Uradni list Evropske unije

L 360

Slovenska izdaja

Zakonodaja

Letnik 64

11. oktober 2021

Vsebina

[1] Besedilo velja za EGP.

SL

Akti z rahlo natisnjenimi naslovi so tisti, ki se nanašajo na dnevno upravljanje kmetijskih zadev in so splošno veljavni za omejeno obdobje.

Naslovi vseh drugih aktov so v mastnem tisku in pred njimi stoji zvezdica.

II

(Nezakonodajni akti)

SKLEPI

IZVEDBENA UREDBA KOMISIJE (EU) 2021/1772

z dne 28. junija 2021

v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu

(notificirano pod dokumentarno številko C(2021) 4800)

(Besedilo velja za EGP)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) ([1]), zlasti njenega člena 45(3),

ob upoštevanju naslednjega:

1. UVOD

(1) Uredba (EU) 2016/679 določa pravila o prenosu osebnih podatkov od upravljavcev ali obdelovalcev v Evropski uniji v tretje države in mednarodne organizacije, če taki prenosi spadajo na področje uporabe navedene uredbe. Pravila o mednarodnih prenosih podatkov so določena v poglavju V navedene uredbe, natančneje v členih 44 do 50. Pretok osebnih podatkov v države zunaj Evropske unije in iz njih je ključen za širitev mednarodnega sodelovanja in čezmejne trgovine, vendar je treba zagotoviti, da s takimi prenosi v tretje države ni ogrožena raven varstva osebnih podatkov, ki se zagotavlja v Evropski uniji ([2]).

(2) V skladu s členom 45(3) Uredbe (EU) 2016/679 lahko Komisija z izvedbenim aktom odloči, da tretja država, ozemlje ali en oziroma več določenih sektorjev v zadevni tretji državi ali mednarodna organizacija zagotavljajo ustrezno raven varstva. V skladu s temi pogoji se lahko osebni podatki v tretjo državo prenašajo brez dodatnega dovoljenja, kot je določeno v členu 45(1) in uvodni izjavi 103 navedene uredbe.

(3) Kot je navedeno v členu 45(2) Uredbe (EU) 2016/679, mora sprejetje sklepa o ustreznosti temeljiti na celoviti analizi pravnega reda tretje države, kar vključuje pravila, ki se uporabljajo glede uvoznikov podatkov, ter omejitve in zaščitne ukrepe glede dostopa javnih organov do osebnih podatkov. Komisija mora v oceni opredeliti, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, zagotovljeni v Evropski uniji (uvodna izjava 104 Uredbe (EU) 2016/679). Standard, po katerem se ocenjuje dejstvo, da je „v osnovi enakovredna“, je določen v zakonodaji EU, zlasti v Uredbi (EU) 2016/679 in sodni praksi Sodišča Evropske unije ([3]). V tem pogledu je pomemben tudi referenčni dokument Evropskega odbora za varstvo podatkov o ustreznosti ([4]).

([1]) UL L 119, 4.5.2016, str. 1.

([2]) Glej uvodno izjavo 101 Uredbe (EU) 2016/679.

([3]) Glej, nazadnje, sodbo z dne 16. julija 2020, Facebook Ireland Limited in Schrems (v nadaljnjem besedilu: Schrems II), C-311/18, EU:C:2020:559.

([4]) Referenčni dokument Evropskega odbora za varstvo podatkov o ustreznosti, WP 254 rev. 01, je na voljo na povezavi: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Kot je pojasnilo Sodišče Evropske unije, v ta namen ni treba zagotavljati identične ravni varstva ([5]). To pomeni zlasti, da se lahko sredstva, ki jih zadevna tretja država uporablja za varstvo osebnih podatkov, razlikujejo od tistih, ki jih uporablja Evropska unija, če se v praksi izkaže, da so učinkovita pri zagotavljanju ustrezne ravni varstva ([6]). Standard ustreznosti torej ne zahteva dobesednega prepisa pravil Unije. Bolj kot to preskus temelji na proučitvi, ali tuji sistem kot celota prek vsebine pravic do varstva podatkov ter njihovega učinkovitega izvajanja, nadzora in izvrševanja zagotavlja zahtevano raven varstva ([7]).

(5) Komisija je skrbno analizirala zakonodajo in prakso Združenega kraljestva. Na podlagi ugotovitev iz uvodnih izjav (8) do (270) Komisija ugotavlja, da Združeno kraljestvo zagotavlja ustrezno raven varstva osebnih podatkov, ki se v okviru Uredbe (EU) 2016/679 prenašajo iz Evropske unije v Združeno kraljestvo.

(6) Ta ugotovitev se ne nanaša na osebne podatke, ki se prenašajo za namene nadzora priseljevanja v Združeno kraljestvo ali ki sicer spadajo na področje uporabe izjeme glede nekaterih pravic posameznikov, na katere se nanašajo osebni podatki, za namene vzdrževanja učinkovitega nadzora priseljevanja (v nadaljnjem besedilu: izjema glede priseljevanja) v skladu z odstavkom 4(1) dodatka 2 k zakonu Združenega kraljestva o varstvu podatkov. Veljavnost in razlaga izjeme glede priseljevanja v skladu s pravom Združenega kraljestva po odločbi sodišča England and Wales Court of Appeal z dne 26. maja 2021 nista določeni. Ob priznavanju, da se pravice posameznikov, na katere se nanašajo osebni podatki, načeloma lahko omejijo za namene nadzora priseljevanja kot „pomemben vidik javnega interesa“, je sodišče Court of Appeal odločilo, da je izjema glede priseljevanja v sedanji obliki nezdružljiva s pravom Združenega kraljestva, saj zakonodajni ukrep ne vsebuje posebnih določb, ki bi določale zaščitne ukrepe iz člena 23(2) splošne uredbe o varstvu podatkov, kakor se uporablja v Združenem kraljestvu (v nadaljnjem besedilu: UK GDPR) ([8]). Pod temi pogoji bi bilo treba prenose osebnih podatkov iz Unije v Združeno kraljestvo, za katere se lahko uporabi izjema glede priseljevanja, izključiti s področja uporabe tega sklepa ([9]). Ko bo nezdružljivost z zakonodajo Združenega kraljestva odpravljena, bi bilo treba ponovno oceniti izjemo glede priseljevanja in potrebo po ohranitvi omejitve področja uporabe te odločbe.

(7) Ta sklep ne bi smel vplivati na neposredno uporabo Uredbe (EU) 2016/679 s strani organizacij, ustanovljenih v Združenem kraljestvu, če so izpolnjeni pogoji glede ozemeljske veljavnosti iz člena 3 navedene uredbe.

2. PRAVILA, KI SE UPORABLJAJO ZA OBDELAVO OSEBNIH PODATKOV

2.1 Ustavni okvir

(8) Združeno kraljestvo je parlamentarna demokracija, katere vodja je ustavni monarh. Ima neodvisen parlament, ki je nadrejen vsem drugim vladnim institucijam, izvršilno vejo oblasti, ki izhaja iz parlamenta in je temu tudi odgovorna, ter neodvisno sodstvo. Izvršilna veja oblasti, katere pristojnosti temeljijo na zmožnosti, da uživa zaupanje izvoljenega spodnjega doma parlamenta Združenega kraljestva, je odgovorna obema domovoma parlamenta, ki sta odgovorna za pregled dela vlade ter razpravo o zakonih in njihovo sprejemanje.

([5]) Sodba z dne 6. oktobra 2015, Schrems (v nadaljnjem besedilu: Schrems I), C-362/14, EU:C:2015:650, točka 73.

([6]) Sodba v zadevi Schrems I, točka 74.

([7]) Glej Sporočilo Komisije Evropskemu parlamentu in Svetu: Izmenjava in varstvo osebnih podatkov v globaliziranem svetu (COM (2017) 7, 10.1.2017, oddelek 3.1, str. 6), na voljo na povezavi: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

([8]) Court of Appeal (Civil Division), Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport, [2021] EWCA Civ 800, odstavki 53 do 56. Sodišče Court of Appeal je razveljavilo odločitev sodišča High Court of Justice, ki je predhodno presodilo izjemo glede na Uredbo (EU) 2016/679 (zlasti njen člen 23) in Listino Evropske unije o temeljnih pravicah, in ugotovilo, da je izjema zakonita (Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562).

([9]) Če so izpolnjeni veljavni pogoji, se lahko prenosi za namene nadzora priseljevanja v Združeno kraljestvo izvedejo na podlagi mehanizmov za prenos iz členov 46 do 49 Uredbe (EU) 2016/679.

(9) Parlament Združenega kraljestva je pravice za sprejemanje zakonodaje o lokalnih vprašanjih na Škotskem, v Walesu in na Severnem Irskem, ki jih ni zadržal zase, prenesel na škotski parlament, valižanski parlament (Senedd Cymru) in skupščino Severne Irske. Vprašanje varstva podatkov ni delegirano, tj. ista zakonodaja se uporablja po vsej državi, druga področja politike, ki se nanašajo na ta sklep, pa so delegirana. Urejanje sistemov kazenskega pravosodja na Škotskem in Severnem Irskem, vključno s policijskim delom, je na primer delegirano škotskemu parlamentu oziroma skupščini Severne Irske. Združeno kraljestvo nima kodificirane ustave v smislu uzakonjenega konstitutivnega dokumenta. Ustavna načela so se razvijala počasi, zlasti na podlagi sodne prakse in običajev. Sodišča so priznala ustavnopravno vrednost nekaterih listin, kot so Magna Carta, Bill of Rights iz leta 1689 in zakon o človekovih pravicah iz leta 1998 (Human Rights Act 1998). Kot del ustave so se z občim pravom, navedenimi listinami in mednarodnimi pogodbami, zlasti Evropsko konvencijo o varstvu človekovih pravic, ki jo je Združeno kraljestvo ratificiralo leta 1951, razvile temeljne pravice posameznikov. Združeno kraljestvo je leta 1987 ratificiralo tudi Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) ([10]).

(10) Z zakonom o človekovih pravicah iz leta 1998 so pravice iz Evropske konvencije o varstvu človekovih pravic vključene v pravo Združenega kraljestva. Zakon o človekovih pravicah vsakemu posamezniku zagotavlja temeljne pravice in svoboščine iz členov 2 do 12 in člena 14 Evropske konvencije o varstvu človekovih pravic, iz členov 1, 2 in 3 Protokola št. 1 te konvencije ter člena 1 Protokola št. 13 te konvencije, v povezavi s členi 16, 17 in 18 navedene konvencije. To vključuje pravico do spoštovanja zasebnega in družinskega življenja (ter pravico do varstva podatkov, ki je del te pravice) in pravico do poštenega sojenja ([11]). Natančneje, v skladu s členom 8 navedene konvencije se lahko javna oblast vmešava v izvrševanje pravice do zasebnosti le, če je to določeno z zakonom, kadar je to nujno v demokratični družbi zaradi državne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.

(11) V skladu z zakonom o človekovih pravicah iz leta 1998 mora biti vsak ukrep javnih organov združljiv s pravico, ki jo zagotavlja konvencija ([12]). Poleg tega je treba primarno in sekundarno zakonodajo razumeti in izvajati tako, da sta združljivi s pravicami iz konvencije ([13]).

2.2 **Okvir varstva podatkov v Združenem kraljestvu**

(12) Združeno kraljestvo je 31. januarja 2020 izstopilo iz Evropske unije. Na podlagi Sporazuma o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo ([14]) se je v Združenem kraljestvu v prehodnem obdobju do 31. decembra 2020 še naprej uporabljalo pravo Unije. Pred izstopom in v prehodnem obdobju sta zakonodajni okvir o varstvu osebnih podatkov v Združenem kraljestvu sestavljali relevantna zakonodaja EU (zlasti Uredba (EU) 2016/679 in Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta ([15])) in nacionalna zakonodaja, zlasti zakon o varstvu podatkov iz leta 2018 (DPA 2018) ([16]), ki vsebuje nacionalna pravila, kadar to omogoča Uredba (EU) 2016/679, pri čemer opredeljuje in omejuje uporabo pravil Uredbe (EU) 2016/679 ter prenaša Direktivo (EU) 2016/680 v nacionalno zakonodajo.

([10]) Načela Konvencije št. 108 so bila sprva prenesena v pravo Združenega kraljestva prek zakona o varstvu podatkov iz leta 1984 (Data Protection Act of 1984), ki ga je nadomestil zakon o varstvu podatkov iz leta 1998, nato pa zakon o varstvu podatkov iz leta 2018 (v povezavi z UK GDPR). Združeno kraljestvo je leta 2018 podpisalo tudi protokol o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (znan kot Konvencija št. 108+) in trenutno vodi postopek za ratifikacijo konvencije.

([11]) Člena 6 in 8 EKČP (glej tudi dodatek 1 k zakonu o človekovih pravicah iz leta 1998).

([12]) Člen 6 zakona o človekovih pravicah iz leta 1998.

([13]) Člen 3 zakona o človekovih pravicah iz leta 1998.

([14]) Sporazum o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo (2019/C 384 I/01, XT/21054/2019/INIT, UL C 384 I, 12.11.2019, str. 1), ki je na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN.

([15]) Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L 119, 4.5.2016, str. 89), na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:02016L0680-20160504&from=EN .

([16]) Zakon o varstvu podatkov iz leta 2018 (Data Protection Act 2018) je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) Za pripravo na izstop iz Evropske unije je vlada Združenega kraljestva sprejela zakon o izstopu iz Evropske unije iz leta 2018 (European Union (Withdrawal) Act 2018) ([17]), ki v zakonodajo Združenega kraljestva vključuje zakonodajo Unije, ki se neposredno uporablja ([18]). To ohranjeno pravo EU v celoti vključuje Uredbo (EU) 2016/679, vključno z uvodnimi določbami ([19]). V skladu z navedenim zakonom morajo sodišča v Združenem kraljestvu nespremenjeno ohranjeno pravo EU razlagati v skladu z relevantno sodno prakso Sodišča EU in splošnimi načeli prava Unije, kot ta učinkujejo tik pred iztekom prehodnega obdobja (tako imenovana ohranjena sodna praksa EU in ohranjena splošna načela prava EU) ([20]).

(14) Na podlagi zakona o izstopu iz Evropske unije iz leta 2018 lahko nižji ministri Združenega kraljestva sprejemajo sekundarno zakonodajo v obliki aktov z zakonsko močjo, s katerimi se spreminja ohranjeno pravo EU, kot je potrebno zaradi izstopa Združenega kraljestva iz Evropske unije. To pooblastilo je bilo izvršeno s predpisi o varstvu podatkov, zasebnosti in elektronski komunikaciji (spremembe itd., izstop iz EU) iz leta 2019 (predpisi DPPEC) ([21]). Predpisi DPPEC spreminjajo Uredbo (EU) 2016/679, kakor je bila vključena v pravo Združenega kraljestva na podlagi zakona o izstopu iz Evropske unije iz leta 2018, zakona o varstvu podatkov iz leta 2018 in druge zakonodaje o varstvu podatkov, da ustreza nacionalnemu okviru ([22]).

(15) Posledično po izteku prehodnega obdobja pravni okvir o varstvu osebnih podatkov v Združenem kraljestvu sestavljata:

— UK GDPR, kakor je bila vključena v pravni red Združenega kraljestva na podlagi zakona o izstopu iz Evropske unije iz leta 2018 in spremenjena na podlagi predpisov DPPEC ([23]), ter

— zakon o varstvu podatkov iz leta 2018, kakor je bil spremenjen s predpisi DPPEC ([24]).

(16) Glede na to, da UK GDPR temelji na zakonodaji EU, so pravila o varstvu podatkov v Združenem kraljestvu v številnih primerih zelo podobna ustreznim pravilom, ki se uporabljajo v Evropski uniji.

(17) Poleg pooblastil, ki jih ima pristojni minister na podlagi zakona o izstopu iz Evropske unije iz leta 2018, ima na podlagi več določb zakona o varstvu podatkov iz leta 2018 tudi pristojnost za sprejemanje sekundarne zakonodaje, s katero se spreminjajo nekatere določbe navedenega zakona ali s katero so določena dopolnilna in dodatna pravila ([25]). Pristojni minister je do zdaj uporabil le pooblastila na podlagi člena 137 zakona o varstvu podatkov iz

([17]) Zakon o izstopu iz Evropske unije iz leta 2018, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) Namen in učinek zakona o izstopu iz Evropske unije iz leta 2018 sta, da se vsa zakonodaja Unije, ki se neposredno uporablja in ki je bila ob koncu prehodnega obdobja vključena v pravo Združenega kraljestva, vključi v pravo Združenega kraljestva v obliki, kot učinkuje v pravu EU tik pred koncem prehodnega obdobja; glej člen 3 zakona o izstopu iz Evropske unije iz leta 2018.

([19]) V pojasnjevalnih opombah k zakonu o izstopu iz Evropske unije iz leta 2018 je navedeno: „Kadar se na podlagi tega člena prenaša zakonodaja, del domače zakonodaje postane besedilo same zakonodaje, ki se prenaša. To vključuje celotno besedilo katerega koli instrumenta EU, vključno z uvodnimi izjavami.“ (Pojasnjevalne opombe k zakonu o izstopu iz Evropske unije iz leta 2018, točka 83, ki so na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). V skladu z informacijami, ki so jih predložili organi Združenega kraljestva, velja, da uvodnih izjav ni bilo treba spreminjati tako, kot so bili s predpisi o varstvu podatkov, zasebnosti in elektronskih komunikacijah (spremembe itd., izstop iz EU) (predpisi DPPEC) spremenjeni členi Uredbe (ES) 2016/679, saj uvodne izjave niso zavezujoča pravna pravila.

([20]) Člen 6 zakona o izstopu iz Evropske unije iz leta 2018.

([21]) The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, na voljo na povezavi: https://www.legislation.gov.uk/uksi/2019/419/contents/made, kakor so bili spremenjeni s predpisi DPPEC iz leta 2020, ki so na voljo na povezavi: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Te spremembe UK GDPR in zakona o varstvu podatkov iz leta 2018 so večinoma tehnične narave, na primer črtanje sklicevanja na države članice ali prilagoditev terminologije, npr. zamenjava sklicev na Uredbo (EU) 2016/679 s sklici na UK GDPR. V nekaterih primerih so bile spremembe potrebne, ker odražajo povsem nacionalni okvir določb, na primer glede tega, „kdo“ sprejema „sklepe o ustreznosti“ za zakonodajni okvir Združenega kraljestva o varstvu podatkov (glej člen 17A zakona o varstvu podatkov iz leta 2018), in sicer pristojni minister, ne Evropska komisija.

([23]) Splošna uredba o varstvu podatkov, dodatek Keeling, na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) Zakon o varstvu podatkov iz leta 2018, dodatek Keeling, na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Taka pooblastila vsebujejo na primer člen 16 zakona o varstvu podatkov iz leta 2018 (pristojnost odobriti nadaljnje izjeme od posameznih določb UK GDPR, vendar samo v posebnih, ozko opredeljenih primerih), člen 17A (pristojnost za sprejemanje predpisov o ustreznosti), člena 212 in 213 (pristojnost predlagati zakonodajo in sprejemati prehodne določbe) ter člen 211 (pristojnost sprejemati manjše in posledične spremembe) navedenega zakona.

leta 2018 in sprejel spremembo predpisov o varstvu podatkov, pristojbinah in informacijah iz leta 2019 (Data Protection (Charges and Information) (Amendment) Regulations 2019), ki določajo okoliščine, v katerih morajo upravljavci podatkov plačati letno pristojbino informacijskemu pooblaščencu (Information Commissioner), ki je neodvisni organ za varstvo podatkov v Združenem kraljestvu.

(18) Nazadnje, nadaljnje smernice glede zakonodaje Združenega kraljestva o varstvu podatkov vsebujejo kodeks ravnanja in druge smernice, ki jih je sprejel informacijski pooblaščenec. Čeprav navedene smernice niso uradno pravno zavezujoče, pa so pomembne za razlago in prikazujejo, kako informacijski pooblaščenec v praksi uporablja in izvršuje zakonodajo o varstvu podatkov. Natančneje, na podlagi členov 121 do 125 zakona o varstvu podatkov iz leta 2018 mora informacijski pooblaščenec pripraviti kodekse ravnanja o izmenjavi podatkov, neposrednem trženju, starosti primernem oblikovanju, varstvu podatkov in novinarstvu.

(19) Po svoji strukturi in glavnih sestavinah je pravni okvir Združenega kraljestva, ki se uporablja za podatke, ki se prenašajo na podlagi tega sklepa, torej zelo podoben tistemu, ki se uporablja v Evropski uniji. To vključuje dejstvo, da navedeni okvir ne temelji le na obveznostih iz notranjega prava, na katere je vplivalo pravo EU, temveč tudi na obveznostih, kot so določene v mednarodnem pravu, zlasti s pristopom Združenega kraljestva k EKČP in Konvenciji št. 108, ter njegovem priznavanju pristojnosti Evropskega sodišča za človekove pravice. Te obveznosti, ki izhajajo iz pravno zavezujočih mednarodnih instrumentov, ki se nanašajo zlasti na varstvo osebnih podatkov, so torej še posebno pomemben element pravnega okvira, ki se obravnava v tem sklepu.

2.3 **Stvarno področje uporabe in ozemeljska veljavnost**

(20) Po vzoru Uredbe (EU) 2016/679 se UK GDPR uporablja za obdelavo osebnih podatkov, ki v celoti ali delno poteka avtomatizirano, ali za druge vrste obdelav, če so osebni podatki del zbirke ([26]). Opredelitve pojmov „osebni podatki“, „posameznik, na katerega se nanašajo osebni podatki“ in „obdelava“ so v UK GDPR enaki kot v Uredbi (EU) 2016/679 ([27]). Poleg tega se UK GDPR uporablja za obdelavo neavtomatiziranih in nestrukturiranih osebnih podatkov ([28]), ki jih hranijo nekateri javni organi v Združenem kraljestvu ([29]), čeprav se načela in pravice iz UK GDPR, ki se ne nanašajo na take osebne podatke, na podlagi členov 24 in 25 zakona o varstvu podatkov iz leta 2018 ne uporabljajo. Podobno kot na podlagi Uredbe (EU) 2016/679 tudi na podlagi UK GDPR velja, da se ta ne uporablja, kadar osebne podatke obdeluje fizična oseba zgolj med izvajanjem popolnoma osebne ali domače dejavnosti ([30]).

(21) Področje uporabe UK GDPR vključuje tudi obdelavo v okviru dejavnosti, ki je bila tik pred iztekom prehodnega obdobja zunaj področja uporabe prava Evropske unije (npr. nacionalna varnost) ([31]) ali ki je spadala na področje uporabe poglavja 2 naslova 5 Pogodbe o Evropski uniji (dejavnosti skupne zunanje in varnostne politike) ([32]). Tako kot v sistemu Evropske unije se UK GDPR ne uporablja za obdelavo osebnih podatkov, ki jo izvaja pristojni organ z namenom preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij,

([26]) Člen 2(1) in (5) UK GDPR.

([27]) Člen 4(1) in (2) UK GDPR.

([28]) Neavtomatizirana in nestrukturirana obdelava osebnih podatkov je opredeljena v členu 2(5)(b) kot obdelava osebnih podatkov, pri kateri ne gre za avtomatizirano ali strukturirano obdelavo osebnih podatkov.

([29]) Člen 2(1A) UK GDPR določa, da se zadevna uredba uporablja tudi za neavtomatizirano in nestrukturirano obdelavo osebnih podatkov, ki jih hranijo javni organi, zavezanci za dostop do informacij javnega značaja. Sklic na javne organe, zavezance za dostop do informacij javnega značaja, pomeni vse javne organe, kakor so opredeljeni v zakonu o dostopu do informacij javnega značaja iz leta 2000 (Freedom of Information Act 2000), ali kateri koli škotski javni organ, kakor je opredeljen v škotskem zakonu o dostopu do informacij javnega značaja iz leta 2002 (Freedom of Information (Scotland) Act 2002, škotski uradni list (Acts of the Scottish Parliament) št. 13). Člen 21(5) zakona o varstvu podatkov iz leta 2018.

([30]) Člen 2(2)(a) UK GDPR.

([31]) UK GDPR ureja dejavnosti s področja nacionalne varnosti le, kadar jih ne izvaja pristojni organ za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (v takem primeru se uporablja del 3 zakona o varstvu podatkov iz leta 2018), ali kadar jih ne izvaja obveščevalna služba oziroma se ne izvajajo v njenem imenu, saj so njene dejavnosti izvzete s področja uporabe UK GDPR in jih ureja del 4 zakona o varstvu podatkov iz leta 2018, na podlagi člena 2(2)(c) UK GDPR. Policija lahko na primer izvaja varnostne preglede delavcev in presoja, ali jim je mogoče zaupati dostop do gradiva s področja nacionalne varnosti. Čeprav je policija pristojni organ za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, pa zadevna obdelava ni namenjena temu in UK GDPR se ne uporablja. Glej UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, stran 8, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Člen 2(1)(a) in (b) UK GDPR.

vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem (tako imenovani namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj) – tako obdelavo ureja del 3 zakona o varstvu podatkov iz leta 2018, tako kot Direktiva (EU) 2016/680 v okviru prava Evropske unije – ali za obdelavo osebnih podatkov s strani obveščevalnih služb (varnostna služba (Security Service), tajna obveščevalna služba (Secret Intelligence Service) in vladna obveščevalna služba GCHQ), ki jo ureja del 4 zakona o varstvu podatkov iz leta 2018 ([33]).

