zmeniť toto rozhodnutie.

5. Komisia môže toto rozhodnutie pozastaviť, zrušiť alebo zmeniť ak nedostatočná spolupráca vlády Spojeného kráľovstva bráni Komisii určiť, či je dotknutý záver uvedený v článku 1.

Článok 4

Toto rozhodnutie stráca účinnosť 27. júna 2025, pokiaľ sa nepredĺži v súlade s postupom uvedeným v článku 58 ods. 2 smernice (EÚ) 2016/680.

Článok 5

Toto rozhodnutie je určené členským štátom.

V Bruseli 28. júna 2021

Za Komisiu
Didier REYNDERS
člen Komisie