(22) Ozemeljska veljavnost UK GDPR je navedena v členu 3 UK GDPR ([34]) in vključuje obdelavo osebnih podatkov (ne glede na to, kje se ta izvaja) v okviru dejavnosti ustanovitve upravljavca ali obdelovalca v Združenem kraljestvu ter obdelavo osebnih podatkov posameznikov, na katere se nanašajo osebni podatki in ki so v Združenem kraljestvu, kadar so dejavnosti obdelave povezane z nudenjem blaga ali storitev takim posameznikom ali s spremljanjem njihovega vedenja ([35]) To odraža pristop iz člena 3 Uredbe (EU) 2016/679.

2.4 **Opredelitev pojma osebni podatki ter pojmov upravljavec in obdelovalec**

(23) V UK GDPR so brez bistvenih posegov ohranjene opredelitve pojmov osebni podatki, obdelava, upravljavec, obdelovalec ter psevdonimizacija iz Uredbe (EU) 2016/679 ([36]). Nadalje, posebne vrste podatkov so v členu 9(1) UK GDPR opredeljene enako kot v Uredbi (EU) 2016/679 („ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo“). Člen 205 zakona o varstvu podatkov iz leta 2018 vsebuje opredelitev pojma „biometričnih podatkov“ ([37]), „podatkov o zdravstvenem stanju“ ([38]) in „genetskih podatkov“ ([39]).

2.5 **Zaščitni ukrepi, pravice in obveznosti**

2.5.1 *Zakonitost in poštenost obdelave*

(24) Osebni podatki se morajo obdelovati zakonito in pošteno.

(25) Načela zakonitosti, poštenosti in preglednosti ter razlogi, na podlagi katerih je obdelava zakonita, so v zakonodaji Združenega kraljestva zagotovljeni na podlagi člena 5(1)(a) in člena 6(1) UK GDPR, ki sta enaka zadevnima določbama iz Uredbe (EU) 2016/679 ([40]). Člen 8 zakona o varstvu podatkov iz leta 2018 dopolnjuje člen 6(1)(e), saj določa, da obdelava osebnih podatkov na podlagi člena 6(1)(e) UK GDPR (ki je potrebna za izvajanje nalog v javnem

([33]) Člen 2(2)(b) in (c) UK GDPR.

([34]) Ista ozemeljska veljavnost se nanaša na obdelavo osebnih podatkov na podlagi dela 2 zakona o varstvu podatkov iz leta 2018, ki dopolnjuje UK GDPR (člen 207(1A)).

([35]) To zlasti pomeni, da se zakon o varstvu podatkov iz leta 2018 in zato ta sklep ne uporabljata za kronske odvisnosti (Jersey, Guernsey in Otok Man) in čezmorska ozemlja Združenega kraljestva, kot so Falklandski otoki in ozemlje Gibraltarja.

([36]) Člen 4(1), (2), (5), (7) in (8) UK GDPR.

([37]) „Biometrični podatki“ pomeni osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki.

([38]) „Podatki o zdravstvenem stanju“ pomeni osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju.

([39]) „Genetski podatki“ pomeni osebne podatke v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika.

([40]) V skladu s členom 6(1) UK GDPR je obdelava zakonita le in v kolikor: (a) je posameznik, na katerega se nanašajo osebni podatki, privolil v obdelavo svojih osebnih podatkov v enega ali več določenih namenov; (b) je obdelava potrebna za izvajanje pogodbe, katere pogodbena stranka je posameznik, na katerega se nanašajo osebni podatki, ali za izvajanje ukrepov na zahtevo takega posameznika pred sklenitvijo pogodbe; (c) je obdelava potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca; (d) je obdelava potrebna za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe; (e) je obdelava potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, ali (f) je obdelava potrebna zaradi zakonitih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali temeljne pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, za katere je potrebno varstvo, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu) vključuje obdelavo osebnih podatkov, ki je potrebna za izvajanje sodne oblasti, izvrševanje nalog spodnjega ali zgornjega doma parlamenta, izvrševanje nalog, za katere je oseba pooblaščena na podlagi pravnega akta ali pravnega pravila, izvrševanje nalog države, nižjega ministra ali vladne službe, ali za izvajanje dejavnosti, ki podpira ali spodbuja demokratično udeležbo.

(26) V zvezi s privolitvijo (enem od razlogov, na podlagi katerih je obdelava zakonita) UK GDPR prav tako ohranja pogoje iz člena 7 Uredbe (EU) 2016/679 nespremenjene, tj. upravljavec mora biti zmožen dokazati, da je posameznik, na katerega se nanašajo osebni podatki, privolil, predložena mora biti pisna zahteva za privolitev v jasnem in preprostem jeziku, posameznik, na katerega se nanašajo osebni podatki, mora imeti pravico, da kadar koli prekliče privolitev, pri ugotavljanju, ali je bila privolitev dana prostovoljno, pa je treba upoštevati, ali je izvajanje pogodbe pogojeno s privolitvijo v obdelavo osebnih podatkov, ki ni potrebna za izvedbo zadevne pogodbe. Poleg tega je v skladu s členom 8 UK GDPR v zvezi z zagotavljanjem storitev informacijske družbe privolitev otroka zakonita le, če je otrok star vsaj 13 let. To spada v starostno mejo iz člena 8 Uredbe (EU) 2016/679.

2.5.2 *Obdelava posebnih vrst osebnih podatkov*

(27) Glede obdelave posebnih vrst podatkov bi morali veljati posebni zaščitni ukrepi.

(28) UK GDPR in zakon o varstvu podatkov iz leta 2018 vsebujeta posebna pravila glede obdelave posebnih vrst osebnih podatkov, ki so v členu 9(1) UK GDPR opredeljeni enako kot v Uredbi (EU) 2016/679 (glej uvodno izjavo (23) above). V skladu s členom 9 UK GDPR je obdelava posebnih vrst podatkov načeloma prepovedana, razen če se uporablja posebna izjema.

(29) Te izjeme (navedene v členu 9(2) in (3) UK GDPR) nikakor ne spreminjajo vsebine člena 9(2) in (3) Uredbe (EU) 2016/679. Razen če je posameznik, na katerega se nanašajo osebni podatki, izrecno privolil v obdelavo navedenih osebnih podatkov, je obdelava posebnih vrst osebnih podatkov dovoljena le v specifičnih in omejenih okoliščinah. V večini primerov mora biti obdelava občutljivih podatkov potrebna zaradi posebnega namena, opredeljenega v zadevni določbi (glej člen 9(2)(b), (c), (f), (g), (h), (i) in (j)).

(30) Poleg tega velja, da kadar izjema na podlagi člena 9(2) UK GDPR zahteva pooblastilo na podlagi zakona ali se nanaša na javni interes, člen 10 zakona o varstvu podatkov iz leta 2018 v povezavi z dodatkom 1 k navedenemu zakonu nadalje določa pogoje, ki morajo biti izpolnjeni za uporabo izjeme. Na primer pri obdelavi občutljivih podatkov za namen varstva javnega zdravja (glej člen 9(2)(i) UK GDPR) točka 3(b) dela 1 dodatka 1 zahteva, da je poleg pogoja preskusa potrebnosti izpolnjen tudi pogoj, da tako obdelavo izvaja „zdravstveni delavec ali da se izvaja v okviru njegove pristojnosti“ ali da jo izvaja „druga oseba, ki je dolžna varovati zaupnost na podlagi pravnega akta ali pravnega pravila“, tudi na podlagi uveljavljene obveznosti varovanja zaupnosti na podlagi občega prava.

(31) Kadar se občutljivi podatki obdelujejo zaradi bistvenega javnega interesa (člen 9(2)(g) UK GDPR), del 2 dodatka 1 k zakonu o varstvu podatkov iz leta 2018 določa izčrpen seznam namenov, ki se lahko štejejo za bistven javni interes, ter za vsakega od navedenih namenov določa posebne dodatne pogoje. Na primer spodbujanje rasne in etnične raznolikosti v višjih ravneh organizacij se šteje za bistven javni interes. Glede obdelave občutljivih podatkov za ta specifični namen veljajo podrobne zahteve, vključno z zahtevo, da se obdelava izvaja kot del postopka identifikacije primernih posameznikov za najvišja mesta, če je treba spodbujati rasno in etnično raznolikost in če ni verjetno, da bi to posamezniku, na katerega se nanašajo osebni podatki, povzročilo znatno škodo ali stisko.

(32) Člen 11(1) zakona o varstvu podatkov iz leta 2018 določa pogoje, na podlagi katerih je mogoče obdelovati osebne podatke v okoliščinah, opisanih v členu 9(3) UK GDPR), ki se nanašajo na ohranjanje tajnosti. To vključuje okoliščine, v katerih obdelavo izvaja zdravstveni ali socialni delavec ali druga oseba, ki mora v zadevnih okoliščinah varovati zaupnost na podlagi pravnega akta ali pravnega pravila, ali kadar se obdelava izvaja v okviru pristojnosti take osebe.

(33) Poleg tega številne izjeme, navedene v členu 9(2) UK GDPR za uporabo zahtevajo ustrezne in specifične zaščitne ukrepe. Odvisno od vrste obdelave in stopnje tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, so s pogoji za obdelavo iz dodatka 1 k zakonu o varstvu podatkov iz leta 2018 vzpostavljeni različni zaščitni ukrepi. Dodatek 1 določa pogoje za vsak primer okoliščin obdelave posamezno.

(34) V nekaterih primerih zakon o varstvu podatkov iz leta 2018 ureja in omejuje vrsto občutljivih podatkov, ki jih je mogoče obdelovati, da se zagotovi skladnost s specifično pravno podlago. Na primer točka 8 dodatka 1 dovoljuje obdelavo občutljivih podatkov za namene spodbujanja enakih možnosti ali enake obravnave. Ta pogoj za obdelavo je mogoče uporabiti le, če podatki razkrivajo raso ali narodnost, versko ali filozofsko prepričanje, spolno usmerjenost ali če gre za podatke o zdravstvenem stanju.

(35) V nekaterih primerih zakon o varstvu podatkov iz leta 2018 omejuje vrsto upravljavca, ki lahko uporablja izjemo glede obdelave. Na primer točka 23 dodatka 1 določa obdelavo občutljivih podatkov v zvezi z odzivi izvoljenih predstavnikov javnosti. Ta izjema glede obdelave se lahko uporabi le, če je upravljavec izvoljeni predstavnik ali druga oseba, ki deluje na podlagi njegovih pristojnosti.

(36) V nekaterih drugih primerih zakon o varstvu podatkov iz leta 2018 glede pogoja obdelave, ki se uporabi, določa omejitve glede kategorij posameznikov, na katere se nanašajo osebni podatki. Na primer točka 21 dodatka 1 ureja obdelavo občutljivih podatkov za namene shem poklicnih pokojnin. Ta pogoj je mogoče uporabiti le, če je zadevni posameznik, na katerega se nanašajo osebni podatki, sorojenec, starš, stari starš ali starš starega starša člana sheme.

(37) Poleg tega velja, da kadar se uporabi izjema iz člena 9(2) UK GDPR, ki je nadalje opredeljena v členu 10 zakona o varstvu podatkov iz leta 2018, v povezavi z dodatkom 1 k navedenemu zakonu, mora upravljavec v večini primerov sestaviti dokument o ustrezni politiki (Appropriate Policy Document). V njem morajo biti orisani postopki upravljavca za zagotavljanje skladnosti z načeli iz člena 5 UK GDPR. Vsebovati mora tudi politike za hrambo in izbris ter navedbo verjetnega obdobja hrambe. Upravljavci morajo navedeni dokument po potrebi pregledati in posodobiti. Upravljavec mora dokument o politiki hraniti še šest mesecev po koncu obdelave in ga predložiti na zahtevo informacijskega pooblaščenca ([41]).

(38) V skladu s točko 41 dodatka 1 k zakonu o varstvu podatkov iz leta 2018 mora biti dokumentu o politiki vedno priložena posodobljena evidenca obdelave. Ta evidenca mora vsebovati zaveze iz dokumenta o politiki, tj. ali se podatki brišejo oziroma hranijo v skladu s politikami. Če se politike ne upoštevajo, mora biti v dnevniku naveden razlog za to. V evidencah mora biti tudi opisano, kako se zagotavlja skladnost obdelave s členom 6 UK GDPR (zakonitost obdelave) in z zadevnimi posebnimi pogoji iz dodatka 1 k zakona o varstvu podatkov iz leta 2018.

(39) Nazadnje, tako kot Uredba (EU) 2016/679 tudi UK GDPR določa splošne zaščitne ukrepe za nekatera dejanja obdelave posebnih vrst podatkov. Člen 35 UK GDPR določa, da mora biti izvedena ocena učinka v zvezi z varstvom podatkov, kadar se v velikem obsegu obdelujejo posebne vrste podatkov. V skladu s členom 37 UK GDPR mora upravljavec ali obdelovalec imenovati pooblaščeno osebo za varstvo podatkov, kadar njegova temeljna dejavnost vključuje obsežno obdelavo posebnih vrst podatkov.

(40) Glede osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški je člen 10 UK GDPR enak členu 10 Uredbe (EU) 2016/679. Ta omogoča obdelavo osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški le pod nadzorom uradnega organa ali če obdelavo dovoljuje notranje pravo, ki zagotavlja ustrezne zaščitne ukrepe za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

(41) Kadar se obdelava podatkov v zvezi s kazenskimi obsodbami in prekrški ne izvaja pod nadzorom uradnega organa, člen 10(5) zakona o varstvu podatkov iz leta 2018 določa, da je taka obdelava mogoča le za posebne namene oziroma v posebnih okoliščinah, navedenih v delih 1, 2 in 3 dodatka 1 k zakonu o varstvu podatkov iz leta 2018, zanjo pa veljajo posebne zahteve, ki so določene za vsakega od navedenih namenov oziroma okoliščin. Podatke o kazenskih obsodbah lahko na primer obdelujejo nepridobitni organi, če (a) obdelavo pri svojih zakonitih dejavnostih z ustreznimi zaščitnimi ukrepi izvaja ustanova, združenje ali drug nepridobitni organ s političnim, filozofskim, verskim ali sindikalnim ciljem in (b) pod pogojem, da (i) se obdelava nanaša samo na člane oziroma nekdanje člane organa ali na osebe, ki so v rednem stiku z njim v zvezi z njegovimi nameni, in (ii) da se podatki ne posredujejo tretji osebi brez privolitve posameznikov, na katere se nanašajo.

([41]) Točke 38 do 40 dodatka 1 k zakonu o varstvu podatkov iz leta 2018.

(42) Nadalje, del 3 dodatka 1 k zakonu o varstvu podatkov iz leta 2018 določa nadaljnje okoliščine, v katerih je mogoče uporabiti podatke o kazenskih obsodbah in ki ustrezajo pravnim razlogom za obdelavo občutljivih podatkov iz člena 9(2) Uredbe (EU) 2016/679 in UK GDPR (npr. privolitev posameznika, na katerega se nanašajo osebni podatki; življenjski interesi takega posameznika, če ta pravno ali fizično ne more izraziti privolitve; če je posameznik, na katerega se nanašajo osebni podatki, te že očitno sam objavil; če je obdelava potrebna za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov itd.).

2.5.3 *Omejitev namena, točnost, najmanjši obseg podatkov, omejitev hrambe in varstvo podatkov*

(43) Osebni podatki bi se morali obdelovati za določen namen in se nato uporabljati samo, če to ni nezdružljivo z namenom obdelave.

(44) To načelo je določeno v členu 5(1)(b) Uredbe (EU) 2016/679 in je nespremenjeno ohranjeno v členu 5(1)(b) UK GDPR. Pogoji nadaljnje združljive obdelave na podlagi člena 6(4) Uredbe (EU) 2016/679 so bili prav tako brez bistvenih sprememb ohranjeni v členu 6(4)(a) do (e) UK GDPR.

(45) Še več, podatki morajo biti točni in po potrebi posodobljeni. Prav tako morajo biti osebni podatki ustrezni in relevantni ter ne smejo presegati namenov, za katere se obdelujejo; načeloma se jih ne sme hraniti dlje, kot je potrebno za namene, za katere se obdelujejo.

(46) Ta načela najmanjšega obsega podatkov, točnosti in omejitve hrambe so opredeljena v členu 5(1)(c) do (e) Uredbe (EU) 2016/679 ter so brez sprememb ohranjena v členu 5(1)(c) do (e) UK GDPR.

(47) Osebni podatki se morajo tudi obdelovati tako, da se zagotavlja njihovo varstvo, vključno z zaščito pred nepooblaščeno ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem. Zato morajo poslovni subjekti sprejeti ustrezne tehnične ali organizacijske ukrepe za varstvo osebnih podatkov pred morebitnimi grožnjami. Navedene ukrepe je treba presojati glede na najsodobnejšo tehnologijo in zadevne stroške.

(48) Varstvo podatkov je v pravu Združenega kraljestva zagotovljeno na podlagi načela celovitosti in zaupnosti iz člena 5(1)(f) UK GDPR ter v členu 32 UK GDPR o varnosti obdelave. Navedene določbe so enake relevantnim določbam v Uredbi (EU) 2016/679. Poleg tega UK GDPR pod enakimi pogoji, kot so določeni v členih 33 in 34 Uredbe (EU) 2016/679, zahteva obveščanje nadzornega organa o kršitvi varstva osebnih podatkov (člen 33 UK GDPR) in sporočilo posamezniku, na katerega se nanašajo osebni podatki, o kršitvi varstva osebnih podatkov (člen 34 UK GDPR).

2.5.4 *Preglednost*

(49) Posamezniki, na katere se nanašajo osebni podatki, morajo biti obveščeni o glavnih značilnostih obdelave svojih osebnih podatkov.

(50) To zagotavljata člena 13 in 14 UK GDPR, ki poleg splošnega načela preglednosti določata pravila o informacijah, ki se morajo zagotoviti posamezniku, na katerega se nanašajo osebni podatki ([42]). UK GDPR ne uvaja nobenih bistvenih sprememb teh pravil v primerjavi z ustreznimi členi Uredbe (EU) 2016/679. Vendar pa za zahteve glede preglednosti v navedenih členih tako kot na podlagi Uredbe (EU) 2016/679 velja več izjem, ki so določene v zakona o varstvu podatkov iz leta 2018 (glej uvodne izjave (55) do (72)).

([42]) V členu 13(1)(f) in členu 14(1)(f) so sklici na sklepe o ustreznosti, ki jih izda Komisija, nadomeščeni s sklici na enak instrument Združenega kraljestva, tj. na predpise o ustreznosti na podlagi zakona o varstvu podatkov iz leta 2018. Poleg tega so bili v členu 14(5)(c) do (d) sklici na pravo EU ali pravo držav članic nadomeščeni s sklici na notranje pravo (Združeno kraljestvo je kot primere takega notranjega prava, ki lahko spada na področje uporabe člena 14(5)(c), navedlo člen 7 zakona o trgovcih z odpadno kovino iz leta 2013 (Scrap Metal Dealers Act 2013), ki določa pravila o evidenci dovoljenj za trgovanje z odpadno kovino, in del 35 zakona o gospodarskih družbah iz leta 2006 (Companies Act 2006), ki določa pravila glede vodje registra gospodarskih družb. Podobno so primeri notranjega prava, ki lahko spada na področje člena 14(5)(d), tudi zakonodaja, ki določa pravila o poklicni tajnosti, ali obveznosti, ki izhajajo iz pogodb o zaposlitvi, ali obveznost varovanja zaupnosti, ki izhaja iz občega prava (na primer osebni podatki, ki jih obdelujejo zdravstveni delavci, kadrovske službe, socialni delavci itd.).

2.5.5 *Pravice posameznikov*

(51) Posamezniki, na katere se nanašajo osebni podatki, bi morali imeti določene pravice, ki jih lahko uresničujejo zoper upravljavca ali obdelovalca, zlasti pravico do dostopa do podatkov, pravico ugovarjati obdelavi in pravico do popravka in izbrisa podatkov. Hkrati so te pravice lahko omejene, če so take omejitve potrebne in sorazmerne za zaščito javne varnosti ali za doseganje drugih pomembnih ciljev splošnega javnega interesa.

2.5.5.1 Materialne pravice

(52) UK GDPR posameznikom priznava enake izvršljive pravice kot Uredba (EU) 2016/679. Določbe o pravicah posameznikov so v UK GDPR ohranjene brez bistvenih sprememb.

(53) Navedene pravice vključujejo pravico posameznika, na katerega se nanašajo osebni podatki, do dostopa do takih podatkov (člen 15 UK GDPR), pravico do popravka (člen 16 UK GDPR), pravico do izbrisa (člen 17 UK GDPR), pravico do omejitve obdelave (člen 18 UK GDPR), obveznost obveščanja o popravku ali izbrisu osebnih podatkov ali o omejitvi obdelave (člen 19 UK GDPR), pravico do prenosljivosti podatkov (člen 20 UK GDPR) ter pravico do ugovora (člen 21 UK GDPR) ([43]). Slednja vključuje tudi pravico posameznika, na katerega se nanašajo osebni podatki, ugovarjati obdelavi osebnih podatkov za namene neposrednega trženja, kot je določeno v členu 21(2) in (3) Uredbe (EU) 2016/679. Nadalje, na podlagi člena 122 zakona o varstvu podatkov iz leta 2018 mora informacijski pooblaščenec pripraviti kodeks ravnanja v zvezi z izvajanjem neposrednega trženja v skladu z zahtevami zakonodaje o varstvu podatkov (ter predpisov o zasebnosti in elektronskih komunikacijah iz leta 2003 (direktiva ES) (Privacy and Electronic Communications (EC Directive) Regulations 2003)) ter druge smernice za spodbujanje dobrih praks pri neposrednem trženju, za katere informacijski pooblaščenec meni, da so ustrezne. Urad informacijskega pooblaščenca trenutno pripravlja kodeks neposrednega trženja ([44]).

(54) V UK GDPR je bila brez vsebinskih sprememb ohranjena tudi pravica posameznika, na katerega se nanašajo osebni podatki, da zanj ne velja odločitev, ki temelji zgolj na avtomatizirani obdelavi, ki ima pravne učinke v zvezi z njim ali na podoben način nanj znatno vpliva, kakor je določeno v členu 22 splošne uredbe o varstvu podatkov. Dodan pa je bil nov odstavek 3A s sklicem na člen 14 zakona o varstvu podatkov iz leta 2018, ki določa zaščitne ukrepe glede pravic, svoboščin in zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, kadar se obdelava izvaja na podlagi člena 22(2)(b) UK GDPR. To se uporablja le, kadar je temelj za tako odločitev pooblastilo ali zahteva na podlagi prava Združenega kraljestva, ne uporablja pa se, kadar je odločitev potrebna na podlagi pogodbe ali sprejeta na podlagi izrecne privolitve posameznika, na katerega se nanašajo osebni podatki. Kadar se uporablja člen 14 zakona o varstvu podatkov iz leta 2018, mora upravljavec posameznika, na katerega se nanašajo osebni podatki, v najkrajšem možnem času pisno obvestiti, da je bila odločitev sprejeta le na podlagi avtomatizirane obdelave. Posameznik, na katerega se nanašajo osebni podatki, ima pravico zahtevati, da upravljavec v enem mesecu od prejema obvestila odločitev ponovno prouči, ali pa sprejme novo odločitev, ki ne temelji zgolj na podlagi avtomatizirane obdelave. Pristojni minister lahko sprejema nadaljnje zaščitne ukrepe glede avtomatiziranega odločanja. Ta pristojnost še ni bila izkoriščena.

2.5.5.2 Omejitve pravic posameznikov in druge določbe

(55) Zakon o varstvu podatkov iz leta 2018 določa več omejitev pravic posameznikov, ki ustrezajo okviru člena 23 UK GDPR. Okvir ne vsebuje omejitev pravice do ugovora neposrednemu trženju, kot je določena v členu 21(2) in (3) UK GDPR, ali pravice, da za posameznika ne velja odločitev, ki bi temeljila zgolj na avtomatizirani obdelavi, kakor je določena v členu 22 UK GDPR.

(56) Omejitve so navedene v dodatkih 2 do 4 k zakonu o varstvu podatkov iz leta 2018. Organi Združenega kraljestva so pojasnili, da morajo upoštevati dve načeli: načelo specifičnosti (vprašanja je treba obravnavati podrobno in razdeliti široke omejitve v več bolj specifičnih določb) ter načelo pogojenosti (vsako določbo spremljajo zaščitni ukrepi v obliki omejitev ali pogojev, da se preprečijo zlorabe) ([45]).

([43]) V členu 17(1)(e) in (3)(b) so bili sklici na pravo EU oziroma pravo držav članic nadomeščeni s sklicem na notranje pravo (kot primere takega notranjega prava na podlagi člena 17(1)(e) je Združeno kraljestvo navedlo angleške predpise o izobraževanju in informacijah za učence iz leta 2006 (Education (Pupil Information) (England) Regulations 2006), ki zahteva, da se imena učencev izbrišejo iz šolskih evidenc, ko učenec zapusti šolo, ali člen 34F zakona o zdravstveni dejavnosti iz leta 1983 (Medical Act 1983), ki določa pravila o izbrisu imen iz evidence družinskih zdravnikov in evidence specialistov.

([44]) Osnutek kodeksa ravnanja je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) UK Explanatory Framework for Adequacy Discussion, Section E: Restrictions, stran 1, na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Namen omejitev iz člena 23(1) UK GDPR je zagotoviti, da se uporabljajo le v specifičnih okoliščinah, kadar je to v demokratični družbi potrebno in kadar je sorazmerno glede na zakoniti cilj omejitve. Poleg tega v skladu z uveljavljeno sodno prakso o razlagi omejitev velja, da se lahko izjema od ureditve varstva podatkov v posameznem primeru uporabi le, če je to potrebno in sorazmerno ([46]). Preskus, ali je izjema potrebna, mora biti „strog, saj mora biti vsak poseg v pravice posameznika sorazmeren resnosti grožnje javnemu interesu. To torej zahteva klasično analizo sorazmernosti ([47])."

(58) Cilj teh omejitev ustreza omejitvam v členu 23 Uredbe (EU) 2016/679, razen glede omejitev v zvezi z nacionalno varnostjo in obrambo, ki so urejene v členu 26 zakona o varstvu podatkov iz leta 2018, vendar zanje veljajo enake zahteve glede potrebnosti in sorazmernosti (glej uvodne izjave (63) do (66)).

(59) Nekatere od omejitev, na primer tiste, ki se nanašajo na preprečevanje ali odkrivanje kaznivih dejanj, prijetje ali pregon storilcev ter izračun ali zbiranje davkov ali dajatev ([48]), dovoljujejo omejitve vseh pravic posameznikov in obveznosti glede preglednosti (razen pravic na podlagi člena 21(2) in člena 22). Obseg drugih omejitev je omejen na obveznosti glede preglednosti in pravic do dostopa, na primer omejitev, ki se nanašajo na varovanje zaupnosti sporazumevanja med odvetnikom in stranko ([49]), na pravico, da posamezniku ni treba izpovedati zoper sebe ([50]), in na financiranje podjetja, predvsem trgovanje na podlagi notranjih informacij ([51]). Nekaj omejitev omogoča omejevanje obveznosti upravljavca glede obveščanja posameznika, na katerega se nanašajo osebni podatki, o kršitvi varstva podatkov ter načel omejevanja namena, zakonitosti, poštenosti in preglednosti obdelave ([52]).

(60) Nekatere omejitve se samodejno v celoti uporabljajo za nekatere vrste obdelave osebnih podatkov (uporaba obveznosti v zvezi s preglednostjo in pravic posameznikov je na primer izključena, kadar se osebni podatki obdelujejo za namene presoje primernosti posameznika za sodno funkcijo ali kadar osebne podatke obdeluje sodišče ali posameznik, ki izvršuje sodno pristojnost).

(61) Vendar pa v večini primerov zadevna točka v dodatku 2 k zakonu o varstvu podatkov iz leta 2018 določa, da se omejitve uporabljajo le, kadar in kolikor bi uporaba določb „verjetno posegala" v zakoniti cilj zadevne omejitve: navedene določbe UK GDPR se na primer ne uporabljajo za osebne podatke, ki se obdelujejo zaradi preprečevanja ali odkrivanja kaznivih dejanj, prijetja ali pregona storilcev ali zaradi izračuna oziroma zbiranja davkov oziroma dajatev, „če bi uporaba navedenih določb verjetno posegala" v katero koli od navedenih zadev ([53]).

(62) Standard, „da bi verjetno posegalo" so sodišča Združenega kraljestva razlagala tako, da obstaja „znatna in pomembna verjetnost poseganja v opredeljene javne interese" ([54]). Na omejitev, za katero je treba izvesti preskus glede poseganja, se je torej mogoče sklicevati le, če je zelo verjetno, da bi podelitev določene pravice škodovala zadevnemu javnemu interesu. Upravljavec mora za vsak primer posebej oceniti, ali so ti pogoji izpolnjeni ([55]).

(63) Poleg omejitev iz dodatka 2 k zakonu o varstvu podatkov iz leta 2018 člen 26 navedenega zakona določa izjemo, ki jo je mogoče uporabiti pri nekaterih določbah UK GDPR in zakona o varstvu podatkov iz leta 2018, če je taka izjema potrebna za zagotavljanje nacionalne varnosti ali v obrambne namene. Ta izjema se nanaša na načela o varstvu podatkov (razen na načelo zakonitosti), na obveznost preglednosti, pravice posameznikov, na katere se nanašajo osebni podatki, obveznost obveščanja o kršitvi varstva podatkov, pravila o mednarodnih prenosih, nekatere obveznosti in pristojnosti informacijskega pooblaščenca ter na pravila o pravnih sredstvih, odgovornosti in

([46]) Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), točki 40 in 41.

([47]) Guriev v Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), točka 43. Glede tega glej tudi sodbo v zadevi Lin v Commissioner of Police for the Metropolis [2015] EWHC 2484 (QB), točka 80.

([48]) Točka 2 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([49]) Točka 19 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([50]) Točka 20 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([51]) Točka 21 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([52]) Omejitve pravice do obveščanja o kršitvi varstva podatkov so na primer dovoljene le v zvezi s kaznivimi dejanji in obdavčenjem (točka 2 dodatka 2 k zakonu o varstvu podatkov iz leta 2018), parlamentarnimi privilegiji (točka 13 dodatka 2 k zakonu o varstvu podatkov iz leta 2018) in obdelavo za novinarske, akademske, umetniške in književne namene (točka 26 dodatka 2 k zakonu o varstvu podatkov iz leta 2018).

([53]) Točka 2 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([54]) R (Lord) v Secretary of State for the Home Department [2003] EWHC 2073 (Admin), točka 100, in Guriev v Community Safety Development (Združeno kraljestvo) Ltd [2016] EWHC 643 (QB), točka 43.

([55]) Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor, točka 31.

sankcijah, razen glede določbe o splošnih pogojih za uvedbo upravnih glob iz člena 83 UK GDPR in določbe o sankcijah iz člena 84 UK GDPR. Nadalje, člen 28 zakona o varstvu podatkov iz leta 2018 spreminja uporabo člena 9(1), da se omogoči obdelava posebnih vrst podatkov iz člena 9(1) UK GDPR, če se obdelava izvaja za zagotavljanje nacionalne varnosti ali v obrambne namene ter ob upoštevanju ustreznih zaščitnih ukrepov za varstvo pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki ([56]).

(64) Izjema se lahko uporabi le, kolikor je potrebno za zagotavljanje nacionalne varnosti ali obrambe. Tako kot velja tudi pri drugih izjemah na podlagi zakona o varstvu podatkov iz leta 2018, mora upravljavec to izjemo proučiti in uporabiti za vsak primer posebej. Nadalje, vsaka uporaba izjeme mora biti v skladu s standardi, ki veljajo za človekove pravice (na podlagi zakona o človekovih pravicah iz leta 1998), v skladu s katerimi mora biti v demokratični družbi vsak poseg v pravice do zasebnosti potreben in sorazmeren ([57]).

(65) To razlago izvzetja potrjuje urad informacijskega pooblaščenca, ki je izdal podrobne smernice o uporabi izjeme glede nacionalne varnosti in obrambe, pri čemer je jasno, da jo mora upravljavec obravnavati in uporabiti za vsak primer posebej ([58]). V smernicah je poudarjeno, da ne gre za splošno izjemo in da se nanjo ni mogoče sklicevati samo zato, ker se podatki obdelujejo za namene nacionalne varnosti. Upravljavec mora pri sklicevanju nanjo dokazati, da obstaja resnična možnost negativnega učinka za nacionalno varnost, in od njega se po po potrebi pričakuje, da bo [uradu informacijskega pooblaščenca] predložil dokaze o tem, zakaj jo je uporabil. Smernice vsebujejo kontrolni seznam in vrsto primerov za nadaljnjo pojasnitev pogojev, pod katerimi se to izvzetje lahko uveljavlja.

(66) Zgolj dejstvo, da se podatki obdelujejo za namene nacionalne varnosti ali obrambe, torej samo po sebi ne zadošča za uporabo izjeme. Upravljavec mora proučiti dejanske posledice za nacionalno varnost, če bi moral upoštevati posamezno določbo o varstvu podatkov. Izjema se lahko uporabi le pri posebnih določbah, za katere je bilo ugotovljeno, da pomenijo tveganje, in jo je treba uporabiti kolikor je mogoče omejujoče ([59]).

(67) Ta pristop je potrdilo tudi sodišče Information Tribunal ([60]). V zadevi Baker v Secretary of State for the Home Department (v nadaljnjem besedilu: Baker proti Secretary of State) je ugotovilo, da je nezakonito uporabiti izjemo zaradi nacionalne varnosti kar na splošno glede vseh zahtev za dostop do podatkov, ki jih prejmejo obveščevalne službe. Namesto tega je treba izjemo uporabiti v vsakem primeru posebej in vsako zahtevo vsebinsko proučiti, tudi z vidika pravice posameznikov do spoštovanja njihovega zasebnega življenja ([61]).

([56]) Iz informacij organov Združenega kraljestva izhaja, da kadar se obdelava izvaja v okviru zagotavljanja nacionalne varnosti, upravljavci običajno uporabljajo okrepljene zaščitne in varnostne ukrepe, ki odražajo občutljivost take obdelave. Kateri zaščitni ukrepi so ustrezni, bo odvisno od tveganj posamezne obdelave. To lahko pomeni omejitve dostopa do podatkov, do katerih imajo lahko dostop le pooblaščene osebe, ki so opravile ustrezen varnostni pregled, stroge omejitve glede izmenjave podatkov in visok standard varnosti, ki se uporablja za postopke hrambe in ravnanja s podatki.

([57]) Glej tudi Guriev v Community Safety Development (United Kingdom) Ltd [2016] EWHC 643 (QB), točka 45, in sodbo v zadevi Lin v Commissioner of the Police for the Metropolis [2015] EWHC 2484 (QB), točka 80.

([58]) Glej smernice urada informacijskega pooblaščenca o izjemi glede nacionalne varnosti in obrambe, ki so na voljo na naslednji povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([59]) V skladu s primerom, ki so ga navedli organi Združenega kraljestva, bi bilo treba, kadar bi osumljeni terorist, glede katerega poteka preiskava pri MI5, od notranjega ministrstva zahteval dostop do podatkov (na primer ker je v sporu z notranjim ministrstvom zaradi vprašanj s področja priseljevanja), pred razkritjem posamezniku, na katerega se nanašajo osebni podatki, zaščititi vse podatke, ki jih je MI5 izmenjala z notranjim ministrstvom v zvezi z odprtimi preiskavami in ki bi lahko posegali v občutljive vire, metode ali tehnike in/ali povečali tveganje, ki ga pomeni posameznik. V takih okoliščinah je verjetno, da bo izpolnjen pogoj za uporabo izjeme iz člena 26 in bo treba uporabiti izjemo od razkritja informacij, da se zagotovi nacionalna varnost. Vendar pa velja, da če bi imelo notranje ministrstvo tudi osebne podatke o posamezniku, ki se ne nanašajo na preiskavo MI5, in bi bilo mogoče take informacije zagotoviti brez tveganja za nacionalno varnost, se izjema zaradi nacionalne varnosti ne bi smela uporabiti pri presoji, ali naj se informacije posamezniku razkrijejo. Urad informacijskega pooblaščenca trenutno pripravlja smernice o tem, kako naj upravljavci uporabijo izjemo iz člena 26. Pričakuje se, da bodo smernice objavljene ob koncu marca 2021.

([60]) Sodišče Information Tribunal je bilo ustanovljeno za obravnavo pritožb glede varstva podatkov na podlagi zakona o varstvu podatkov iz leta 1984. Leta 2010 je sodišče Information Tribunal postalo del splošnega regulativnega senata sodišč prve stopnje (General Regulatory Chamber of the First Tier Tribunal), in sicer v okviru reform strukture sistema sodišč v Združenem kraljestvu.

([61]) Glej Baker proti Secretary of State [2001] UKIT NSA2.

2.5.6 *Omejitve glede osebnih podatkov, ki se obdelujejo za novinarske, umetniške, akademske in književne namene ter za namene arhiviranja in raziskav*

(68) Člen 85(2) UK GDPR omogoča, da se obdelava osebnih podatkov za novinarske umetniške , akademske,in književne namene izvzame iz uporabe več določb UK GDPR. Del 5 dodatka 2 k zakonu o varstvu podatkov iz leta 2018 določa izjeme glede obdelave za navedene namene. Določa izjeme od načel o varstvu podatkov (razen od načela celovitosti in zaupnosti), pravno podlago za obdelavo (vključno s posebnimi vrstami podatkov in podatki v zvezi s kazenskimi obsodbami ipd.), pogoje privolitve, obveznosti glede preglednosti, pravice posameznikov, na katere se nanašajo osebni podatki, obveznost obveščanja o kršitvi varstva podatkov, zahtevo glede posvetovanja z informacijskim pooblaščencem pred izvedbo visoko tvegane obdelave podatkov in pravila o mednarodnih prenosih ([62]). V tem smislu se UK GDPR vsebinsko ne razlikuje od Uredbe (EU) 2016/679, ki v členu 85 prav tako omogoča izjemo glede obdelave v novinarske namene ali zaradi akademskega, umetniškega ali književnega izražanja od zahtev Uredbe (EU) 2016/679. Določbe zakona o varstvu podatkov iz leta 2018, predvsem del 5 dodatka 2, so skladne z UK GDPR.

(69) Ključna presoja, ki jo je treba izvesti na podlagi člena 85 UK GDPR, se nanaša na vprašanje, ali je izjema od pravil o varstvu podatkov iz uvodne izjave (68) „potrebna za uravnoteženje pravice do varstva osebnih podatkov s svobodo izražanja in obveščanja“ ([63]). Na podlagi točke 26(2) in (3) dodatka 2 k zakonu o varstvu podatkov iz leta 2018 Združeno kraljestvo pri taki presoji uporablja preskus „razumne domneve“. Izjema je upravičena, če upravljavec razumno domneva (i) da je objava v javnem interesu, in (ii) da uporaba zadevnih določb UK GDPR ne bi bila skladna z obdelavo za novinarske, akademske, umetniške in književne namene. V skladu s sodno prakso ([64]) ima preskus „razumne domneve“ subjektivno in objektivno komponento: ne zadošča, če upravljavec dokaže, da je sam osebno domneval, da upoštevanje ne bi bilo skladno. Njegova domneva mora biti utemeljena, tj. enako mora domnevati vsaka razumna oseba, ki pozna zadevna dejstva. Upravljavec mora torej pri odločanju ravnati s potrebno skrbnostjo, da lahko dokaže razumnost. Iz pojasnil organov Združenega kraljestva izhaja, da je treba preskus „razumne domneve“ izvesti pri uporabi vsake izjeme posebej ([65]). Če so pogoji izpolnjeni, se šteje, da je izjema potrebna in sorazmerna na podlagi prava Združenega kraljestva.

(70) Na podlagi člena 124 zakona o varstvu podatkov iz leta 2018 mora urad informacijskega pooblaščenca pripraviti kodeks ravnanja glede varstva podatkov na področju novinarstva. Navedeni kodeks je v pripravi. Izdane so bile smernice o vprašanjih v zvezi z zakonom o varstvu podatkov iz leta 1998, v katerih je poudarjeno predvsem, da za uporabo navedene izjeme ne zadošča zgolj navesti, da bi zagotavljanje skladnosti povzročalo nevšečnosti pri izvajanju novinarskih dejavnosti, ampak mora obstajati jasen argument, da zadevna

([62]) Glej člen 85 UK GDPR in točko 26(9) dela 5 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([63]) V skladu s točko 26(2) dela 5 dodatka 2 k zakonu o varstvu podatkov iz leta 2018 se izjema uporablja za obdelavo osebnih podatkov, ki se izvaja v posebne namene (novinarske, akademske, umetniške in književne), če je namen obdelave objava novinarskega, akademskega, umetniškega ali književnega gradiva, upravljavec pa razumno domneva, da bi bila objava takega gradiva v javnem interesu. Pri presoji, ali bi bila objava v javnem interesu, mora upravljavec upoštevati posebni pomen javnega interesa v okviru svobode izražanja in obveščanja. Nadalje, upravljavec mora upoštevati kodekse ravnanja ali smernice, ki se nanašajo na zadevno objavo (uredniške smernice BBC (BBC Editorial Guidelines), kodeks radiofuzije britanskega regulatorja komunikacij Ofcom (Ofcom Broadcasting Code) ter kodeks ravnanja urednikov (Editors' Code of Practice)). Nadalje, za uporabo izjeme mora upravljavec razumno domnevati, da bi bilo zagotavljanje skladnosti z zadevno določbo neskladno s posebnim namenom (točka 26(3) dodatka 2 k zakonu o varstvu podatkov iz leta 2018).

([64]) V točki 102 sodbe v zadevi NT1 proti Googlu [2018] EWHC 799 (QB) je obravnavano vprašanje, ali je upravljavec podatkov razumno domneval, da je objava v javnem interesu in da bi bilo zagotavljanje skladnosti z zadevnimi določbami neskladno s posebnimi nameni. Sodišče je navedlo, da ima člen 32(1)(b) in (c) zakona o varstvu podatkov iz leta 1998 subjektivno in objektivno komponento: upravljavec podatkov mora dokazati, da je bil prepričan, da bi bila objava v javnem interesu, in da je bila ta njegova domneva objektivno razumna; dokazati mora subjektivno domnevo, da bi bilo zagotavljanje skladnosti z določbami, pri katerih želi uporabiti izjemo, neskladno z zadevnim posebnim namenom.

([65]) V odločitvi urada informacijskega pooblaščenca o izreku globe družbi *True Visions Productions*, ki je bila izrečena na podlagi zakona o varstvu podatkov iz leta 1998, je naveden primer uporabe preskusa „razumne domneve“. Urad informacijskega pooblaščenca je sprejel navedbo, da je medijski upravljavec subjektivno domneval, da zagotavljanje skladnosti s prvim načelom o varstvu podatkov (poštenost in zakonitost) ne bi bila skladna z novinarskim namenom. Vendar pa urad informacijskega pooblaščenca ni sprejel navedb, da je bila ta domneva objektivno razumna. Odločba urada informacijskega pooblaščenca je na voljo na povezavi: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

določba pomeni oviro odgovornemu novinarstvu ([66]). Smernice glede uporabe preskusa javnega interesa in glede tehtanja javnega interesa z interesom posameznika do zasebnosti sta objavila tudi britanski regulator telekomunikacij OFCOM in BBC v okviru svojih uredniških smernic ([67]). Smernice vsebujejo predvsem primere informacij, za katere se lahko šteje, da so v javnem interesu, ter pojasnjujejo, da je treba dokazati, da v okviru posebnih okoliščin primera javni interes prevlada nas pravicami do zasebnosti.

(71) Podobno kot na podlagi člena 89 UK GDPR je mogoče iz uporabe več določb UK GDPR izvzeti tudi osebne podatke, ki se obdelujejo za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinskoraziskovalne namene ali statistične namene ([68]). V zvezi z raziskovalnimi in statističnimi nameni so izjeme mogoče glede določb UK GDPR, ki se nanašajo na potrditev obdelave, dostop do podatkov in zaščitne ukrepe za prenos v tretje države, pravico do popravka, omejitev obdelave in ugovor obdelavi. Glede arhiviranja v javnem interesu so izjeme mogoče tudi glede obveznosti obveščanja o popravku ali izbrisu osebnih podatkov ali glede omejitve obdelave, pa tudi glede pravice do prenosljivosti podatkov.

(72) V skladu s točkama 27(1) in 28(1) dodatka 2 k zakonu o varstvu podatkov iz leta 2018 so izjeme od določb, navedenih v UK GDPR, mogoče, kadar bi uporaba določbe „onemogočila ali resno ovirala doseganje“ zadevnih namenov ([69]).

(73) Glede na njihov pomen za učinkovito uveljavljanje pravic posameznikov se bodo v okviru stalnega spremljanja tega sklepa ustrezno upoštevale vse pomembne spremembe v zvezi z razlago in uporabo navedenih izjem v praksi (poleg tistih, ki se nanašajo na ohranjanje učinkovitega nadzora priseljevanja, kot je pojasnjeno v uvodni izjavi (6)), vključno z nadaljnjim razvojem sodne prakse ter smernic in izvršilnih ukrepov urada informacijskega pooblaščenca ([70]).

2.5.7 *Omejitve nadaljnjih prenosov podatkov*

(74) Raven varstva, ki se zagotavlja osebnim podatkom, prenesenim iz Evropske unije upravljavcem ali obdelovalcem v Združenem kraljestvu, se ne sme poslabšati z nadaljnjim prenosom takih podatkov prejemnikom v tretji državi. Taki „nadaljnji prenosi“ podatkov, ki z vidika upravljavca ali obdelovalca iz Združenega kraljestva pomenijo mednarodni prenos iz Združenega kraljestva, bi morali biti dovoljeni le, kadar tudi za nadaljnjega prejemnika zunaj Združenega kraljestva veljajo pravila, ki zagotavljajo podobno raven varstva, kot je zagotovljena v okviru pravnega reda Združenega kraljestva. Zato je uporaba pravil iz UK GDPR in iz zakona o varstvu podatkov iz leta 2018 o mednarodnih prenosih osebnih podatkov pomemben dejavnik za zagotavljanje nadaljnjega varstva v primeru, ko se na podlagi tega sklepa prenašajo osebni podatki iz Evropske unije v Združeno kraljestvo.

([66]) V skladu s smernicami morajo organizacije pojasniti, zakaj bi bilo zagotavljanje skladnosti z zadevnimi določbami zakona o varstvu podatkov iz leta 1998 neskladno z novinarskimi nameni. Upravljavci morajo zlasti pretehtati škodljive učinke, ki bi jih zagotavljanje skladnosti lahko imelo na novinarstvo, in škodljive učinke, ki bi jih izjema imela na pravice posameznikov, na katere se nanašajo osebni podatki. Če lahko novinar razumno doseže uredniški cilj tako, da zagotavlja skladnost s standardnimi določbami zakona o varstvu podatkov, mora to storiti. Organizacije morajo utemeljiti uporabe omejitev pri vsaki določbi, glede katere niso zagotovile skladnosti. Data protection and journalism: a guide for the media (Varstvo podatkov na področju novinarstva: smernice za medije), na voljo na povezavi: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Primeri javnega interesa so razkritje ali odkrivanje kaznivega dejanja, varstvo javnega zdravja ali zaščita javne varnosti, razkrivanje zavajajočih trditev posameznikov ali organizacij, ali razkrivanje nesposobnosti, ki vpliva na javnost. Glej smernice organa OFCOM, ki so na voljo na povezavi: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf , in uredniške smernice BBC, ki so na voljo na povezavi: https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Glej člen 89 UK GDPR ter točki 27(2) in 28(2) dela 6 dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([69]) Glede tega velja zahteva, da se osebni podatki obdelujejo v skladu s členom 89(1) UK GDPR, kakor je bil dopolnjen s členom 19 zakona o varstvu podatkov iz leta 2018.

([70]) Glej uvodne izjave (281) do (287).

(75) Ureditev mednarodnega prenosa osebnih podatkov iz Združenega kraljestva je določena v členih 44 do 49 UK GDPR, kakor je bila dopolnjena z zakonom o varstvu podatkov iz leta 2018, in odraža ureditev iz poglavja V Uredbe (EU) 2016/679 ([71]). Osebni podatki se lahko prenašajo v tretjo državo ali mednarodno organizacijo le na podlagi predpisov o ustreznosti (instrument, ki je v Združenem kraljestvu enak sklepu o ustreznosti na podlagi Uredbe (EU) 2016/679), če takih predpisov o ustreznosti ni, pa kadar upravljavec ali obdelovalec zagotovi ustrezne zaščitne ukrepe, v skladu s členom 46 UK GDPR. Če ne obstajajo niti predpisi o ustreznosti, niti ustrezni zaščitni ukrepi, se lahko podatki prenašajo le na podlagi odstopanj iz člena 49 UK GDPR.

(76) Predpisi o ustreznosti, ki jih izda pristojni minister, lahko določajo, da tretja država (ali ozemlje oziroma področje znotraj tretje države), mednarodna organizacija ali opis ([72]) take države, ozemlja, področja ali organizacije zagotavlja ustrezno raven varstva osebnih podatkov. Pri presoji ustreznosti ravni varstva mora pristojni minister upoštevati iste elemente, kot jih mora proučiti Komisija na podlagi člena 45(2)(a) do (c) Uredbe (EU) 2016/679, v povezavi z uvodno izjavo 104 navedene uredbe, ter ohranjene sodne prakse EU. To pomeni, da je pri presoji ustrezne ravni varstva v tretji državi zadevni standard, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, ki se zagotavlja v Združenem kraljestvu.

(77) Glede postopka se za predpise o ustreznosti uporabljajo „splošne“ procesne zahteve iz člena 182 zakona o varstvu podatkov iz leta 2018. V skladu s tem postopkom se mora pristojni minister pred sprejetjem predpisov Združenega kraljestva o ustreznosti posvetovati z informacijskim pooblaščencem ([73]). Ko pristojni minister sprejme navedene predpise, se jih predloži parlamentu, ki jih obravnava v postopku tako imenovane negativne potrditve, v katerem lahko oba domova parlamenta proučita predpise in jih v 40 dneh razveljavita ([74]).

(78) V skladu s členom 17B(1) zakona o varstvu podatkov iz leta 2018 je treba predpise o ustreznosti preverjati na največ štiri leta, pristojni minister pa mora redno spremljati dogajanje v tretjih državah in mednarodnih organizacijah, ki bi lahko vplivalo na odločitve o sprejemanju predpisov o ustreznosti, njihovem spreminjanju ali odpravi. Če pristojni minister izve, da določena država ali organizacija ne zagotavlja več ustrezne ravni varstva osebnih podatkov, mora po potrebi spremeniti ali odpraviti navedene predpise ter se z zadevno tretjo državo ali mednarodno organizacijo posvetovati o izboljšanju ravni varstva. Ti procesni vidiki odražajo ustrezne zahteve iz Uredbe (EU) 2016/679.

([71]) Z izjemo člena 48 Uredbe (EU) 2016/679, ki ga Združeno kraljestvo ni vključilo v UK GDPR. V zvezi s tem je treba najprej opozoriti, da je standard, za katerega se šteje, da zagotavlja ustrezno raven varstva, standard „osnovne enakovrednosti“ in ne identitete, kot je pojasnilo Sodišče Evropske unije (Schrems I, točke 73 in 74) in kot priznava Evropski odbor za varstvo podatkov (referenčni dokument o ustreznosti, stran 3). Zato, kot je Evropski odbor za varstvo podatkov pojasnil v svojem referenčnem dokumentu o ustreznosti, „cilj ni natančno posnemati evropsko zakonodajo, temveč določiti bistvene – temeljne zahteve te zakonodaje“. V zvezi s tem je treba opozoriti, da pravni red Združenega kraljestva sicer formalno ne vsebuje določbe, ki bi bila enaka členu 48, vendar je enak učinek zagotovljen z drugimi pravnimi določbami in načeli, tj. da se lahko v odgovor na zahtevek sodišča ali upravnega organa tretje države za osebne podatke osebni podatki prenesejo v to tretjo državo le, če obstaja mednarodni sporazum – na podlagi katerega se sodna odločba ali upravna odločba zadevne tretje države priznava ali izvršuje v Združenem kraljestvu – ali če temelji na enem od mehanizmov za prenos iz poglavja V UK GDPR. Za izvršitev tuje sodne odločbe morajo imeti sodišča v Združenem kraljestvu podlago v občem pravu ali listini, ki tako izvršljivost omogoča. Vendar niti obče pravo (glej Adams and Others v Cape Industries Plc., [1990] 2 W.L.R. 657) niti listine ne določajo izvrševanja tujih sodnih odločb, ki zahtevajo prenos podatkov brez sklenjenega mednarodnega sporazuma. Zato so zahtevki po podatkih po pravu Združenega kraljestva neizvršljivi, če takega mednarodnega sporazuma ni. Poleg tega za vsak prenos osebnih podatkov v tretje države - tudi na zahtevo tujega sodišča ali upravnega organa – še naprej veljajo omejitve iz poglavja V UK GDPR, ki so enake ustreznim določbam Uredbe (EU) 2016/679, zato se je treba sklicevati na enega od razlogov za prenos iz poglavja V v skladu s posebnimi pogoji, ki veljajo zanj na podlagi navedenega poglavja.

([72]) Organi Združenega kraljestva so pojasnili, da se opis države ali mednarodne organizacije nanaša na okoliščine, ko bi bilo treba izvesti specifično in delno oceno ustreznosti z določenimi omejitvami (na primer predpisi o ustreznosti, ki se nanašajo le na določeno vrsto prenosov podatkov).

([73]) Glej memorandum o soglasju med ministrom za digitalne tehnologije, kulturo, medije in šport (Secretary of State for the Department for Digital, Culture, Media and Sport) ter uradom informacijskega pooblaščenca o vlogi urada informacijskega pooblaščenca pri novi oceni Združenega kraljestva o ustreznosti, ki je na voljo na naslednji povezavi: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Če je taka odločitev izglasovana, predpisi nimajo več nobenega nadaljnjega pravnega učinka.

(79) Če predpisi o ustreznosti niso sprejeti, se lahko mednarodni prenosi podatkov izvajajo, če upravljavec ali obdelovalec zagotovi ustrezne zaščitne ukrepe v skladu s členom 46 UK GDPR. Ti zaščitni ukrepi so podobni tistim iz člena 46 Uredbe (EU) 2016/679. Vključujejo pravno zavezujoče in izvršljive instrumente med javnimi organi ali telesi, zavezujoča poslovna pravila ([75]), standardne klavzule o varstvu podatkov, odobrene kodekse ravnanja, odobrene mehanizme certificiranja ter ob odobritvi informacijskega pooblaščenca pogodbene klavzule med upravljavci (ali obdelovalci) oziroma upravne dogovore med javnimi organi. Vendar pa so bila pravila s procesnega vidika spremenjena tako, da delujejo v okviru Združenega kraljestva; standardne klavzule o varstvu podatkov lahko sprejema pristojni minister (člen 17C) ali informacijski pooblaščenec (člen 119A), v skladu z zakonom o varstvu podatkov iz leta 2018.

(80) Če ne obstajajo niti sklep o ustreznosti, niti ustrezni zaščitni ukrepi, se lahko podatki prenašajo le na podlagi odstopanj iz člena 49 UK GDPR ([76]). UK GDPR ne uvaja nobenih bistvenih sprememb teh odstopanj v primerjavi z ustreznimi pravili iz Uredbe (EU) 2016/679. V skladu z UK GDPR in Uredbo (EU) 2016/679 se nekatera odstopanja lahko uporabijo le, če je prenos občasen ([77]). Nadalje, urad informacijskega pooblaščenca v svojih smernicah o mednarodnih prenosih podatkov pojasnjuje: „Uporabiti jih je treba le kot dejanske ‚izjeme' od splošnega pravila, da je omejeni prenos prepovedan, razen če se izvede na podlagi sklepa o ustreznosti ali če obstajajo ustrezni zaščitni ukrepi" ([78]). Pristojni minister lahko glede prenosov, ki so potrebni zaradi pomembnih razlogov javnega interesa (člen 49(1)(d)), izda predpise z opredelitvijo okoliščin, v katerih je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo potreben oziroma ni potreben zaradi pomembnih razlogov javnega interesa. Nadalje, pristojni minister lahko s predpisi omeji prenos posamezne vrste osebnih podatkov v tretjo državo ali mednarodno organizacijo, kadar prenosa ni mogoče izvesti na podlagi predpisov o ustreznosti in pristojni minister meni, da je omejitev potrebna zaradi pomembnih razlogov javnega interesa. Tak predpis do zdaj še ni bil izdan.

(81) Ta okvir glede mednarodnih prenosov podatkov se je začel uporabljati ob koncu prehodnega obdobja ([79]). Vendar pa točka 4 dodatka 21 k zakonu o varstvu podatkov iz leta 2018 (ki je bil uveden s predpisi DPPEC) določa, da se od konca prehodnega obdobja naprej nekateri prenosi osebnih podatkov obravnavajo, kot da temeljijo na predpisih o ustreznosti. Ti prenosi vključujejo prenose v države EGP, na ozemlje Gibraltarja, v institucije, organe, urade ali agencije Unije, ustanovljene s Pogodbo EU ali na njeni podlagi, in v tretje države, glede katerih je bil ob koncu prehodnega obdobja izdan sklep EU o ustreznosti. Posledično se prenosi

([75]) V UK GDPR so ohranjena pravila iz člena 47 Uredbe (EU) 2016/679, ki so spremenjena le toliko, da ustrezajo notranjemu okviru; sklici na pristojni nadzorni organ so na primer nadomeščeni s sklici na informacijskega pooblaščenca, črtani so sklici na mehanizem za skladnost iz odstavka 1, črtan pa je tudi celoten odstavek 3.

([76]) Na podlagi člena 49 UK GDPR je prenos mogoč, če je izpolnjen eden od teh pogojev: (a) posameznik, na katerega se nanašajo osebni podatki, je izrecno privolil v predlagani prenos, potem ko je bil obveščen o morebitnih tveganjih, ki jih zaradi nesprejetja sklepa o ustreznosti in ustreznih zaščitnih ukrepov takšni prenosi pomenijo zanj; (b) prenos je potreben za izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem ali za izvajanje predpogodbenih ukrepov, sprejetih na zahtevo posameznika, na katerega se nanašajo osebni podatki; (c) prenos je potreben za sklenitev ali izvajanje pogodbe med upravljavcem in drugo fizično ali pravno osebo, ki je v interesu posameznika, na katerega se nanašajo osebni podatki; (d) prenos je potreben zaradi pomembnih razlogov javnega interesa; (e) prenos je potreben za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov; (f) prenos je potreben za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih oseb, kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali poslovno ni sposoben dati privolitve, (g) prenos se opravi iz registra, ki je po notranjem pravu namenjen zagotavljanju informacij javnosti in je na voljo za vpogled bodisi javnosti na splošno bodisi kateri koli osebi, ki lahko izkaže zakoniti interes, vendar le, če so v posameznem primeru izpolnjeni pogoji za tak vpogled, določeni v notranjem pravu. Poleg tega, kadar ni izpolnjen nobeden od zgoraj navedenih pogojev, se prenos lahko opravi le, če ni ponavljajoč, zadeva le omejeno število posameznikov, na katere se nanašajo osebni podatki, je potreben zaradi nujnih zakonitih interesov, za katere si prizadeva upravljavec in nad katerimi ne prevladajo interesi ali pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, in pod pogojem, da je upravljavec ocenil vse okoliščine v zvezi s prenosom podatkov in na podlagi te ocene predvidel ustrezne zaščitne ukrepe v zvezi z varstvom osebnih podatkov.

([77]) V uvodni izjavi 111 UK GDPR je navedeno, da se prenosi v zvezi s pogodbo ali pravnim zahtevkom lahko izvajajo le, če so občasni.

([78]) Smernice urada informacijskega pooblaščenca o mednarodnih prenosih podatkov so na voljo na naslednji povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) V obdobju največ šestih mesecev, ki se izteče najpozneje 30. junija 2021, je treba uporabo tega novega okvira razumeti v smislu člena 782 Sporazuma o trgovini in sodelovanju med Evropsko unijo in Evropsko skupnostjo za atomsko energijo na eni strani ter Združenim kraljestvom Velika Britanija in Severna Irska na drugi strani (L 444/14 z dne 31.12.2020) (v nadaljnjem besedilu: sporazum o trgovini in sodelovanju med EU in Združenim kraljestvom), ki je na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:22020A1231(01)&qid=1618247029009&from=EN.

v navedene države lahko nadaljujejo kot pred izstopom Združenega kraljestva iz EU. Po koncu prehodnega obdobja mora pristojni minister v štirih letih opraviti pregled teh ugotovitev glede ustreznosti, tj. do konca decembra 2024. Iz pojasnila organov Združenega kraljestva izhaja, da čeprav mora pristojni minister tak pregled opraviti do konca decembra 2024, pa prehodne določbe ne vključujejo samoderogacijske klavzule in zadevne prehodne določbe ne prenehajo samodejno veljati, če pregled ni opravljen do konca decembra 2024.

(82) Kar zadeva prihodnji razvoj ureditve mednarodnega prenosa podatkov v Združenem kraljestvu – s sprejetjem novih predpisov o ustreznosti, sklepanjem mednarodnih sporazumov ali razvojem drugih mehanizmov za prenos – bo Komisija pozorno spremljala razmere, ocenila, ali se različni mehanizmi za prenos uporabljajo na način, ki zagotavlja neprekinjeno varstvo, in po potrebi sprejela ustrezne ukrepe za odpravo morebitnih škodljivih učinkov (glej uvodne izjave (278) do (287)). Ker imata EU in Združeno kraljestvo podobna pravila o mednarodnih prenosih, bi se problematičnim razlikam lahko izognili tudi s sodelovanjem ter izmenjavo informacij in izkušenj, tudi med uradom informacijskega pooblaščenca in Evropskim odborom za varstvo podatkov.

2.5.8 *Odgovornost*

(83) V skladu z načelom odgovornosti morajo subjekti, ki obdelujejo podatke, sprejeti ustrezne tehnične in organizacijske ukrepe, da lahko uspešno izpolnjujejo svoje obveznosti glede varstva podatkov in dokažejo tako skladnost, predvsem pristojnim nadzornim organom.

(84) Načelo odgovornosti iz Uredbe (EU) 2016/679 je ohranjeno v členu 5(2) UK GDPR brez bistvenih sprememb, enako pa velja glede člena 24 o odgovornosti upravljavca, člena 25 o vgrajenem in privzetem varstvu podatkov ter člena 30 o evidenci dejavnosti obdelave. Prav tako sta bila ohranjena člena 35 in 36 o oceni učinka v zvezi z varstvom podatkov in predhodnim posvetovanjem z nadzornim organom. Členi 37 do 39 Uredbe (EU) 2016/679 o imenovanju in nalogah pooblaščenih oseb za varstvo podatkov so bili v UK GDPR ohranjeni brez bistvenih sprememb. V UK GDPR so ohranjene tudi določbe členov 40 in 42 Uredbe (EU) 2016/679 o kodeksih ravnanja in certificiranju ([80]).

2.6 **Nadzor in izvrševanje**

2.6.1 *Neodvisen nadzor*

(85) Vzpostaviti bi bilo treba neodvisen nadzorni organ s pristojnostjo spremljanja in zagotavljanja skladnosti s pravili o varstvu podatkov, da se tudi v praksi zagotovi ustrezna raven varstva podatkov. Pri izvajanju svojih obveznosti in pooblastil bi moral ta organ ravnati popolnoma neodvisno in nepristransko.

(86) V Združenem kraljestvu nadzor in uveljavljanje skladnosti z UK GDPR in zakonom o varstvu podatkov iz leta 2018 izvaja informacijski pooblaščenec. Informacijski pooblaščenec je „Corporation Sole“, tj. ločen enoosebni pravni subjekt. Pri delu mu pomaga urad. Dne 31. marca 2020 je imel urad informacijskega pooblaščenca 768 stalnih članov osebja ([81]). Podporno ministrstvo informacijskega pooblaščenca je ministrstvo za digitalne tehnologije, kulturo, medije in šport ([82]).

(87) Neodvisnost informacijskega pooblaščenca je izrecno določena v členu 52 UK GDPR, ki v ničemer bistveno ne spreminja člena 52(1) do (3) splošne uredbe o varstvu podatkov. Informacijski pooblaščenec mora pri opravljanju svojih nalog in izvajanju svojih pooblastil v skladu z UK GDPR ravnati popolnoma neodvisno, ne sme biti

([80]) Ti sklici so po potrebi nadomeščeni s sklici na organe Združenega kraljestva. V skladu s členom 17 zakona o varstvu podatkov iz leta 2018 lahko na primer informacijski pooblaščenec ali nacionalni akreditacijski organ Združenega kraljestva akreditira osebo, ki izpolnjuje zahteve iz člena 43 UK GDPR za spremljanje zagotavljanja skladnosti s certifikatom.

([81]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2019–2020 sta na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Odnosi med njima so urejeni s sporazumom o upravljanju. Ključne odgovornosti ministrstva za digitalne tehnologije, kulturo, medije in šport kot podpornega ministrstva so zlasti: zagotavljanje ustreznega financiranja in ustreznih virov informacijskemu pooblaščencu; zastopanje interesov informacijskega pooblaščenca v parlamentu in drugih vladnih službah; zagotavljanje trdnega nacionalnega okvira varstva podatkov ter zagotavljanje usmerjanja in podpore uradu informacijskega pooblaščenca v zvezi s poslovnimi vprašanji, kot so vprašanja nepremičnin, najemov in nabav (sporazum o upravljanju za obdobje 2018–2021 je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

izpostavljen niti neposrednemu niti posrednemu zunanjemu vplivu ter ne sme nikogar prositi za navodila niti jih od nikogar sprejeti. Poleg tega se mora vzdržati vsakega delovanja, ki je nezdružljivo z njegovimi dolžnostmi, in se v času svojega mandata ne sme ukvarjati z nobenim nezdružljivim delom, bodisi profitnim bodisi neprofitnim.

(88) Pogoji za imenovanje in razrešitev informacijskega pooblaščenca so določeni v dodatku 12 k zakonu o varstvu podatkov iz leta 2018. Informacijskega pooblaščenca imenuje kraljica na podlagi priporočila vlade ter na podlagi poštenega in odprtega postopka izbire. Kandidat mora imeti ustrezne kvalifikacije, izkušnje in znanje. V skladu s kodeksom upravljanja v zvezi z javnimi imenovanji ([83]) seznam ustreznih kandidatov pripravi svetovalni ocenjevalni odbor. Preden minister za digitalne tehnologije, kulturo, medije in šport sprejme končno odločitev, mora zadevni izbrani parlamentarni odbor opraviti preverjanje pred imenovanjem. Mnenje odbora se javno objavi ([84]).

(89) Mandat informacijskega pooblaščenca traja največ sedem let. Posameznik je lahko za informacijskega pooblaščenca imenovan le enkrat. Informacijskega pooblaščenca lahko s funkcije razreši kraljica, na podlagi nagovora obeh domov parlamenta ([85]). Predloga za razrešitev informacijskega pooblaščenca ni mogoče predložiti nobenemu od domov parlamenta brez poročila pristojnega nižjega ministra, iz katerega izhaja, da je po njegovem mnenju informacijski pooblaščenec kriv hujše kršitve dolžnega ravnanja uradnih oseb in/ali da ne izpolnjuje več pogojev za opravljanje svoje funkcije ([86]).

(90) Financiranje informacijskega pooblaščenca temelji na treh virih: (i) pristojbinah za varstvo podatkov, ki jih plačujejo upravljavci in so določene s predpisi pristojnega ministra ([87]) (Data Protection (Charges and Information) Regulations 2018 (predpisi o varstvu podatkov, pristojbinah in informacijah iz leta 2018)); te znašajo od 85 % do 90 % letnega proračuna urada ([88]); (ii) nepovratnih sredstvih, ki jih informacijskemu pooblaščencu nameni vlada. Ta sredstva so namenjena predvsem financiranju operativnih stroškov informacijskega pooblaščenca v zvezi z nalogami, ki se ne nanašajo na varstvo podatkov ([89]), in (iii) pristojbinah, ki se zaračunavajo za opravljanje storitev ([90]). Trenutno se take pristojbine ne zaračunavajo.

(91) Splošne naloge informacijskega pooblaščenca v zvezi z obdelavo osebnih podatkov, na katere se nanaša UK GDPR, so navedene v členu 57 UK GDPR, ki tesno odraža ustrezna pravila iz Uredbe (EU) 2016/679. Med njegovimi nalogami so spremljanje in izvrševanje UK GDPR, ozaveščanje javnosti, obravnava pritožb posameznikov, na katere se nanašajo osebni podatki, vodenje preiskav itd. Poleg tega so v členu 115 zakona o varstvu podatkov iz leta 2018 navedene druge splošne naloge informacijskega pooblaščenca, ki vključujejo obveznost svetovanja parlamentu,

([83]) Governance Code on Public Appointments (Kodeks upravljanja v zvezi z javnimi imenovanji) je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) Drugo poročilo o srečanjih odbora spodnjega doma parlamenta za kulturo, medije in šport za obdobje 2015–2016 je na voljo na povezavi: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) Nagovor (Address) je predlog, predložen parlamentu, katerega namen je monarha opozoriti na stališča parlamenta o posameznem vprašanju.

([86]) Točka 3(3) dodatka 12 k zakonu o varstvu podatkov iz leta 2018.

([87]) Člen 137 zakona o varstvu podatkov iz leta 2018, glej uvodno izjavo (17).

([88]) Člena 137 in 138 zakona o varstvu podatkov iz leta 2018 vsebujeta več zaščitnih ukrepov, da se zagotovi ustrezna raven pristojbin. Člen 137(4) vsebuje seznam vprašanj, ki jih mora pristojni minister upoštevati pri sprejemanju predpisov, ki določajo višino plačil raznih organizacij. Člen 138(1) in člen 182 zakona o varstvu podatkov iz leta 2018 vsebujeta tudi pravno zahtevo, da se mora pristojni minister pred sprejetjem predpisov posvetovati z informacijskim pooblaščencem in drugimi predstavniki oseb, na katere bodo predpisi verjetno vplivali, da se omogoči upoštevanje njihovih stališč. Poleg tega mora informacijski pooblaščenec na podlagi člena 138(2) zakona o varstvu podatkov iz leta 2018 redno preverjati učinkovanje predpisov o pristojbinah in lahko ministru predlaga njihove spremembe. Nazadnje, razen kadar so predpisi izdani zgolj zaradi upoštevanja zvišanja indeksa maloprodajnih cen (v takem primeru se izvede postopek negativne potrditve), se glede predpisov izvede postopek pozitivne potrditve, kar pomeni, da se ti ne smejo izdati, dokler jih s sklepom ne potrdita spodnji in zgornji dom parlamenta.

([89]) V sporazumu o upravljanju je pojasnjeno, da „lahko pristojni minister opravi izplačila informacijskemu pooblaščencu iz sredstev, ki jih zagotovi parlament na podlagi točke 9 dodatka 12 k zakonu o varstvu podatkov iz leta 2018. Po posvetovanju z uradom informacijskega pooblaščenca ministrstvo za digitalne tehnologije, kulturo, medije in šport temu izplača ustrezne zneske (nepovratna sredstva), namenjene kritju upravnih stroškov urada informacijskega pooblaščenca ter izvrševanju nalog informacijskega pooblaščenca v zvezi s številnimi posebnimi nalogami, vključno z zagotavljanjem svobode obveščanja“ (sporazum o upravljanju za obdobje 2018–2021, točka 1.12, opomba 82).

([90]) Glej člen 134 zakona o varstvu podatkov iz leta 2018.

vladi ter drugim splošnim institucijam in organom o zakonodajnih in upravnih ukrepih, ki se nanašajo na varstvo pravic in svoboščin posameznikov glede obdelave osebnih podatkov, ter pristojnost izdati (na svojo pobudo ali na zahtevo) mnenje parlamentu, vladi ali drugim institucijam in organom ter javnosti o vseh zadevah, ki se nanašajo na varstvo osebnih podatkov. Informacijski pooblaščenec zaradi vzdrževanja neodvisnosti sodstva ne sme izvajati nalog v zvezi z obdelavo osebnih podatkov, ki jo izvaja posameznik ali sodišče v okviru svoje sodne pristojnosti. Vendar pa je nadzor nad sodstvom zagotovljen prek posebnih organov (glej uvodne izjave (99) do (103)).

2.6.2 *Izvrševanje, vključno s sankcijami*

(92) Pristojnosti informacijskega pooblaščenca so določene v členu 58 UK GDPR, ki ne uvaja nobenih bistvenih sprememb glede na ustrezne člene Uredbe (EU) 2016/679. Zakon o varstvu podatkov iz leta 2018 določa dodatna pravila o izvrševanju teh pristojnosti. Informacijski pooblaščenec je pristojen zlasti za to, da: (a) upravljavcu in obdelovalcu (v nekaterih primerih pa kateri koli drugi osebi) odredi, naj predloži potrebne informacije, z izdajo obvestila o predložitvi informacij (v nadaljnjem besedilu: obvestilo o predložitvi informacij) ([91]); (b) izvaja preiskave in preglede z izdajo obvestila o preverjanju, na podlagi katerega mora upravljavec ali obdelovalec informacijskemu pooblaščencu morda dovoliti vstop v določene prostore, pregled ali proučitev dokumentov ali opreme, razgovore z osebami, ki obdelujejo osebne podatke v imenu upravljavca itd. (v nadaljnjem besedilu: obvestilo o preverjanju ([92])); (c) na drug način pridobi dostop do dokumentov itd. upravljavcev in obdelovalcev ter dostop v njihove prostore, v skladu s členom 154 zakona o varstvu podatkov iz leta 2018 (v nadaljnjem besedilu: pooblastilo za vstop in pregled); (d) izvršuje popravne pristojnosti, tudi na podlagi opozoril in opominov ali z izdajo odločb v obliki obvestil o izvršitvi, s katerimi od upravljavcev/obdelovalcev zahteva določeno ukrepanje ali prenehanje izvajanja določenih ukrepov, vključno z odredbo, da mora upravljavec ali obdelovalec storiti kar koli, kar je navedeno v členu 58(2)(c) do (g) in (j) UK GDPR (v nadaljnjem besedilu: obvestilo o izvršitvi) ([93]), (e) ter izreče upravne globe v obliki obvestila o plačilnem nalogu (v nadaljnjem besedilu: obvestilo o plačilnem nalogu) ([94]). Slednje se lahko izda tudi, če javni organ ne ravna v skladu z določbami UK GDPR ([95]).

(93) Politika urada informacijskega pooblaščenca o regulativnih ukrepih (Regulatory Action Policy) določa okoliščine, v katerih se izdajo obvestilo o predložitvi informacij, obvestilo o preverjanju, obvestilo o izvršitvi ali obvestilo o plačilnem nalogu ([96]). Z obvestilom o izvršitvi, ki se izda kot odziv na pomanjkljivost upravljavca ali obdelovalca, se lahko izrečejo le zahteve, za katere informacijski pooblaščenec meni, da so ustrezne glede na namen odprave pomanjkljivosti. Obvestilo o izvršitvi ali o plačilnem nalogu se lahko izda le upravljavcu ali obdelovalcu v zvezi s kršitvami poglavja II UK GDPR (načela obdelave), členov 12 do 22 UK GDPR (pravice posameznika, na katerega se nanašajo osebni podatki), členov 25 do 39 UK GDPR (obveznosti upravljavcev in obdelovalcev) in členov 44 do 49 UK GDPR (mednarodni prenosi). Obvestilo o izvršitvi se lahko izda tudi, če upravljavec ne zagotovi skladnosti z zahtevo za plačilo pristojbine, kakor je določena v predpisih, izdanih na podlagi člena 137 zakona o varstvu podatkov iz leta 2018. Poleg tega se lahko organu za spremljanje na podlagi člena 41 ali ponudniku certificiranja izda obvestilo o izvršitvi, če ne izpolnjujeta svojih obveznosti na podlagi UK GDPR. Obvestilo o plačilnem nalogu se lahko izda tudi osebi, ki ni izvršila obvestila o predložitvi informacij, obvestila o preverjanju ali obvestila o izvršitvi.

(94) Na podlagi obvestila o plačilnem nalogu mora oseba informacijskemu pooblaščencu plačati znesek, naveden v obvestilu. Pri odločanju o tem, ali osebi izdati obvestilo o plačilnem nalogu in kako visoka naj bo globa, mora informacijski pooblaščenec upoštevati, kar je navedeno v členu 83(1) in (2) UK GDPR, ki je enak ustreznim pravilom iz Uredbe (EU) 2016/679 ([97]). V skladu s členom 83(4) in (5) sta najvišja zneska upravne globe v primeru neizpolnjevanja obveznosti iz navedenih določb 8700000 GBP oziroma 17500000 GBP. V primeru podjetij lahko informacijski pooblaščenec izreče globo tudi v obliki deleža svetovnega letnega prometa, če je ta višja. Tako kot pri

([91]) Člen 142 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 143 zakona o varstvu podatkov iz leta 2018).

([92]) Člen 146 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 147 zakona o varstvu podatkov iz leta 2018).

([93]) Členi 149 do 151 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 152 zakona o varstvu podatkov iz leta 2018).

([94]) Člen 155 zakona o varstvu podatkov iz leta 2018 in člen 83 UK GDPR.

([95]) To izhaja iz člena 155(1) zakona o varstvu podatkov iz leta 2018 v povezavi s členom 149(2) in (5) navedenega zakona ter člena 156(4) navedenega zakona, ki omejuje izdajanje obvestil o plačilnem nalogu samo za Crown Estate Commissioners in upravljavce kraljevega gospodinjstva v skladu s členom 209(4) zakona o varstvu podatkov iz leta 2018.

([96]) Regulatory Action Policy, na voljo na naslednji povezavi: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

([97]) Vključno z naravo in težo kršitve (ob upoštevanju narave, obsega ali namena zadevne obdelave ter števila posameznikov, na katere se nanašajo osebni podatki, in raven škode, ki so jo ti utrpeli), ali je kršitev naklepna ali posledica malomarnosti, vsemi ukrepi, ki jih je sprejel upravljavec, da bi omilil škodo, ki so jo utrpeli posamezniki, na katere se nanašajo osebni podatki, stopnjo odgovornosti upravljavca ali obdelovalca (ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih je ta sprejel), vsemi zadevnimi predhodnimi kršitvami upravljavca ali obdelovalca; stopnjo sodelovanja z informacijskim pooblaščencem, vrstami osebnih podatkov, ki jih zadeva kršitev, morebitnimi drugimi oteževalnimi ali olajševalnimi dejavniki v zvezi z okoliščinami primera, kot so pridobljene finančne koristi ali preprečene izgube, ki neposredno ali posredno izhajajo iz kršitve.

enakovrednih določbah Uredbe (EU) 2016/679 so ti zneski v členu 83(4) in (5) določeni kot 2 % oziroma 4 %. V primeru neizpolnitve obvestila o predložitvi informacij, obvestila o preverjanju ali obvestila o izvršitvi je najvišji znesek kazni, ki se lahko izreče na podlagi obvestila o plačilnem nalogu, 17500000 GBP oziroma v primeru podjetja 4 % svetovnega letnega prometa, odvisno od tega, kateri znesek je višji.

(95) Z UK GDPR in zakonom o varstvu podatkov iz leta 2018 so se okrepile tudi druge pristojnosti informacijskega pooblaščenca. Informacijski pooblaščenec lahko zdaj na primer izvaja obvezne preglede upravljavcev in obdelovalcev na podlagi obvestil o preverjanju, pri čemer je na podlagi predhodne zakonodaje (zakona o varstvu podatkov iz leta 1998) imel to pristojnost le glede osrednje vlade in zdravstvenih organizacij, ostali subjekti pa so morali s pregledi soglašati.

(96) Od sprejetja Uredbe (EU) 2016/679 urad informacijskega pooblaščenca na leto obravnava približno 40000 pritožb posameznikov, na katere se nanašajo osebni podatki ([98]), poleg tega pa opravi tudi približno 2000 preiskav po uradni dolžnosti ([99]). Večina pritožb se nanaša na pravice do dostopa do podatkov in do razkritja podatkov. Na podlagi preiskav informacijski pooblaščenec sprejema izvršilne ukrepe v raznih sektorjih. Natančneje, iz zadnjega letnega poročila informacijskega pooblaščenca (2019–2020) ([100]) izhaja, da je v zadevnem obdobju poročanja izdal 54 obvestil o predložitvi informacij, 8 obvestil o preverjanju, 7 obvestil o izvršitvi, 4 opozorila, 8 pregonov in 15 glob ([101]).

(97) To vključuje več pomembnih denarnih kazni, ki so bile izrečene na podlagi Uredbe (EU) 2016/679 in zakona o varstvu podatkov iz leta 2018. Natančneje, informacijski pooblaščenec je oktobra 2020 izrekel globo britanski letalski družbi v višini 20 milijonov GBP zaradi kršitve varstva podatkov, ki je prizadela več kot 400000 strank. Ob koncu oktobra 2020 je bila mednarodni hotelski verigi izrečena globa v višini 18,4 milijona GBP, ker ni zagotovila varstva osebnih podatkov milijonov strank, novembra 2020 pa je bila britanskemu ponudniku storitev, ki je prek spleta prodajal vstopnice za dogodke, izrečena globa v višini 1,25 milijona GBP, ker ni zagotovil varstva podatkov o plačilih strank ([102]).

(98) Poleg pooblastil, ki jih ima informacijski pooblaščenec za izvrševanje in so opisana v uvodni izjavi (92), se nekatere kršitve zakonodaje o varstvu podatkov štejejo za kazniva dejanja, zato se lahko zanje izrečejo kazenske sankcije (člen 196 zakona o varstvu podatkov iz leta 2018). To se na primer nanaša na namerno ali malomarno pridobitev ali razkritje osebnih podatkov brez privolitve upravljavca, zagotovitev razkritja osebnih podatkov drugi osebi brez privolitve upravljavca ([103]), ponovno identifikacijo informacij v primeru anonimizacije osebnih podatkov brez privolitve upravljavca, ki je odgovoren za anonimizacijo osebnih podatkov ([104]), namerno oviranje informacijskega pooblaščenca pri izvrševanju njegovih pristojnosti v zvezi s preverjanjem osebnih podatkov v skladu z mednarodnimi obveznostmi ([105]), dajanje neresničnih izjav v odgovor na obvestilo o predložitvi informacij, ali uničenje informacij v zvezi z obvestilom o predložitvi informacij ali obvestilom o preverjanju ([106]).

([98]) Iz informacij, ki so jih zagotovili organi Združenega kraljestva, izhaja, da v obdobju, na katerega se nanaša letno poročilo informacijskega pooblaščenca za obdobje 2019–2020, v približno 25 % primerov ni bila ugotovljena kršitev; v približno 29 % primerov je bil posameznik, na katerega se nanašajo osebni podatki, pozvan, naj se s pritožbo najprej obrne na upravljavca podatkov, naj počaka na njegov odgovor ali naj najprej zaključi pogovore z njim; v približno 17 % primerov ni bila ugotovljena kršitev, vendar je informacijski pooblaščenec upravljavcu podatkov zagotovil nasvet; v približno 25 % primerov je informacijski pooblaščenec ugotovil kršitev ter bodisi dal nasvet upravljavcu podatkov bodisi je od njega zahteval določene ukrepe; v približno 3 % primerov je bilo ugotovljeno, da pritožba ne spada na področje uporabe Uredbe (EU) 2016/679; približno 1 % primerov je bilo napotenih na drug organ za varstvo podatkov v okviru evropskega odbora za varstvo podatkov.

([99]) Urad informacijskega pooblaščenca lahko začne navedene preiskave na podlagi informacij, ki jih prejme iz raznih virov, vključno s prijavami kršitev varstva osebnih podatkov, predlogi drugih javnih organov Združenega kraljestva ali tujih organov za varstvo podatkov ter pritožbami posameznikov ali organizacij civilne družbe.

([100]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2019–2020 (opomba 81).

([101]) Iz predhodnega letnega poročila, ki se je nanašalo na obdobje 2018–2019, izhaja, da je informacijski pooblaščenec v obdobju poročanja izdal 22 obvestil o plačilnem nalogu na podlagi zakona o varstvu podatkov iz leta 1998, pri čemer je bil skupni znesek glob 3010610 GBP, vključno z dvema globama v višini 500000 GBP (najvišja dovoljena globa na podlagi zakona o varstvu podatkov iz leta 1998). Leta 2018 je informacijski pooblaščenec po razkritjih v zvezi z družbo Cambridge Analytica izvedel preiskavo uporabe analize podatkov v politične namene. Na podlagi preiskave so bili pripravljeni poročilo glede politike, več priporočil, družbi Facebook je bila izrečena globa v višini 500000 GBP, družbi Aggregate IQ, posredniku podatkov iz Kanade, pa je bilo izdano obvestilo o izvršitvi, na podlagi katerega je morala izbrisati osebne podatke, ki jih je imela o državljanih in prebivalcih Združenega kraljestva (glej letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2018–2019, ki je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Povzetek sprejetih izvršilnih ukrepov je na voljo na spletišču urada informacijskega pooblaščenca na povezavi: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Člen 170 zakona o varstvu podatkov iz leta 2018.

([104]) Člen 171 zakona o varstvu podatkov iz leta 2018.

([105]) Člen 119 zakona o varstvu podatkov iz leta 2018.

([106]) Člena 144 in 148 zakona o varstvu podatkov iz leta 2018.

2.6.3 *Nadzor nad sodstvom*

(99) Nadzor nad obdelavo osebnih podatkov, ki jo izvajajo sodišča in sodstvo, je dvostranski. Kadar nosilec sodne funkcije ali sodišče ne deluje v okviru svoje sodne pristojnosti, nadzor izvaja urad informacijskega pooblaščenca. Kadar pa upravljavec deluje v okviru svoje sodne pristojnosti, urad informacijskega pooblaščenca ne more izvajati svoje nadzorne funkcije ([107]), zato jo izvajajo posebni organi. To odraža pristop iz Uredbe (EU) 2016/679 (člen 55(3)).

(100) Natančneje, v drugem primeru glede sodišč Anglije in Walesa ter glede prvostopenjskih in višjih sodišč Anglije in Walesa tak nadzor zagotavlja sodni svet za varstvo podatkov (Judicial Data Protection Panel) ([108]). Poleg tega sta vodja sodstva Anglije in Walesa (Lord Chief Justice) in vodja sodišč Tribunals (Senior President of Tribunals) izdala obvestilo o zasebnosti ([109]), ki določa, kako sodišča v Angliji in Walesu obdelujejo osebne podatke za namene opravljanja sodne funkcije. Podobni obvestili sta izdali tudi sodstvo Severne Irske ([110]) in sodstvo Škotske ([111]).

(101) Še več, na Severnem Irskem je vodja sodstva Severne Irske sodnika sodišča High Court imenoval za sodnika, pristojnega za nadzor podatkov (Data Supervisory Judge) ([112]). Poleg tega so izdali smernice za sodstvo Severne Irske o tem, kako ravnati v primeru izgube ali potencialne izgube podatkov ter kako obravnavati vsa vprašanja, ki iz tega izhajajo ([113]).

(102) Na Škotskem je vodja sodstva (Lord President) imenoval sodnika za nadzor podatkov (Data Supervisory Judge) za obravnavo vseh pritožb s področja varstva podatkov. Ta sistem je vzpostavljen na podlagi pravil o pritožbah v sodstvu, ki so podobna tistim v Angliji in Walesu ([114]).

(103) Nazadnje, eden od sodnikov pri sodišču Supreme Court je pooblaščen za nadzor nad varstvom podatkov.

2.6.4 *Pravna sredstva*

(104) Posameznik, na katerega se nanašajo osebni podatki, mora imeti na voljo učinkovito upravno in sodno varstvo, vključno z odškodnino za škodo, da se zagotovita ustrezno varstvo in zlasti uresničevanje pravic posameznika.

([107]) Člen 117 zakona o varstvu podatkov iz leta 2018.

([108]) Naloga sveta je zagotavljati smernice in usposabljanje v sodstvu. Obravnava tudi pritožbe posameznikov, na katere se nanašajo osebni podatki, v zvezi z obdelavo osebnih podatkov s strani sodišč in posameznikov, ki izvajajo sodno pristojnost. Cilj sveta je zagotoviti način za reševanje vsake pritožbe. Če pritožnik ni zadovoljen z odločitvijo sveta in če predloži dodatne dokaze, lahko svet znova prouči svojo odločitev. Čeprav svet sam ne izreka finančnih sankcij, lahko zadevo preda uradu za preiskave ravnanja pravosodnih organov (Judicial Conduct Investigation Office), če meni, da je bila storjena dovolj resna kršitev zakona o varstvu podatkov iz leta 2018, navedeni urad nato pritožbo prouči. Če je pritožba potrjena, lord kancler in vodja sodstva Anglije in Walesa (ali višji sodnik, ki ga ta pooblasti) odloči, kateri ukrepi se sprejmejo zoper nosilca funkcije. To lahko vključuje (po vrstnem redu glede na težo): uradni nasvet, uradno opozorilo, opomin in nazadnje razrešitev s položaja. Če posameznik ni zadovoljen z načinom, kako je urad za preiskave ravnanja pravosodnih organov obravnaval pritožbo, se lahko nadalje pritoži varuhu pravic v zvezi z imenovanji v pravosodju in ravnanjem pravosodnih organov (Judicial Appointments and Conduct Ombudsman; glej https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Varuh pravic lahko od urada za preiskave ravnanja pravosodnih organov zahteva ponovno obravnavo pritožbe in predlaga izplačilo odškodnine pritožniku, če meni, da je ta zaradi nepravilnosti utrpel škodo.

([109]) Obvestilo vodje sodstva Anglije in Walesa ter vodje sodišč Tribunals o zasebnosti je na voljo na povezavi: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) Obvestilo vodje sodstva Severne Irske o zasebnosti je na voljo na povezavi: https://judiciaryni.uk/data-privacy.

([111]) Obvestilo o zasebnosti, ki se nanaša na škotska sodišča, je na voljo na povezavi: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) Sodnik, pristojen za nadzor podatkov, zagotavlja smernice sodstvu ter obravnava kršitve in/ali pritožbe v zvezi z obdelavo osebnih podatkov s strani sodišč ali posameznikov, ki izvajajo svojo sodno pristojnost.

([113]) Če se šteje, da gre za resno pritožbo ali težjo kršitev, se zadeva predloži uradniku za obravnavo pritožb v sodstvu (Judicial Complaints Officer) v nadaljnjo obravnavo, v skladu s kodeksom ravnanja glede pritožb, ki ga je izdal vodja sodstva Severne Irske. Rezultat take pritožbe je lahko, da se ne sprejme noben nadaljnji ukrep, izdaja nasveta, usposabljanje ali mentorstvo, neuradno opozorilo, uradno opozorilo, zadnje opozorilo, omejitev delovanja ali napotitev pred sodišče, ustanovljeno na podlagi zakona. Kodeks ravnanja glede pritožb (Code of Practice on Complaints), ki ga je izdal vodja sodstva Severne Irske, je na voljo na povezavi: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([114]) Vsako utemeljeno pritožbo obravnava sodnik za nadzor podatkov, nato pa se predloži vodji sodstva, ki je pristojen izdati nasvet, uradno opozorilo ali opomin, če meni, da je to potrebno (enakovredna pravila obstajajo glede članov sodišč in so na voljo na povezavi: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Prvič, posameznik, na katerega se nanašajo osebni podatki, ima pravico vložiti pritožbo pri informacijskem pooblaščencu, če meni, da je v zvezi z osebnimi podatki, ki se nanašajo nanj, prišlo do kršitve UK GDPR ([115]). V UK GDPR so brez bistvenih sprememb ohranjena pravila iz člena 77 Uredbe (EU) 2016/679 o navedeni pravici. Enako velja za člen 57(1)(f) in (2), ki določa naloge informacijskega pooblaščenca v zvezi z obravnavo pritožb. Kot je opisano v uvodnih izjavah (92) do (98) above, lahko informacijski pooblaščenec preverja zagotavljanje skladnosti upravljavca in obdelovalca z UK GDPR in zakonom o varstvu podatkov iz leta 2018, od njiju zahteva, da v primeru neskladnosti sprejmeta potrebne ukrepe ali se vzdržita določenih ukrepov ter izreče globe.

(106) Drugič, UK GDPR in zakon o varstvu podatkov iz leta 2018 določata pravico do pravnega sredstva zoper odločitev informacijskega pooblaščenca. Na podlagi člena 78(1) UK GDPR ima posameznik pravico do učinkovitega pravnega sredstva zoper pravno zavezujočo odločitev informacijskega pooblaščenca v zvezi z njim. V okviru sodne presoje sodnik prouči v zahtevku izpodbijano odločbo in odloči, ali je informacijski pooblaščenec ravnal zakonito. Nadalje, iz člena 78(2) UK GDPR izhaja, da če informacijski pooblaščenec pritožbe posameznika, na katerega se nanašajo osebni podatki, ne obravnava ustrezno ([116]), ima pritožnik na voljo pravno sredstvo. Od sodišča prve stopnje lahko zahteva, naj informacijskemu pooblaščencu naloži ustrezne ukrepe v odgovor na pritožbo ali da pritožnika obvesti o stanju zadeve ([117]). Poleg tega se lahko vsakdo, ki mu informacijski pooblaščenec izda eno od zgoraj navedenih obvestil (o predložitvi informacij, o preverjanju, o izvršitvi ali o plačilnem nalogu), pritoži pri sodišču prve stopnje (First Tier Tribunal) ([118]). Če sodišče ugotovi, da odločba informacijskega pooblaščenca ni v skladu s pravom ali da bi moral informacijski pooblaščenec odločiti drugače, mora sodišče pritožbo dovoliti ali obvestilo oziroma odločbo informacijskega pooblaščenca nadomestiti z drugo.

(107) Tretjič, posamezniki lahko pravna sredstva zoper upravljavce in obdelovalce uveljavljajo neposredno pred sodiščem v skladu s členom 79 UK GDPR in členom 167 zakona o varstvu podatkov iz leta 2018. Če sodišče na podlagi vloge posameznika, na katerega se nanašajo osebni podatki, ugotovi, da so bile kršene njegove pravice s področja zakonodaje o varstvu podatkov, lahko upravljavcu, ki je zadolžen za obdelavo takih podatkov, ali obdelovalcu, ki deluje v njegovem imenu, odredi sprejetje ali opustitev določenih ukrepov, navedenih v odločbi.

(108) Poleg tega ima v skladu s členom 82 UK GDPR in členom 168 zakona o varstvu podatkov iz leta 2018 vsak posameznik, ki je utrpel premoženjsko ali nepremoženjsko škodo kot posledico kršitve UK GDPR, pravico, da od upravljavca ali obdelovalca dobi odškodnino za nastalo škodo. Pravila o odškodnini in odgovornosti iz člena 82(1) do (5) UK GDPR so enaka ustreznim pravilom iz Uredbe (EU) 2016/679. V skladu s členom 168 zakona o varstvu podatkov iz leta 2018 nepremoženjska škoda vključuje tudi stisko. V skladu s členom 80 UK GDPR ima posameznik, na katerega se nanašajo osebni podatki, tudi pravico, da pooblasti zastopnika ali organizacijo, da v njegovem imenu vloži pritožbo pri informacijskem pooblaščencu (v skladu s členom 77 UK GDPR) in pravico, da v njegovem imenu uresničuje pravice iz člena 78 (pravica do učinkovitega pravnega sredstva zoper informacijskega pooblaščenca), člena 79 (pravica do učinkovitega pravnega sredstva zoper upravljavca ali obdelovalca) in člena 82 (pravica do odškodnine in odgovornost) UK GDPR.

(109) Četrtič, poleg zgornjih možnosti za uveljavljanje pravnih sredstev lahko vsakdo, ki meni, da so javni organi kršili njegove pravice, vključno s pravico do zasebnosti in varstva podatkov, uveljavlja pravna sredstva pred sodišči Združenega kraljestva na podlagi zakona o človekovih pravicah iz leta 1998 ([119]). Posameznik, ki trdi, da je javni organ ravnal (ali predlaga ravnanje) neskladno s pravico iz konvencije, kar je posledično nezakonito na podlagi člena 6(1) zakona o človekovih pravicah iz leta 1998, lahko pri pristojnem sodišču začne postopek zoper tak organ ali se na zadevne pravice sklicuje v vsakem pravnem postopku, če je (ali bo postal) žrtev nezakonitega dejanja.

(110) Če sodišče ugotovi, da je katero koli dejanje javnega organa nezakonito, lahko odobri odškodnino ali pravno sredstvo ali izda odločbo, kot meni, da je pravično in ustrezno ter v skladu s svojimi pristojnostmi ([120]). Sodišče lahko odloči tudi, da določba primarne zakonodaje ni skladna s pravico na podlagi konvencije.

([115]) Člen 77 UK GDPR.

([116]) Člen 166 zakona o varstvu podatkov iz leta 2018 se nanaša predvsem na naslednje okoliščine: (a) če informacijski pooblaščenec ne sprejme ustreznih ukrepov v odgovor na pritožbo; (b) če informacijski pooblaščenec pritožnika ne obvesti o stanju zadeve ali odločitvi o pritožbi v treh mesecih od dne, ko informacijski pooblaščenec prejme pritožbo; ali (c) če informacijski pooblaščenec v navedenem roku ne odloči o pritožbi in pritožnika ne obvesti o tem v nadaljnjih treh mesecih.

([117]) Člen 78(2) UK GDPR in člen 166 zakona o varstvu podatkov iz leta 2018.

([118]) Člen 78(1) UK GDPR in člen 162 zakona o varstvu podatkov iz leta 2018.

([119]) Člen 7(1) zakona o človekovih pravicah iz leta 1998. V skladu s členom 7(7) je oseba žrtev nezakonitega dejanja le, če bi bila žrtev tudi na podlagi člena 34 Evropske konvencije o varstvu človekovih pravic, če bi se v zvezi z navedenim dejanjem začel postopek pred Evropskim sodiščem za človekove pravice.

([120]) Člen 8(1) zakona o človekovih pravicah iz leta 1998.

(111) Nazadnje, ko posameznik izčrpa nacionalna pravna sredstva, se lahko obrne na Evropsko sodišče za človekove pravice zaradi kršitev pravic, zagotovljenih na podlagi Evropske konvencije o varstvu človekovih pravic.

3. DOSTOP DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V ZDRUŽENEM KRALJESTVU, IN NJIHOVA UPORABA

(112) Komisija je presojala tudi pravni okvir Združenega kraljestva glede zbiranja in posledične uporabe osebnih podatkov, ki jih v javnem interesu javni organi v Združenem kraljestvu prenesejo poslovnim subjektom v Združenem kraljestvu, zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in nacionalne varnosti (v nadaljnjem besedilu: vladni dostop). Komisija je pri oceni pogojev, na podlagi katerih vladni dostop do podatkov, prenesenih v Združeno kraljestvo, na podlagi tega sklepa izpolnjuje preskus „osnovne enakovrednosti“ na podlagi člena 45(1) Uredbe (EU) 2016/679, kakor ga razlaga Sodišče EU glede na Listino o temeljnih pravicah, upoštevala zlasti naslednja merila.

(113) Prvič, vsaka omejitev pravice do varstva osebnih podatkov mora biti določena v zakonu, pravna podlaga, ki dovoljuje tak poseg v uresničevanje pravice, pa mora že sama opredeljevati obseg omejitve izvrševanja zadevne pravice ([121]).

(114) Drugič, da se izpolni zahteva glede sorazmernosti, v skladu s katero se lahko odstopanja od in omejitve varstva osebnih podatkov uporabljajo le, kolikor je nujno potrebno v demokratični družbi, da se dosežejo specifični cilji splošnega interesa, ki so enakovredni interesom, priznanim v Uniji, morajo biti z zakonodajo zadevne tretje države, s katero se ureja poseg, določena jasna in natančna pravila, ki urejajo obseg in uporabo zadevnega ukrepa ter minimalne zahteve, tako da imajo osebe, katerih podatki so bili preneseni, na voljo zadostna jamstva, ki omogočajo učinkovito varovanje njihovih osebnih podatkov pred tveganjem zlorab ([122]). V zakonodaji mora biti zlasti navedeno, v kakšnih okoliščinah in pod katerimi pogoji je mogoče sprejeti ukrep, ki določa obdelavo takih podatkov ([123]), izpolnjevanje teh zahtev pa mora biti podvrženo neodvisnemu nadzoru ([124]).

(115) Tretjič, navedena zakonodaja mora biti pravno zavezujoča na podlagi notranjega prava, za te pravne zahteve pa mora veljati, da ne zavezujejo le organov, ampak so tudi sodno izvršljive zoper organe zadevne tretje države ([125]). Posamezniki, na katere se nanašajo osebni podatki, morajo zlasti imeti možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da bi si tako zagotovili dostop do osebnih podatkov, ki se nanje nanašajo, ali dosegli popravo oziroma izbris takih podatkov ([126]).

3.1 Splošni pravni okvir

(116) V okviru izvajanja pooblastil javnega organa mora biti vladni dostop v Združenem kraljestvu izveden ob popolnem upoštevanju zakona. Združeno kraljestvo je ratificiralo Evropsko konvencijo o varstvu človekovih pravic (glej uvodno izjavo (9)), zato morajo vsi javni organi v Združenem kraljestvu ravnati v skladu z navedeno konvencijo ([127]). Člen 8 konvencije določa, da mora biti vsak poseg v zasebnost v skladu s pravom, v interesu enega od ciljev iz člena 8(2) in sorazmeren glede na cilj. Člen 8 določa tudi, da mora biti poseg „predvidljiv“, tj. da ima jasno in dostopno pravno podlago in da pravo vsebuje ustrezne zaščitne ukrepe za preprečevanje zlorab.

(117) Poleg tega je Sodišče EU v svoji sodni praksi navedlo, da mora biti vsak poseg v pravico do zasebnosti in varstva podatkov podvržen učinkovitemu, neodvisnemu in nepristranskemu nadzornemu sistemu, ki ga zagotavlja sodnik ali drug neodvisni organ ([128]) (na primer upravni ali parlamentarni organ).

([121]) Glej sodbo v zadevi Schrems II, točki 174 in 175 ter navedeno sodno prakso. Glede dostopa javnih organov držav članic glej tudi sodbo z dne 6. oktobra 2020, Privacy International, C-623/17, EU:C:2020:790, točka 65, in sodbo z dne 6. oktobra 2020, La Quadrature du Net in drugi, združene zadeve C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 175.

([122]) Glej sodbo v zadevi Schrems II, točki 176 in 181 ter navedeno sodno prakso. Glede dostopa javnih organov držav članic glej tudi sodbi v zadevi Privacy International, točka 68, in v zadevi La Quadrature du Net in drugi, točka 132.

([123]) Glej sodbo v zadevi Schrems II, točka 176. Glede dostopa javnih organov držav članic glej tudi sodbi v zadevi Privacy International, točka 68, in v zadevi La Quadrature du Net in drugi, točka 132.

([124]) Glej sodbo v zadevi Schrems II, točka 179.

([125]) Glej sodbo v zadevi Schrems II, točki 181 in 182.

([126]) Glej sodbi v zadevi Schrems I, točka 95, in v zadevi Schrems II, točka 194. V tem smislu je Sodišče EU poudarilo predvsem, da skladnost s členom 47 Listine o temeljnih pravicah, ki zagotavlja pravico do učinkovitega pravnega sredstva in nepristranskega sodišča, „prispeva k ravni varstva, ki se zahteva v Uniji, in katere spoštovanje mora Komisija ugotoviti, preden sprejme sklep o ustreznosti na podlagi člena 45(1) Splošne uredbe o varstvu podatkov“ (sodba v zadevi Schrems II, točka 186).

([127]) Člen 6 zakona o človekovih pravicah iz leta 1998.

([128]) Evropsko sodišče za človekove pravice, Klass in drugi proti Nemčiji, pritožba št. 5029/71, točke 17 do 51.

(118) Poleg tega morajo imeti posamezniki učinkovita pravna sredstva, Evropsko sodišče za človekove pravice pa je pojasnilo, da mora pravno sredstvo zagotavljati neodvisen in nepristranski organ, ki sprejme svoj poslovnik, sestavljati ga morajo člani, ki imajo ali so imeli visoko sodno funkcijo ali ki so izkušeni odvetniki, hkrati pa ne sme obstajati dokazno breme, ki bi ga bilo treba premagati za vložitev vloge pri takem organu. Pri obravnavi pritožb posameznikov mora imeti neodvisen in nepristranski organ dostop do vseh zadevnih informacij, vključno s tajnim gradivom. Nazadnje, organ mora imeti pristojnost odpraviti neskladnost ([129]).

(119) Združeno kraljestvo je leta 2018 ratificiralo tudi Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108) ter podpisalo protokol o spremembi navedene konvencije (znan kot Konvencija št. 108+) ([130]). Člen 9 Konvencije št. 108 določa, da so odstopanja od splošnih načel o varstvu podatkov (člen 5, Kakovost podatkov), pravil o posebnih vrstah podatkov (člen 6, Posebne vrste podatkov) in od pravic posameznikov, na katere se nanašajo osebni podatki (člen 8, Dodatni zaščitni ukrepi za posameznika, na katerega se nanašajo osebni podatki), dovoljena le, kadar je tako odstopanje določeno v zakonu podpisnice in če gre za ukrep, ki je v interesu zaščite nacionalne varnosti, javne varnosti, monetarnih interesov države, zatiranja kaznivih dejanj ali varstva posameznika, na katerega se nanašajo osebni podatki, oziroma pravic in svoboščin drugih potreben v demokratični družbi ([131]).

(120) Združeno kraljestvo torej na podlagi članstva v Svetu Evrope, zavezanosti Evropski konvenciji o varstvu človekovih pravic ter priznanja pristojnosti Evropskega sodišča za človekove pravice zavezuje več obveznosti iz mednarodnega prava, ki oblikujejo njegov sistem vladnega dostopa na podlagi načel, zaščitnih ukrepov in pravic posameznikov, ki so podobni tistim, ki so zagotovljeni na podlagi prava EU in ki se uporabljajo v državah članicah. Kot je poudarjeno v uvodni izjavi (19), je nadaljnja zavezanost takim instrumentom posebno pomemben element ocene, na kateri temelji ta sklep.

(121) Nadalje, posebne zaščitne ukrepe in pravice za varstvo podatkov zagotavlja tudi zakon o varstvu podatkov iz leta 2018, če podatke obdelujejo javni organi, vključno z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in organi nacionalne varnosti.

(122) Ureditev obdelave osebnih podatkov v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je določena v delu 3 zakona o varstvu podatkov iz leta 2018, ki je bil sprejet za prenos Direktive (EU) 2016/680. Del 3 zakona o varstvu podatkov iz leta 2018 se nanaša na obdelavo osebnih podatkov s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem ([132]).

(123) Pojem „pristojni organ“ je v členu 30 zakona o varstvu podatkov opredeljen kot oseba s seznama v dodatku 7 k zakonu o varstvu podatkov iz leta 2018 oziroma katera koli druga oseba, ki ima zakonsko predpisane naloge za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([133]). Kot je pojasnjeno v nadaljevanju (glej uvodno izjavo (139)), lahko nekateri pristojni organi (na primer National Crime Agency) pod določenimi pogoji uporabijo pooblastila iz zakona o preiskovalnih pooblastilih iz leta 2016 (Investigatory Power Act 2016). V tem primeru se bodo poleg zaščitnih ukrepov iz dela 3 zakona o varstvu podatkov iz leta 2018 uporabljali tudi zaščitni ukrepi iz zakona o preiskovalnih pooblastilih iz leta 2016. Obveščevalne službe (tajna obveščevalna služba, varnostna služba in vladna obveščevalna služba) niso „pristojni organi“ ([134]) iz dela 3 zakona o varstvu podatkov iz leta 2018, zato se v njem določena pravila ne uporabljajo za nobeno od njihovih dejavnosti. Specifičen del zakona o varstvu podatkov iz leta 2018 (del 4) je namenjen obdelavi osebnih podatkov s strani obveščevalnih služb (za več podrobnosti glej uvodno izjavo (125)).

([129]) Evropsko sodišče za človekove pravice, Kennedy proti Združenemu kraljestvu, pritožba št. 26839/05, (v nadaljnjem besedilu: Kennedy), točki 167 in 190.

([130]) Več informacij o Evropski konvenciji o varstvu človekovih pravic in njeni vključitvi v pravo Združenega kraljestva na podlagi zakona o človekovih pravicah iz leta 1998 ter o Konvenciji št. 108 je na voljo v uvodni izjavi (9) zgoraj.

([131]) Podobno so na podlagi člena 11 Konvencije št. 108+ omejitve nekaterih posameznih pravic in obveznosti na podlagi Konvencije za namene nacionalne varnosti ali za preprečevanje, preiskovanje in pregon kaznivih dejanj ter za izvrševanje kazenskih sankcij dovoljene le, če je taka omejitev določena z zakonom, če upošteva bistvo temeljnih pravic in svoboščin ter če gre za potreben in sorazmeren ukrep v demokratični družbi. Dejavnosti obdelave za namene nacionalne varnosti in obrambe morajo biti podvržene tudi neodvisnemu in učinkovitemu pregledu in nadzoru na podlagi notranje zakonodaje zadevne podpisnice konvencije.

([132]) Člen 31 zakona o varstvu podatkov iz leta 2018.

([133]) Pristojni organi iz dodatka 7 vključujejo policijo, pa tudi vsa ministrstva in druge organe, ki so jim zaupane preiskovalne naloge (npr. Commissioner for Her Majesty's Revenue and Customs, National Crime Agency, Welsh Revenue Authority, Competition and Markets Authority ali Her Majesty's Land Register), agencije za pregon, druge agencije kazenskega pravosodja in druge posameznike ali organizacije, ki izvajajo dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (med temi so v dodatku 7 zakona o varstvu podatkov iz leta 2018 navedeni Directors of Public Prosecutors, Director of Public Prosecutors for Northern Ireland in Information Commission).

([134]) Člen 30(2) zakona o varstvu podatkov iz leta 2018.

(124) Po vzoru Direktive (EU) 2016/680 tudi del 3 zakona o varstvu podatkov iz leta 2018 določa načela zakonitosti in poštenosti ([135]), omejitve namena ([136]), najmanjšega obsega podatkov ([137]), točnosti ([138]), omejitve hrambe ([139]) in varstva ([140]). Zakonodaja določa posebne obveznosti glede preglednosti ([141]) ter posameznikom zagotavlja pravico do dostopa ([142]), popravka in izbrisa ([143]) ter pravico, da se zanje ne uporablja avtomatizirano sprejemanje odločitev ([144]) Pristojni organi morajo avtomatično zagotavljati varstvo podatkov, voditi evidenco dejavnosti obdelave ter glede nekaterih dejanj obdelave izvesti ocene učinka v zvezi z varstvom podatkov in se vnaprej posvetovati z informacijskim pooblaščencem ([145]). V skladu s členom 56 zakona o varstvu podatkov iz leta 2018 morajo dokazati skladnost. Poleg tega morajo vzpostaviti tudi ustrezne ukrepe za zagotovitev varnosti obdelave ([146]), v primeru kršitve varstva podatkov pa imajo tudi posebne obveznosti, vključno z obveščanjem informacijskega pooblaščenca in posameznika, na katerega se nanašajo osebni podatki, o taki kršitvi ([147]). Kot je navedeno v Direktivi (EU) 2016/680, mora upravljavec (razen če gre za sodišče ali drug pravosodni organ, ki izvršuje svojo sodno pristojnost) imenovati uradnika za varstvo podatkov ([148]), ki mu pomaga pri zagotavljanju skladnosti z obveznostmi ter pri spremljanju zagotavljanja skladnosti ([149]). Nadalje, zakonodaja določa posebne zahteve glede mednarodnih prenosov osebnih podatkov v tretje države ali mednarodne organizacije za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, da se zagotovi kontinuiteta varstva ([150]). Komisija je na isti datum sprejela ta sklep in sklep o ustreznosti na podlagi člena 36(3) Direktive (EU) 2016/680, v katerem je ugotovila, da ureditev varstva podatkov, ki se uporablja glede obdelave podatkov s strani organov Združenega kraljestva za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, zagotavlja raven varstva, ki je v osnovi enakovredna tisti, ki jo zagotavlja Direktiva (EU) 2016/680.

(125) Del 4 zakona o varstvu podatkov iz leta 2018 se uporablja za vse primere obdelave, ki jih izvajajo obveščevalne službe ali ki se izvajajo v njihovem imenu. V njem so zlasti določena glavna načela o varstvu podatkov (zakonitost, poštenost in preglednost ([151]), omejitev namena ([152]), najmanjši obseg podatkov ([153]), točnost ([154]), omejitev hrambe ([155]) in varstva ([156])), poleg tega določa pogoje glede obdelave posebnih vrst podatkov ([157]), določa pravice posameznikov, na katere se nanašajo osebni podatki ([158]), zahteva vgrajeno

([135]) Člen 35 zakona o varstvu podatkov iz leta 2018.
([136]) Člen 36 zakona o varstvu podatkov iz leta 2018.
([137]) Člen 37 zakona o varstvu podatkov iz leta 2018.
([138]) Člen 38 zakona o varstvu podatkov iz leta 2018.
([139]) Člen 39 zakona o varstvu podatkov iz leta 2018.
([140]) Člen 40 zakona o varstvu podatkov iz leta 2018.
([141]) Člen 44 zakona o varstvu podatkov iz leta 2018.
([142]) Člen 45 zakona o varstvu podatkov iz leta 2018.
([143]) Člena 46 in 47 zakona o varstvu podatkov iz leta 2018.
([144]) Člena 49 in 50 zakona o varstvu podatkov iz leta 2018.
([145]) Členi 56 do 65 zakona o varstvu podatkov iz leta 2018.
([146]) Člen 66 zakona o varstvu podatkov iz leta 2018.
([147]) Člena 67 in 68 zakona o varstvu podatkov iz leta 2018.
([148]) Členi 69 do 71 zakona o varstvu podatkov iz leta 2018.
([149]) Člena 67 in 68 zakona o varstvu podatkov iz leta 2018.
([150]) Poglavje 5 dela 3 zakona o varstvu podatkov iz leta 2018.
([151]) V skladu s členom 86(6) zakona o varstvu podatkov iz leta 2018 je treba pri ugotavljanju poštenosti in preglednosti obdelave upoštevati tudi metodo pridobitve podatkov. V tem smislu je zahteva glede poštenosti in preglednosti izpolnjena, če so podatki pridobljeni od osebe, ki je zakonito pooblaščena, da jih lahko zagotovi, ali ki jih na podlagi zakona mora zagotoviti.
([152]) V skladu s členom 87 zakona o varstvu podatkov iz leta 2018 mora biti namen obdelave specifičen, izrecen in zakonit. Podatki se ne smejo obdelovati na način, ki ni skladen z nameni, za katere so bili zbrani. V skladu s členom 87(3) zakona o varstvu podatkov iz leta 2018 je nadaljnja obdelava osebnih podatkov dovoljena le, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni namen ter če je obdelava potrebna in sorazmerna z navedenim drugim namenom. Obdelava se šteje za skladno, če se izvaja za namene arhiviranja v javnem interesu, za namene znanstvenih ali zgodovinskih raziskav ali za statistične namene in če zanjo veljajo ustrezni zaščitni ukrepi (člen 87(4) zakona o varstvu podatkov iz leta 2018).
([153]) Osebni podatki morajo biti ustrezni, relevantni in ne smejo biti prekomerni (člen 88 zakona o varstvu podatkov iz leta 2018).
([154]) Osebni podatki morajo biti točni in posodobljeni (člen 89 zakona o varstvu podatkov iz leta 2018).
([155]) Osebnih podatkov se ne sme hraniti dlje, kot je potrebno (člen 90 zakona o varstvu podatkov iz leta 2018).
([156]) Šesto načelo o varstvu podatkov je, da je treba osebne podatke obdelovati tako, da so upoštevani ustrezni zaščitni ukrepi glede tveganj, ki izhajajo iz obdelave osebnih podatkov. Tveganja med drugim vključujejo nenameren ali nepooblaščen dostop do osebnih podatkov, njihovo uničenje, izgubo, uporabo, spreminjanje ali razkritje (člen 91 zakona o varstvu podatkov iz leta 2018). Člen 107 zahteva tudi, da (1) mora vsak upravljavec vzpostaviti ustrezne zaščitne ukrepe, ki so primerni glede na tveganja, ki izhajajo iz obdelave osebnih podatkov, (2) v primeru avtomatizirane obdelave pa mora vsak upravljavec in vsak obdelovalec na podlagi ocene tveganja vzpostaviti preventivne ukrepe ali ukrepe za zmanjšanje tveganja.
([157]) Člen 86(2)(b) in dodatek 10 k zakonu o varstvu podatkov iz leta 2018.
([158]) V skladu s poglavjem 3 dela 4 zakona o varstvu podatkov iz leta 2018 gre predvsem za te pravice: za pravico do dostopa, pravico do popravka in izbrisa, pravico do ugovora obdelavi, pravico, da se za posameznika ne uporablja avtomatizirano sprejemanje odločitev, pravico poseči v avtomatizirano sprejemanje odločitev in pravico do obveščanja o sprejemanju odločitev. Poleg tega mora upravljavec posameznika, na katerega se nanašajo osebni podatki, obvestiti o obdelavi njegovih osebnih podatkov. Kot je pojasnjeno v smernicah urada informacijskega pooblaščenca o obdelavi s strani obveščevalnih služb, lahko posamezniki uveljavljajo vse svoje pravice (vključno z zahtevkom za popravek) tako, da vložijo pritožbo pri uradu informacijskega pooblaščenca ali vložijo tožbo pri sodišču (glej smernice urada informacijskega pooblaščenca o obdelavi s strani obveščevalnih služb, ki so na voljo na naslednji povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

varstvo podatkov ([159]) in ureja mednarodni prenos osebnih podatkov ([160]). Urad informacijskega pooblaščenca je nedavno izdal podrobne smernice o obdelavi s strani obveščevalnih agencij v skladu z delom 4 zakona o varstvu podatkov iz leta 2018 ([161]).

(126) Hkrati člen 110 zakona o varstvu podatkov iz leta 2018 določa izjemo od posebnih določb v delu 4 navedenega zakona ([162]), kadar je taka izjema potrebna za zaščito nacionalne varnosti. To izjemo je mogoče uporabiti le na podlagi analize vsakega primera posebej ([163]). Kot so pojasnili organi Združenega kraljestva in je bilo potrjeno s sodno prakso sodišč Združenega kraljestva, „mora upravljavec upoštevati dejanske posledice za nacionalno varnost ali obrambo, če bi moral zagotoviti skladnost s posamezno določbo za varstvo podatkov, ter ali bi razumno lahko zagotovil skladnost z običajnim pravilom brez ogrožanja nacionalne varnosti ali obrambe“ ([164]). O tem, ali je bila izjema ustrezno uporabljena, odloča urad informacijskega pooblaščenca ([165]).

(127) Nadalje, v zvezi z možnostjo omejitve uporabe navedenih posebnih določb iz člena 111 zakona o varstvu podatkov iz leta 2018 zaradi zaščite nacionalne varnosti, lahko upravljavec zaprosi za izdajo potrdila, ki ga podpiše višji minister ali generalni državni tožilec in pravni svetovalec vlade (Attorney General) in ki potrjuje, da je omejitev take pravice potreben in sorazmeren ukrep za zaščito nacionalne varnosti ([166]).

(128) Vlada Združenega kraljestva je izdala smernice v pomoč upravljavcem, kadar se ti odločajo, ali naj na podlagi zakona o varstvu podatkov iz leta 2018 zaprosijo za izdajo potrdila glede nacionalne varnosti; navedene smernice predvsem poudarjajo, da morajo biti vse omejitve pravic posameznikov, na katere se nanašajo osebni podatki, z namenom zaščite nacionalne varnosti sorazmerne in potrebne ([167]). Vsa potrdila glede nacionalne varnosti morajo biti objavljena na spletišču urada informacijskega pooblaščenca ([168]).

([159]) Člen 103 zakona o varstvu podatkov iz leta 2018.

([160]) Člen 109 zakona o varstvu podatkov iz leta 2018. Prenosi osebnih podatkov mednarodnim organizacijam ali državam zunaj Združenega kraljestva so mogoči, če je tak prenos potreben in sorazmeren ukrep, ki se izvaja za namene izvajanja zakonskih nalog upravljavca ali za druge namene, določene v zadevnih členih zakona o varnostnih službah iz leta 1989 (Security Service Act 1989) in zakona o obveščevalnih službah iz leta 1994 (Intelligence Services Act 1994).

([161]) Smernice urada informacijskega pooblaščenca, glej opombo 158.
Člen 30 zakona o varstvu podatkov iz leta 2018 in dodatek 7 k navedenemu zakonu.

([162]) Člen 110(2) zakona o varstvu podatkov iz leta 2018 navaja seznam določb, pri katerih je mogoče uporabiti izjemo. Med njimi so načela o varstvu podatkov (razen načela zakonitosti), pravice posameznika, na katerega se nanašajo osebni podatki, obveznost obveščanja informacijskega pooblaščenca o kršitvi varstva podatkov, inšpekcijska pooblastila informacijskega pooblaščenca v skladu z mednarodnimi obveznostmi, nekatera pooblastila informacijskega pooblaščenca za izvrševanje, določbe, na podlagi katerih se nekatere kršitve varstva podatkov štejejo za kaznivo dejanje, in določbe, ki se nanašajo na posebne namene obdelave, na primer za novinarske, akademske ali umetniške namene.

([163]) Glej zadevo Baker proti Secretary of State, opomba 61.

([164]) UK Explanatory Framework for Adequacy Discussion, Section H: Glej National Security Data Protection and Investigatory Powers Framework, strani 15–16 (glej opombo 31). Glej tudi zadevo Baker proti Secretary of State (opomba 61), v kateri je sodišče razveljavilo potrdilo glede nacionalne varnosti, ki ga je izdal minister za notranje zadeve in ki je omogočalo uporabo izjeme na podlagi nacionalne varnosti, saj je menilo, da ni razloga za dovolitev splošne izjeme od obveznosti odzvati se na zahteve za dostop do podatkov ter da bi omogočanje take izjeme v vseh okoliščinah, brez analize v vsakem posameznem primeru, presegalo kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

([165]) Glej memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, v skladu s katerim „se mora urad informacijskega pooblaščenca po prejetju pritožbe posameznika, na katerega se nanašajo osebni podatki, prepričati, ali je bila zadeva pravilno obravnavana ter po potrebi ali so bile morebitne izjeme ustrezno uporabljene“. Memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, točka 16, na voljo na povezavi: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) Zakon o varstvu podatkov iz leta 2018 je razveljavil možnost izdaje potrdil v skladu s členom 28(2) zakona o varstvu podatkov iz leta 1998. Vendar možnost izdaje „starih potrdil“ še vedno obstaja, če obstaja zgodovinski ugovor v skladu z zakonom iz leta 1998 (glej odstavek 17 dela 5 dodatka 20 k zakonu o varstvu podatkov iz leta 2018). Vendar se zdi ta možnost zelo redka in se bo uporabljala le v omejenih primerih, na primer če bo posameznik, na katerega se nanašajo osebni podatki, izpodbijal uporabo izjeme zaradi nacionalne varnosti v zvezi z obdelavo s strani javnega organa, ki je izvedel obdelavo v skladu z zakonom iz leta 1998. Opozoriti je treba, da se bo v teh primerih v celoti uporabljal člen 28 zakona o varstvu podatkov iz leta 1998, vključno z možnostjo, da posameznik, na katerega se nanašajo osebni podatki, izpodbija potrdilo pred sodiščem.

([167]) Smernice vlade Združenega kraljestva v zvezi s potrdili glede nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018 so na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Iz pojasnil organov Združenega kraljestva izhaja, da čeprav ima potrdilo dokazno moč, da se glede podatkov ali obdelave, opisane v potrdilu, lahko uporabi izjema, pa potrdilo upravljavca ne odvezuje obveznosti v vsakem posameznem primeru proučiti, ali je izjema potrebna.

([168]) V skladu s členom 130 zakona o varstvu podatkov iz leta 2018 se lahko urad informacijskega pooblaščenca odloči, da ne objavi besedila ali dela besedila potrdila, če bi bilo to v nasprotju z interesom nacionalne varnosti ali javnim interesom ali bi lahko ogrozilo varnost katere koli osebe. V teh primerih urad informacijskega pooblaščenca še vedno objavi, da je bilo potrdilo izdano.

(129) Potrdilo se izda za določen čas največ pet let, da ga lahko izvršilna oblast redno preverja ([169]). Potrdilo opredeljuje osebne podatke ali vrste osebnih podatkov, za katere se lahko uporabi izjema, ter določbe zakona o varstvu podatkov iz leta 2018, glede katerih se lahko uporabi izjema ([170]).

(130) Treba je opozoriti, da potrdila glede nacionalne varnosti ne zagotavljajo dodatnega razloga za omejevanje pravic do varstva podatkov iz razlogov nacionalne varnosti. Povedano drugače se lahko upravljavec ali obdelovalec na potrdilo zanese le, če ugotovi, da je treba v posameznem primeru (kot je pojasnjeno zgoraj) uporabiti izjemo zaradi nacionalne varnosti ([171]). Tudi če se potrdilo glede nacionalne varnosti nanaša na posamezno zadevo, lahko urad informacijskega pooblaščenca prouči, ali je bilo v posameznem primeru sklicevanje na izjemo zaradi nacionalne varnosti upravičeno ([172]).

(131) Neposredno prizadeti zaradi izdaje potrdila ([173]), se lahko pritožijo pri sodišču Upper Tribunal ([174]), če so v potrdilu podatki opredeljeni s splošnim opisom, pa lahko izpodbija uporabo potrdila glede posameznih podatkov ([175]). Sodišče prouči odločitev o izdaji potrdila in odloči, ali so za izdajo potrdila obstajali utemeljeni razlogi ([176]). Prouči lahko več vprašanj, vključno s potrebnostjo, sorazmernostjo in zakonitostjo, pri čemer upošteva vpliv na pravice posameznikov, na katere se nanašajo podatki, in pretehta potrebo po zaščiti nacionalne varnosti. Posledično lahko sodišče ugotovi, da se potrdilo ne nanaša na specifične osebne podatke, ki so predmet pritožbe ([177]).

(132) Druga vrsta morebitnih omejitev se nanaša na tiste, ki se na podlagi dodatka 11 k zakonu o varstvu podatkov iz leta 2018 nanašajo na nekatere določbe dela 4 zakona o varstvu podatkov iz leta 2018 ([178]) za zaščito drugih pomembnih ciljev splošnega javnega interesa ali zaščitenih interesov, kot so na primer parlamentarni privilegij, varovanje zaupnosti sporazumevanja med odvetnikom in stranko, vodenje sodnega postopka ali bojna učinkovitost oboroženih sil ([179]). Uporaba teh določb je izključena glede nekaterih vrst informacij (izjema na podlagi vrste) ali v kolikor bi uporaba teh določb verjetno posegala v zaščitene interese (izjema na podlagi poseganja) ([180]). Na izjeme

([169]) Smernice vlade Združenega kraljestva v zvezi s potrdili glede nacionalne varnosti, točka 15, opomba 167.

([170]) Smernice vlade Združenega kraljestva v zvezi s potrdili glede nacionalne varnosti, točka 5, glej opombo 167.

([171]) Glej opombo 164.

([172]) Člen 102 zakona o varstvu podatkov iz leta 2018 določa, da mora upravljavec dokazati, da je zagotovil skladnost z zakonom o varstvu podatkov iz leta 2018. To pomeni, da mora obveščevalna služba uradu informacijskega pooblaščenca dokazati, da je pri uporabi izjeme proučila posebne okoliščine posamezne zadeve. Urad informacijskega pooblaščenca objavlja tudi evidenco potrdil glede nacionalne varnosti, ki je na voljo na naslednji povezavi: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/

([173]) Člen 111(3) zakona o varstvu podatkov iz leta 2018.

([174]) Sodišče Upper Tribunal je pristojno za obravnavo pritožb zoper odločitve nižjih upravnih sodišč in ima posebne pristojnosti glede neposrednih pritožb zoper odločitve nekaterih vladnih organov.

([175]) Člen 111(5) zakona o varstvu podatkov iz leta 2018.

([176]) V zadevi Baker proti Secretary of State (opomba 61) je sodišče Information Tribunal razveljavilo potrdilo glede nacionalne varnosti, ki ga je izdal minister za notranje zadeve, saj je menilo, da ni razloga, da bi se dovolila splošna izjema od obveznosti odzvati se na zahteve za dostop do podatkov ter da bi omogočanje take izjeme v vseh okoliščinah, brez analize v vsakem primeru posebej, presegalo tisto, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

([177]) Smernice vlade Združenega kraljestva v zvezi s potrdili glede nacionalne varnosti, točka 25, opomba 167.

([178]) To vključuje: (i) načela o varstvu podatkov iz dela 4, razen zahteve glede zakonitosti obdelave na podlagi prvega načela ter dejstva, da mora obdelava izpolnjevati enega od zadevnih pogojev iz dodatkov 9 in 10; (ii) pravice posameznikov, na katere se nanašajo osebni podatki, in (iii) obveznosti, ki se nanašajo na kršitev poročanja uradu informacijskega pooblaščenca.

([179]) Del 4 zakona o varstvu podatkov iz leta 2018 določa pravni okvir, ki se uporablja za vse vrste obdelave osebnih podatkov, ki jo izvajajo obveščevalne agencije (in ne le za izvajanje njihovih nalog na področju nacionalne varnosti). Zato se del 4 uporablja tudi za primere, kadar obveščevalne agencije obdelujejo podatke v okviru sodnih postopkov ali v okviru javnega naročanja, na primer za namene upravljanja človeških virov. Omejitve, navedene v dodatku 11, naj bi se uporabljale predvsem v teh drugih okoliščinah. Na primer, v okviru sodnega postopka z zaposlenim se je mogoče sklicevati na omejitev za namene „sodnega postopka“, v okviru javnega naročanja se je mogoče sklicevati na omejitev za namene „pogajanja“ itd. To se odraža v smernicah urada informacijskega pooblaščenca o obdelavi s strani obveščevalnih služb, v katerih je kot primer za uporabo omejitev iz dodatka 11 navedeno pogajanje o poravnavi med obveščevalno službo in nekdanjim zaposlenim, ki uveljavlja terjatev iz delovnega razmerja (glej opombo 161). Opozoriti je treba tudi, da so v skladu z dodatkom 2 k delu 2 zakona o varstvu podatkov iz leta 2018 enake omejitve na voljo tudi drugim javnim organom.

([180]) V skladu z obrazložitvenim okvirom Združenega kraljestva so izjeme na podlagi vrste: (i) informacije o podelitvi državnih častnih odlikovanj; (ii) varovanje zaupnosti sporazumevanja med odvetnikom in stranko; (iii) zaupni sklici na zaposlitev, usposabljanje ali izobraževanje ter (iv) izpitne pole in ocene. Izjeme na podlagi poseganja se nanašajo na naslednje zadeve: (i) preprečevanje ali odkrivanje kaznivih dejanj; prijetje in pregon storilcev; (ii) parlamentarni privilegij; (iii) sodni postopki; (iv) bojna učinkovitost oboroženih sil države; (v) gospodarska blaginja Združenega kraljestva; (vi) pogajanja s posameznikom, na katerega se nanašajo osebni podatki; (vii) znanstvene ali zgodovinske raziskave ali statistični nameni; (viii) arhiviranje v javnem interesu. UK Explanatory Framework for Adequacy Discussions, section H: National Security, stran 13, opomba 31.

na podlagi poseganja se je mogoče sklicevati le, če je verjetno, da bi uporaba navedene določbe o varstvu podatkov posegala v zadevni interes. Uporaba izjeme mora biti torej vedno upravičena s sklicevanjem na zadevno poseganje, do katerega bi v posameznem primeru verjetno prišlo. Na izjeme na podlagi vrste se je mogoče sklicevati le glede specifičnih, ozko opredeljenih vrst informacij, glede katerih je uporaba izjeme mogoča. Te so glede na namen in učinek podobne več izjemam od UK GDPR (na podlagi dodatka 2 k zakonu o varstvu podatkov iz leta 2018), ki pa izražajo tiste iz člena 23 Splošne uredbe o varstvu podatkov.

(133) Iz navedenega izhaja, da so na podlagi pravnih določb Združenega kraljestva, ki se uporabljajo, vzpostavljene omejitve in pogoji, kakor jih razlagajo tudi sodišča in informacijski pooblaščenec, ki zagotavljajo, da navedene izjeme in omejitve ostajajo znotraj okvirov tega, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

3.2 **Dostop in uporaba s strani javnih organov Združenega kraljestva za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj**

(134) Pravo Združenega kraljestva določa več omejitev glede dostopa do in uporabe osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter na tem področju zagotavlja nadzorne mehanizme in mehanizme pravnih sredstev, ki so v skladu z zahtevami iz uvodnih izjav (113) do (115) tega sklepa. Pogoji, na podlagi katerih je tak dostop mogoč, in zaščitni ukrepi glede uporabe teh pooblastil so podrobneje ocenjeni v oddelkih v nadaljevanju.

3.2.1 *Pravna podlaga in omejitve/zaščitni ukrepi, ki se uporabljajo*

(135) V skladu z načelom zakonitosti iz člena 35 zakona o varstvu podatkov iz leta 2018 je obdelava osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zakonita le, če temelji na pravu in je posameznik, na katerega se nanašajo osebni podatki, privolil v njihovo obdelavo za navedeni namen ([181]), ali pa je obdelava potrebna za opravljanje naloge, ki jo v ta namen izvaja pristojni organ.

3.2.1.1 Odredbe o preiskavi in o predložitvi dokazov

(136) V pravnem okviru Združenega kraljestva je zbiranje osebnih podatkov od poslovnih subjektov, tudi tistih, ki bodo obdelovali podatke, prenesene iz EU na podlagi tega sklepa o ustreznosti, za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, dovoljeno na podlagi odredbe o preiskavi ([182]) in odredbe o predložitvi dokazov ([183]).

(137) Odredbe o preiskavi izdajajo sodišča, običajno na predlog preiskovalcev. Preiskovalcem omogočajo vstop v prostore z namenom iskanja gradiva ali posameznikov, ki so pomembni za zadevno preiskavo, ter zadržanje vsega, za kar je bila preiskava odobrena, vključno z vsemi zadevnimi dokumenti ali gradivom, ki vsebuje osebne podatke ([184]). Na podlagi odredbe o predložitvi dokazov, ki jo mora prav tako izdati sodišče, mora oseba, ki je v njej navedena, predložiti gradivo, ki ga ima v posesti ali pod svojim nadzorom, oziroma omogočiti dostop do njega. Predlagatelj mora sodišču utemeljiti, zakaj je odredba potrebna in zakaj je v javnem interesu. V veljavi je več zakonskih

([181]) Videti je, da uporaba privolitve v zvezi z ustreznostjo ni pomembna, saj v primeru prenosa podatkov organ Združenega kraljestva za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj podatkov ne bo dobil neposredno od posameznika v EU, na katerega se nanašajo osebni podatki, na podlagi privolitve.

([182]) Glede ustrezne pravne podlage glej člen 8 in naslednje zakona o policiji in kazenskih evidencah iz leta 1984, ki se uporablja v Angliji in Walesu (PACE 1984 (for England and Wales)), člen 10 in naslednje uredbe o policiji in kazenskih evidencah iz leta 1989, ki se uporablja na Severnem Irskem (Police and Criminal Evidence Order (Northern Ireland) 1989), za Škotsko pa temelji na občem pravu (glej člen 46 zakona o kazenskem pravosodju iz leta 2016, ki se uporablja na Škotskem (Criminal Justice (Scotland) Act 2016) in člen 23B prečiščenega besedila zakona o kazenskem pravu, ki se uporablja na Škotskem (Criminal Law (Consolidation) (Scotland)). Glede odredb o preiskavi, ki se izdajo po odvzemu prostosti, je pravna podlaga člen 18 zakona o policiji in kazenskih evidencah iz leta 1984, ki se uporablja v Angliji in Walesu, člen 20 in naslednji uredbe o policiji in kazenskih evidencah iz leta 1989, ki se uporablja na Severnem Irskem, za Škotsko pa obče pravo (glej člen 46 zakona o kazenskem pravosodju iz leta 2016, ki se uporablja na Škotskem. Organi Združenega kraljestva so pojasnili, da odredbe o preiskavi izdajajo sodišča na predlog preiskovalcev. Te odredbe preiskovalcem omogočajo vstop v prostore z namenom iskanja gradiva ali posameznikov, ki so pomembni za preiskavo; izvršitev odredbe pogosto zahteva sodelovanje policistov.

([183]) Kadar se preiskava nanaša na pranje denarja (vključno z zaplembo in civilnim odškodninskim postopkom), so ustrezna pravna podlaga za vložitev predloga za izdajo odredbe o predložitvi dokazov v Angliji, Walesu in na Severnem Irskem členi 345 in naslednji, na Škotskem pa člen 380 in naslednji zakona o premoženjski koristi, pridobljeni s kaznivim dejanjem, iz leta 2002 (Proceeds of Crime Act 2002). Če se preiskava nanaša na druga vprašanja, ne na pranje denarja, je mogoče predlog za izdajo odredbe o predložitvi dokazov vložiti na podlagi člena 9 in dodatka 1 k zakonu o policiji in kazenskih evidencah iz leta 1984, ki se uporablja v Angliji in Walesu, ter na podlagi člena 10 in naslednjih uredbe o policiji in kazenskih evidencah iz leta 1989, ki se uporablja na Severnem Irskem. Na Škotskem je pravna podlaga obče pravo (glej člen 46 zakona o kazenskem pravosodju iz leta 2016, ki se uporablja na Škotskem, in člen 23B prečiščenega besedila zakona o kazenskem pravu, ki se uporablja na Škotskem). Organi Združenega kraljestva so pojasnili, da mora na podlagi odredbe o predložitvi dokazov oseba, na katero se odredba nanaša, predložiti gradivo, ki ga ima v posesti ali pod svojim nadzorom, oziroma omogočiti dostop do njega (glej točko 4 dodatka 1 k zakonu o policiji in kazenskih evidencah iz leta 1984).

([184]) Zakon o policiji in kazenskih evidencah iz leta 1984 v členih 8 in 18 vsebuje pooblastila za zaseg in zadržanje vsega, za kar je bila odobrena preiskava.

pooblastil, ki omogočajo izdajo odredb o preiskavi in o predložitvi dokazov. Vsaka določba vsebuje posebne zakonske pogoje, ki morajo biti izpolnjeni za izdajo odredbe o preiskavi ([185]) ali odredbe o predložitvi dokazov ([186]).

(138) Odredbe o predložitvi dokazov in odredbe o preiskavi se lahko izpodbijajo v okviru sodne presoje ([187]). Glede zaščitnih ukrepov velja, da imajo vsi organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki spadajo na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018, dostop do osebnih podatkov (kar je oblika obdelave) le v skladu z načeli in zahtevami iz navedenega zakona (glej uvodni

([185]) Člena 8 in 18 zakona o policiji in kazenskih evidencah na primer podeljujeta pooblastilo mirovnemu sodniku za izdajo odredbe o preiskavi oziroma pooblastilo policistu za preiskavo lokacije. V prvem primeru (člen 8) mora mirovni sodnik pred izdajo odredbe ugotoviti, ali obstajajo utemeljeni razlogi za sum, da: (i) je bilo storjeno hujše kaznivo dejanje; (ii) je na lokaciji gradivo, za katerega je verjetno, da bo pomembno pri preiskavi kaznivega dejanja (samostojno ali skupaj z drugim materialom); (iii) je verjetno, da ima gradivo pomembno dokazno vrednost; (iv) gradivo ne vključuje predmetov, ki so zaupni kot del sporazumevanja med odvetnikom in stranko, izločenega gradiva ali gradiva iz posebnega postopka, ter (v) da si dostopa ne bi bilo mogoče zagotoviti brez odredbe. V drugem primeru člen 18 policistom omogoča preiskavo prostorov osebe, ki ji je bila odvzeta prostost zaradi suma storitve hujšega kaznivega dejanja, z namenom iskanja gradiva, ki se ne šteje za zaupno kot del sporazumevanja med odvetnikom in stranko, če policisti utemeljeno sumijo, da so v prostorih dokazi, ki se nanašajo na navedeno kaznivo dejanje ali na drugo podobno oziroma povezano hujše kaznivo dejanje. Taka preiskava mora biti omejena na iskanje navedenega gradiva ter jo mora pisno odobriti policist, ki ima vsaj čin inšpektorja, razen če je potrebna za preiskavo kaznivega dejanja. V takem primeru mora biti policist, ki ima vsaj čin inšpektorja, o tem obveščen takoj po izvedbi preiskave, ko je to praktično izvedljivo. Evidentirati je treba podlago za preiskavo in vrsto iskanih dokazov. Nadalje, člena 15 in 16 zakona o policiji in kazenskih evidencah iz leta 1984 določata zakonske zaščitne ukrepe, ki jih je treba upoštevati pri vložitvi predloga za izdajo odredbe o preiskavi. Člen 15 določa zahteve, ki se nanašajo na izdajo odredbe o preiskavi (vključno z vsebino predloga, ki ga vloži policist, in dejstvo, da mora biti v odredbi med drugim navedena pravna podlaga, na podlagi katere se izdaja, prav tako pa morajo biti kolikor je mogoče natančno opredeljeni predmeti in osebe, ki se iščejo, ter prostori, ki se preiskujejo). Člen 16 določa, kako se izvede preiskava na podlagi odredbe (na primer: člen 16(5) določa, da mora policist, ki izvršuje odredbo, osebi, katere prostori se preiskujejo, izročiti kopijo odredbe; člen 16(11) zahteva, da se odredba, ko je izvršena, hrani še 12 mesecev; člen 16(12) osebi, katere prostori se preiskujejo, podeljuje pravico do vpogleda v odredbo v navedenem obdobju, če ta to želi). Ti členi prispevajo k zagotavljanju skladnosti s členom 8 EKČP (glej na primer zadevo Kent Pharmaceuticals v Director of the Serious Fraud Office [2002] EWHC 3023 (QB) at [30] by Lord Woolf CJ). Če ti zaščitni ukrepi niso izpolnjeni, se lahko preiskava razglasi za nezakonito (primeri tega so zadeva R (Brook) v Preston Crown Court [2018] EWHC 2024 (Admin), [2018] ACD 95; R (Superior Import / Export Ltd) v Revenue and Customs Commissioners [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; in R (F) v Blackfriars Crown Court [2014] EWHC 1541 (Admin)). Kodeks B zakona o policiji in kazenskih evidencah iz leta 1984 dopolnjuje člena 15 in 16 navedenega zakona; gre za kodeks ravnanja, ki ureja izvrševanje pristojnosti policije pri hišnih preiskavah.

([186]) Pri izdaji odredbe o predložitvi dokazov na podlagi zakona o premoženjski koristi, pridobljeni s kaznivim dejanjem, iz leta 2002 morajo na primer poleg utemeljenih razlogov za izpolnitev pogojev iz člena 346(2) zakona o premoženjski koristi, pridobljeni s kaznivim dejanjem, obstajati tudi utemeljeni razlogi, da ima oseba v posesti ali pod nadzorom zadevno gradivo in da je verjetno, da je to gradivo pomembno. Nadalje, druga zahteva glede izdaje odredbe o predložitvi dokazov je, da morajo obstajati utemeljeni razlogi za sum, da je predložitev gradiva oziroma omogočanje dostopa do njega v javnem interesu, pri čemer se upoštevajo (a) korist za preiskavo, če bo gradivo pridobljeno, in (b) okoliščine, v okviru katerih ima oseba, za katero je v predlogu navedeno, da verjetno ima v posesti ali pod nadzorom navedeno gradivo, navedene informacije. Podobno mora sodišče, ki obravnava predlog za izdajo odredbe o predložitvi dokazov na podlagi dodatka 1 k zakonu o policiji in kazenskih evidencah iz leta 1984, ugotoviti, ali so izpolnjeni posebni pogoji. Dodatek 1 navedenega zakona določa dva ločena in alternativna sklopa pogojev, od katerih mora biti eden izpolnjen, da lahko sodnik izda odredbo o predložitvi dokazov. Prvi sklop zahteva, da ima sodnik utemeljene razloge za sum, (i) da je bilo storjeno hujše kaznivo dejanje; (ii) da gradivo, ki se išče, vključuje gradivo iz posebnega postopka, vendar ne izključeno gradivo; (iii) da je verjetno, da je gradivo pomembno za preiskavo, samo ali skupaj z drugim gradivom; (iv) ter da je verjetno, da gre za pomembne dokaze; (v) da so bile uporabljene tudi druge metode za pridobivanje gradiva ali da niso bile, ker je očitno, da ne bi bile uspešne; ter (vi) da je glede na korist za preiskavo in glede na okoliščine, v katerih ima posameznik navedeno gradivo v posesti, v javnem interesu, da se gradivo predloži ali da se zagotovi dostop do njega. Drugi sklop pogojev pa vključuje zahteve: (i) da je na lokaciji gradivo, ki vključuje gradivo iz posebnega postopka ali izločeno gradivo; (ii) da če ne bi veljala prepoved izvajanja preiskav na podlagi zakonodaje, sprejete pred sprejetjem zakona o policiji in kazenskih evidencah, glede gradiva iz posebnih postopkov, izločenega gradiva ali gradiva, za katerega velja zaupnost sporazumevanja med odvetnikom in stranko, bi se odredba o preiskavi glede navedenega gradiva lahko izdala, ter (iii) če je to ustrezno.

([187]) Sodna presoja je sodni postopek, v katerem je mogoče izpodbijati odločitev javnega organa pred sodiščem High Court. Sodišča preverijo izpodbijano odločitev in odločijo, ali je ob upoštevanju konceptov/načel javnega prava navedeno odločitev mogoče šteti za pravno napačno. Temeljni pritožbeni razlogi za sodno presojo so torej nezakonitost, nerazumnost, procesne napake, zakonita pričakovanja in človekove pravice. Po uspešni sodni presoji ima sodišče več možnosti: najpogostejša je odločba o razveljavitvi (s katero se razveljavi prvotna odločitev – tj. odločitev o izdaji odredbe o preiskavi), v nekaterih primerih pa lahko sodišče prisodi tudi finančno odškodnino. Več informacij o sodni presoji v Združenem kraljestvu je na voljo v publikaciji vladne pravne službe z naslovom: Judge Over Your Shoulder – a guide to good decision-making (Sodnik vam je v pomoč: vodnik za dobro odločanje), ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

izjavi (122) in (124) above). Predlog katerega koli organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj mora biti torej v skladu z načelom, da mora biti namen obdelave opredeljen, izrecen in legitimen ([188]), ter da morajo biti osebni podatki, ki jih obdeluje pristojni organ, relevantni glede na namen in ne čezmerni ([189]).

3.2.1.2 Preiskovalna pooblastila za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

(139) Za namene preprečevanja ali odkrivanja hudih kaznivih dejanj ([190]) lahko nekateri organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, na primer National Crime Agency ali načelnik policije ([191]), uporabijo ciljna preiskovalna pooblastila v okviru zakona o preiskovalnih pooblastilih iz leta 2016. V tem primeru se bodo poleg zaščitnih ukrepov iz dela 3 zakona o varstvu podatkov iz leta 2018 uporabljali tudi zaščitni ukrepi iz zakona o preiskovalnih pooblastilih iz leta 2016. Preiskovalna pooblastila, ki se jih lahko poslužujejo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, so: ciljno prestrezanje (del 2 zakona o preiskovalnih pooblastilih iz leta 2016), pridobivanje komunikacijskih podatkov (del 3 zakona o preiskovalnih pooblastilih iz leta 2016), hramba komunikacijskih podatkov (del 4 zakona o preiskovalnih pooblastilih iz leta 2016) in ciljno poseganje v opremo (del 5 zakona o preiskovalnih pooblastilih iz leta 2016). Prestrezanje vključuje pridobivanje vsebine komunikacije ([192]), pri čemer pridobivanje in hramba komunikacijskih podatkov nista namenjena pridobivanju vsebine komunikacije, ampak podatkov o tem, kdo, kdaj, kje in kako je komuniciral. To na primer vključuje čas in trajanje komunikacije, telefonsko številko ali elektronski naslov pošiljatelja in prejemnika ter včasih lokacijo naprav, ki so bile uporabljene za komunikacijo, in naročnika telefonskih storitev ali specifikacijo računa ([193]). Poseganje v opremo vključuje več tehnik, ki se uporabljajo za pridobivanje raznih podatkov z opreme, kar vključuje računalnike, tablice in pametne telefone ter kable, žice in naprave za shranjevanje podatkov ([194]).

(140) Pooblastila za ciljno prestrezanje se lahko uporabijo tudi, kadar je to „potrebno zaradi izvrševanja določb instrumenta EU o medsebojni pomoči ali mednarodnega sporazuma o medsebojni pomoči“ (tako imenovana odredba na podlagi medsebojne pomoči ([195])). Odredbe na podlagi medsebojne pomoči se izdajajo le v zvezi s prestrezanjem, ne pa tudi v zvezi s pridobivanjem komunikacijskih podatkov ali poseganjem v opremo. Ta ciljna pooblastila so urejena v zakonu o preiskovalnih pooblastilih iz leta 2016 ([196]), ki skupaj z zakonom o urejanju preiskovalnih pooblastil iz leta 2000, ki se uporablja v Angliji, Walesu in na Severnem Irskem (Regulation of Investigatory Powers Act 2000 (RIPA) for England, Wales and Northern Ireland), ter zakonom o urejanju preiskovalnih pooblastil iz leta 2000, ki se uporablja na Škotskem (Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) for Scotland), pomeni pravno podlago ter določa omejitve in zaščitne ukrepe glede uporabe takih pooblastil. Zakon o preiskovalnih pooblastilih iz leta 2016 ureja tudi uporabo preiskovalnih pooblastil v večjem obsegu, čeprav ta niso na voljo organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (uporabijo jih lahko le obveščevalne agencije) ([197]).

([188]) Člen 36(1) zakona Združenega kraljestva o varstvu podatkov iz leta 2018.

([189]) Člen 37 zakona Združenega kraljestva o varstvu podatkov iz leta 2018.

([190]) Člen 263(1) zakona o preiskovalnih pooblastilih iz leta 2016 določa, da je „hudo kaznivo dejanje“ tisto, pri katerem je mogoče razumno pričakovati, da bo odrasla oseba brez predhodnih obsodb zanj obsojena na zaporno kazen tri leta ali več, ali kaznivo dejanje, ki vključuje uporabo nasilja, ima za posledico znatno finančno izgubo ali ki ga stori več oseb. Poleg tega za namene pridobivanja komunikacijskih podatkov na podlagi dela 4 zakona o preiskovalnih pooblastilih iz leta 2016 člen 87(10B) določa, da „hudo kaznivo dejanje“ pomeni kaznivo dejanje, za katero je mogoče izreči zaporno kazen 12 mesecev ali več, ali kaznivo dejanje, ki ga zagreši subjekt, ki se ne šteje za posameznika, ali ki kot bistveno sestavino vključuje pošiljanje komunikacije ali kršitev zasebnosti posameznika.

([191]) Izdajo odredbe o ciljnem prestrezanju lahko zahtevajo naslednji organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj: generalni direktor nacionalne agencije za boj proti kriminalu (Director General of the National Crime Agency), komisar metropolitanske policije (Commissioner of Police of the Metropolis), vodja policije Severne Irske (Chief Constable of the Police Service of Northern Ireland), vodja policije Škotske (Chief Constable of the Police Service of Scotland), vodja oddelka davčne in carinske uprave (Commissioner for Her Majesty's Revenue and Customs), vodja obrambne obveščevalne službe (Chief of Defence Intelligence) ter oseba, ki je pristojni organ države ali ozemlja zunaj Združenega kraljestva za namene instrumenta EU o medsebojni pomoči ali mednarodnega sporazuma o medsebojni pomoči (člen 18(1) zakona o preiskovalnih pooblastilih iz leta 2016).

([192]) Glej člen 4 zakona o preiskovalnih pooblastilih iz leta 2016.

([193]) Glej člen 261(5) zakona o preiskovalnih pooblastilih iz leta 2016 in kodeks ravnanja glede pridobivanja večjih količin komunikacijskih podatkov (Code of Practice on Bulk Acquisition of Communications Data), ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, točka 2.9.

([194]) Kodeks ravnanja glede poseganja v opremo (Code of Practice on Equipment Interference) je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, točka 2.2.

([195]) Odredba na podlagi medsebojne pomoči organu Združenega kraljestva omogoča, da zagotavlja pomoč organu zunaj ozemlja Združenega kraljestva pri prestrezanju in razkritje prestreženega gradiva takemu organu v skladu z mednarodnim instrumentom o medsebojni pomoči (člen 15(4) zakona o preiskovalnih pooblastilih iz leta 2016).

([196]) Zakon o preiskovalnih pooblastilih iz leta 2016 (glej: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) je nadomestil drugačno zakonodajo o prestrezanju komunikacij, poseganju v opremo in pridobivanju komunikacijskih podatkov, zlasti del I zakona o urejanju preiskovalnih pooblastil iz leta 2000, ki je pomenil predhodni splošni zakonodajni okvir za uporabo preiskovalnih pooblastil s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in organov za nacionalno varnost.

([197]) Členi 138(1), 158(1), 178(1) in 199(1) zakona o preiskovalnih pooblastilih iz leta 2016.

(141) Za izvrševanje teh pooblastil morajo organi pridobiti odredbo ([198]), ki jo izda pristojni organ ([199]) in odobri neodvisni pravosodni pooblaščenec (Judicial Commissioner) ([200]) (tako imenovani postopek z dvojnim varovalom). Za pridobitev take odredbe je treba opraviti preskus potrebnosti in sorazmernosti ([201]). Ker so ta ciljna preiskovalna pooblastila, določena v zakonu o preiskovalnih pooblastilih iz leta 2016, enaka tistim, ki so na voljo agencijam za nacionalno varnost, so pogoji, omejitve in zaščitni ukrepi, ki se uporabljajo pri takih pooblastilih, podrobneje obravnavani v oddelku o dostopu do osebnih podatkov in njihovi uporabi s strani javnih organov Združenega kraljestva za namene nacionalne varnosti (glej uvodno izjavo (177) in naslednje).

3.2.2 *Nadaljnja uporaba zbranih informacij*

(142) Glede izmenjave podatkov med organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in drugim organom za namene, ki se razlikujejo od tistih, za katere so bili podatki prvotno zbrani (tako imenovana nadaljnja izmenjava), veljajo določeni pogoji.

(143) Podobno kot je določeno v členu 4(2) Direktive (EU) 2016/680 tudi člen 36(3) zakona o varstvu podatkov iz leta 2018 omogoča nadaljnjo obdelavo osebnih podatkov (s strani prvotnega ali drugega upravljavca), ki jih pristojni organ zbere za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za kateri koli drug namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni drug namen ter če je obdelava potrebna in sorazmerna glede na navedeni namen ([202]). V takem primeru se vsi zaščitni ukrepi iz dela 3 zakona o varstvu podatkov iz leta 2018, navedeni v uvodnih izjavah (122) in (124), uporabljajo za obdelavo, ki jo izvaja organ prejemnik.

(144) V okviru pravnega reda Združenega kraljestva različni zakoni izrecno omogočajo tako nadaljnjo izmenjavo. Zlasti (i) zakon o digitalnem gospodarstvu iz leta 2017 (Digital Economy Act 2017) omogoča izmenjavo med javnimi organi za več namenov, na primer v primeru kakršne koli goljufije zoper javni sektor, ki vključuje izgubo ali tveganje izgube za javne organe ([203]), ali v primeru dolga javnemu organu ali državi ([204]); (ii) zakon o kriminalu in sodiščih iz leta 2013 (Crime and Courts Act 2013), ki omogoča izmenjavo informacij z nacionalno agencijo za boj proti kriminalu (National Crime Agency (NCA)) ([205]) za namene boja proti hudim kaznivim dejanjem in organiziranemu kriminalu ter preiskovanja in pregona hudih kaznivih dejanj in organiziranega kriminala; (iii) zakon o hudih kaznivih dejanjih iz leta 2007 (Serious Crime Act 2007), ki javnim organom omogoča razkritje informacij organizacijam za boj proti goljufijam za namene preprečevanja goljufij ([206]).

(145) Ti zakoni izrecno določajo, da mora biti izmenjava informacij v skladu z načeli iz zakona o varstvu podatkov iz leta 2018. Poleg tega je strokovni organ uslužbencev policije (College of Policing) izdal dokument o odobreni strokovni praksi glede izmenjave informacij ([207]), ki je policiji v pomoč pri

([198]) Poglavje 2 dela 2 zakona o preiskovalnih pooblastilih iz leta 2016 vsebuje omejeno število primerov, ko je mogoče prestrezanje izvajati brez odredbe. To vključuje: prestrezanje s privolitvijo pošiljatelja ali prejemnika, prestrezanje za upravne ali izvršilne namene, prestrezanje v nekaterih ustanovah (zapor, psihiatrične bolnišnice in centri za pridržanje migrantov) ter prestrezanje, ki se izvaja v skladu z zadevnim mednarodnim sporazumom.

([199]) V večini primerov je pristojni minister tisti organ, ki izdaja odredbe na podlagi zakona o preiskovalnih pooblastilih iz leta 2016, škotski ministri pa so pristojni za izdajanje odredb o ciljnem prestrezanju, odredb na podlagi medsebojne pomoči in odredb o ciljnem poseganju v opremo, kadar so osebe ali prostori, na katere se nanaša prestrezanje, in oprema, v katero je treba poseči, na Škotskem (glej člene 22 in 103 zakona o preiskovalnih pooblastilih iz leta 2016). V primeru ciljnega poseganja v opremo lahko vodja organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (opisan v delih 1 in 2 dodatka 6 k zakonu o preiskovalnih pooblastilih iz leta 2016) izda odredbo na podlagi pogojev iz člena 106 navedenega zakona.

([200]) Pravosodni pooblaščenci (Judicial Commissioners) pomagajo pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil (Investigatory Powers Commissioner, IPC), neodvisnemu organu, ki izvaja nadzor nad uporabo preiskovalnih pooblastil s strani obveščevalnih agencij (več informacij je na voljo v uvodni izjavi (162) in naslednjih).

([201]) Glej zlasti člena 19 in 23 zakona o preiskovalnih pooblastilih iz leta 2016.

([202]) Člen 36(3) zakona o varstvu podatkov iz leta 2018.

([203]) Člen 56 zakona o digitalnem gospodarstvu iz leta 2017, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) Člen 48 zakona o digitalnem gospodarstvu iz leta 2017.

([205]) Člen 7 zakona o kriminalu in sodiščih iz leta 2013, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) Člen 68 zakona o hudih kaznivih dejanjih iz leta 2007, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Authorised Professional Practice on Information Sharing, ki je na voljo na povezavi: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

izpolnjevanju njenih obveznosti glede varstva podatkov na podlagi UK GDPR, zakona o varstvu podatkov in zakona o človekovih pravicah iz leta 1998. Skladnost izmenjave informacij s pravnim okvirom varstva podatkov, ki se uporablja, je seveda stvar sodne presoje ([208]).

(146) Nadalje, podobno kot člen 9 Direktive (EU) 2016/680 tudi zakon o varstvu podatkov iz leta 2018 določa, da se lahko osebni podatki, zbrani za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obdelujejo za namene, ki ne spadajo na področje preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če tako obdelavo omogoča zakon ([209]).

(147) Ta vrsta izmenjave vključuje dva primera: (1) ko organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj posreduje podatke organu z drugega področja, razen obveščevalni agenciji (na primer finančnemu ali davčnemu organu, organu za varstvo konkurence, socialnemu uradu za mladoletnike itd.), ter (2) ko organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj podatke posreduje obveščevalni agenciji. V prvem primeru obdelava osebnih podatkov spada na področje uporabe UK GDPR ter dela 2 zakona o varstvu podatkov iz leta 2018. Komisija je v uvodnih izjavah (12)–(111) ocenila zaščitne ukrepe iz UK GDPR in dela 2 zakona o varstvu podatkov iz leta 2018 ter ugotovila, da Združeno kraljestvo zagotavlja ustrezno raven varstva osebnih podatkov, ki se v okviru Uredbe (EU) 2016/679 prenašajo iz Evropske unije v Združeno kraljestvo.

(148) V drugem primeru, tj. glede izmenjave podatkov, ki jih zbere organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter jih posreduje obveščevalni agenciji za namene nacionalne varnosti, je pravna podlaga za tako izmenjavo člen 19 zakona o boju proti terorizmu iz leta 2008 (Counter Terrorism Act 2008) ([210]). Na podlagi navedenega zakona lahko vsaka oseba daje informacije kateri koli obveščevalni službi za namene izvrševanja katere koli naloge take službe, vključno z nacionalno varnostjo.

(149) Glede pogojev, na podlagi katerih je mogoča izmenjava podatkov za namene nacionalne varnosti, zakon o obveščevalnih službah (Intelligence Services Act) ([211]) in zakon o varnostnih službah (Security Services Act) ([212]) omejujeta zmožnost obveščevalnih služb za pridobivanje podatkov na tisto, kar je potrebno za izvrševanje njihovih zakonskih nalog. Agencije za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki želijo posredovati podatke obveščevalnim službam, morajo proučiti več dejavnikov oziroma upoštevati več omejitev, poleg zakonskih nalog agencij, ki so navedene v zakonu o obveščevalnih službah in zakonu o varnostnih službah ([213]). Člen 20 zakona o boju proti terorizmu iz leta 2008 jasno določa, da mora biti vsaka izmenjava podatkov na podlagi člena 19 v skladu z zakonodajo o varstvu podatkov; to pomeni, da se uporabljajo vse omejitve in zahteve iz dela 3 zakona o varstvu podatkov iz leta 2018. Nadalje, ker so pristojni organi javni organi za namene zakona o človekovih pravicah iz leta 1998, morajo zagotoviti skladnost s pravicami iz Konvencije, vključno s členom 8 EKČP. Te omejitve zagotavljajo, da je vsakršna izmenjava podatkov med agencijami za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in obveščevalnimi službami skladna z zakonodajo o varstvu podatkov in z EKČP.

([208]) Glej na primer zadevo M, R v the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), pri kateri je sodišče High Court presojalo izmenjavo podatkov med policijo in organizacijo Business Crime Reduction Partnership (BCRP), ki upravlja programe obveščanja o izključitvi, na podlagi katerih se osebam prepove vstop v poslovne prostore članov organizacije. Sodišče je proučilo izmenjavo podatkov, ki je potekala na podlagi dogovora, sklenjenega z namenom zaščite javnosti in preprečevanja kriminala, ter ugotovilo, da je bila večina vidikov izmenjave podatkov zakonita, razen glede nekaterih občutljivih podatkov, ki sta si jih izmenjala policija in navedena organizacija. Drug primer je zadeva Cooper v NCA [2019] EWCA Civ 16 , pri kateri je sodišče Court of Appeal potrdilo pravilnost izmenjave podatkov med policijo in agencijo za hude primere organiziranega kriminala (Serious Organised Crime Agency (SOCA)), tj. agencijo za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki je trenutno del nacionalne agencije za boj proti kriminalu (NCA).

([209]) Člen 36(4) zakona o varstvu podatkov iz leta 2018.

([210]) Zakon o boju proti terorizmu iz leta 2008 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) Zakon o obveščevalnih službah iz leta 1994 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) Zakon o varnostnih službah iz leta 1989 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) Člen 2(2) zakona o obveščevalnih službah iz leta 1994 določa, da je „vodja obveščevalne službe odgovoren za učinkovitost navedene službe ter da je njegova dolžnost zagotoviti: (a) ureditev, ki zagotavlja, da lahko obveščevalna služba prejme le tiste informacije, ki so potrebne za ustrezno izvajanje njenih nalog, ter da lahko razkrije le tiste informacije, ki so potrebne (i) za navedeni namen, (ii) za namene nacionalne varnosti, (iii) za namene preprečevanja ali odkrivanja hudih kaznivih dejanj ali (iv) za namene katerega koli kazenskega postopka ter (b) da obveščevalna služba ne sme izvajati nobenih ukrepov v korist katere koli politične stranke v Združenem kraljestvu"; člen 2(2) zakona o varnostnih službah iz leta 1989 pa določa, da je „generalni direktor odgovoren za učinkovitost službe ter da mora zagotoviti: (a) ureditev, ki zagotavlja, da lahko služba prejme le tiste informacije, ki so potrebne za ustrezno izvajanje njenih nalog, ter da lahko razkrije le tiste informacije, ki so potrebne za navedeni namen ali namen [preprečevanja ali odkrivanja] hudih kaznivih dejanj [ali katerega koli kazenskega postopka]; (b) da služba ne sme izvajati nobenih ukrepov v korist katere koli politične stranke ter (c) ureditev, v dogovoru z generalnim direktorjem nacionalne agencije za boj proti kriminalu, glede usklajevanja dejavnosti službe na podlagi člena 1(4) tega zakona z dejavnostmi policije, nacionalne agencije za boj proti kriminalu in drugimi agencijami za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj".

(150) Kadar namerava pristojni organ posredovati osebne podatke, ki jih obdeluje na podlagi dela 3 zakona o varstvu podatkov iz leta 2018, organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj iz tretje države, se uporabljajo posebne zahteve ([214]). Taki prenosi lahko zlasti potekajo, kadar temeljijo na predpisih o ustreznosti, ki jih izda pristojni minister, ali če takih predpisov ni, če so zagotovljeni ustrezni zaščitni ukrepi. Člen 75 zakona o varstvu podatkov iz leta 2018 določa, da so ustrezni zaščitni ukrepi zagotovljeni, če so določeni v pravnem instrumentu, ki zavezuje prejemnika, ali če je upravljavec, po proučitvi vseh okoliščin prenosa zadevne vrste osebnih podatkov v tretjo državo ali mednarodno organizacijo, ugotovil, da obstajajo ustrezni zaščitni ukrepi za varstvo podatkov.

(151) Če prenos ne temelji na predpisih o ustreznosti ali na ustreznih zaščitnih ukrepih, se lahko izvede le v določenih specifičnih okoliščinah, imenovanih „posebne okoliščine“ ([215]). Na primer, kadar je prenos potreben: (a) za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe; (b) za zaščito zakonitih interesov posameznika, na katerega se nanašajo osebni podatki; (c) za preprečitev neposredne in resne grožnje javni varnosti države članice ali tretje države; (d) v posameznih primerih za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali (e) v posameznih primerih iz pravnih razlogov (kot na primer v zvezi s sodnimi postopki ali za zagotavljanje pravnih nasvetov). Opozoriti je treba, da se točki (d) in (e) ne uporabljata, če pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, prevladajo nad javnim interesom pri prenosu. Te okoliščine ustrezajo posebnim razmeram in pogojem, ki so v skladu s členom 38 Direktive (EU) 2016/680 opredeljeni kot odstopanja.

(152) Nadalje, kadar se gradivo, ki ga na podlagi odredbe o uporabi prestrezanja ali poseganja v opremo pridobijo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, posreduje tretji državi, zakon o preiskovalnih pooblastilih iz leta 2016 določa dodatne zaščitne ukrepe. Natančneje, tako razkritje, t. i. razkritje v tujino, je dovoljeno le, če organ izdajatelj meni, da je vzpostavljena posebna ustrezna ureditev, v skladu s katero je omejeno število oseb, ki se jim podatki razkrijejo, omejen obseg razkritja gradiva oziroma dajanja gradiva na voljo, ter v kolikšnem obsegu se gradivo lahko kopira in koliko kopij se lahko izdela. Poleg tega lahko organ izdajatelj meni, da je ustrezna ureditev potrebna, da se zagotovi uničenje vsake kopije vsakega dela navedenega gradiva, takoj ko ne obstajajo več razlogi za njihovo hrambo (če niso bile uničene že prej) ([216]).

(153) Nazadnje, posebne oblike nadaljnjega prenosa iz Združenega kraljestva v Združene države bi lahko v prihodnje potekale na podlagi sporazuma med vlado Združenega kraljestva Velika Britanija in Severna Irska ter vlado Združenih držav Amerike o dostopu do elektronskih podatkov za namene boja proti hudim kaznivim dejanjem (Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime; v nadaljnjem besedilu: sporazum med Združenim kraljestvom in ZDA oziroma samo sporazum) ([217]), ki je bil sklenjen oktobra 2019 ([218]). Čeprav navedeni sporazum [v času sprejetja tega sklepa] še ni začel veljati, lahko njegov predvideni začetek veljavnosti vpliva na nadaljnje prenose podatkov, ki so bili najprej preneseni v Združeno kraljestvo na podlagi sklepa, naprej v ZDA. Natančneje, prenosi podatkov iz EU k ponudnikom storitev v Združenem kraljestvu bi lahko bili predmet odredb o predložitvi elektronskih dokazov, ki jih izdajajo pristojni organi ZDA za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, in take odredbe bi se v Združenem kraljestvu uporabljale na podlagi sporazuma med Združenim kraljestvom in ZDA, ko bi ta začel veljati. Zato je ocena pogojev in zaščitnih ukrepov, na podlagi katerih se take odredbe lahko izdajo in izvršijo, pomembna pri izdaji tega sklepa.

([214]) Glej poglavje 5 dela 3 zakona o varstvu podatkov iz leta 2018.

([215]) Člen 76 zakona o varstvu podatkov iz leta 2018.

([216]) Člena 54 in 130 zakona o preiskovalnih pooblastilih iz leta 2016. Organi izdajatelji morajo proučiti, ali je glede posredovanja gradiva tujim organom treba zagotoviti posebne zaščitne ukrepe, ter zagotoviti, da se glede podatkov uporabljajo zaščitni ukrepi v zvezi s hrambo, uničenjem in razkritjem, ki so podobni tistim iz členov 53 in 129 zakona o preiskovalnih pooblastilih iz leta 2016.

([217]) Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([218]) To je prvi sporazum, ki je bil dosežen na podlagi zakona ZDA o pojasnitvah glede zakonite uporabe podatkov v tujini (US Clarifying Lawful Overseas Use of Data (CLOUD) Act). Navedeni zakon je zvezni zakon ZDA, ki je bil sprejet 23. marca 2018 in ki s spremembami zakona o shranjenih komunikacijah iz leta 1986 (Stored Communications Act of 1986) pojasnjuje, da morajo ponudniki storitev iz ZDA izvrševati odredbe ZDA glede razkritja podatkov o vsebini in podatkov, ki ne vključujejo vsebine, ne glede na to, kje so taki podatki shranjeni. Zakon o pojasnitvah glede zakonite uporabe podatkov v tujini omogoča tudi sklepanje izvršilnih sporazumov s tujimi vladami, na podlagi katerih bi lahko ponudniki storitev iz ZDA predložili podatke o vsebini neposredno takim tujim vladam (besedilo zakona je na voljo na povezavi: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) Glede tega je treba najprej poudariti, da se glede vsebinskega področja uporabe sporazum uporablja le za kazniva dejanja, pri katerih je najvišja zagrožena kazen zapora vsaj tri leta (kar je opredeljeno kot „hudo kaznivo dejanje“) ([219]), vključno s „terorističnо dejavnostjo“. Drugič, podatki, ki se obdelujejo v drugih jurisdikcijah, se lahko na podlagi navedenega sporazuma pridobijo le na podlagi „odločbe […], ki je podvržena preverjanju ali nadzoru sodišča, sodnika, mirovnega sodnika ali drugega neodvisnega organa na podlagi notranjega prava pogodbenice izdajateljice, pred ali med postopkom v zvezi z izvršitvijo odredbe“ ([220]). Tretjič, vsaka odredba mora „temeljiti na zahtevah glede razumne utemeljitve na podlagi jasnih in tehtnih dokazov, posebnosti, zakonitosti in resnosti preiskovanega ravnanja“ ([221]) ter se mora „nanašati na specifične račune ter opredeliti specifično osebo, račun, naslov ali osebno napravo ali kateri koli drug natančen način opredelitve“ ([222]). Četrtič, podatki, pridobljeni na podlagi tega sporazuma, so zaščiteni enako kot na podlagi posebnih zaščitnih ukrepov iz tako imenovanega krovnega sporazuma med ZDA in EU ([223]) (celovit sporazum o varstvu podatkov, ki sta ga decembra 2016 sklenila EU in ZDA ter ki določa zaščitne ukrepe in pravice glede prenosa podatkov na področju sodelovanja pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj), ki so vsi vključeni v ta sporazum s sklicevanjem na smiselno upoštevanje posebne narave prenosa (tj. prenosi od zasebnih subjektov k organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, in ne prenosi med takimi organi) ([224]). Sporazum med Združenim kraljestvom in ZDA izrecno določa, da se „glede vseh osebnih podatkov, predloženih v okviru izvršitve odredb na podlagi sporazuma o zagotovitvi enakovredne zaščite“ uporablja enakovredna zaščita tisti, ki je določena v krovnem sporazumu med EU in ZDA ([225]).

(155) Za prenose podatkov organom ZDA na podlagi sporazuma med Združenim kraljestvom in ZDA bi morala torej veljati zaščita, ki izhaja iz instrumenta prava EU, ob ustreznih prilagoditvah, da se upošteva narava zadevnega prenosa. Organi Združenega kraljestva so nadalje potrdili, da se zaščita na podlagi krovnega sporazuma uporablja za vse osebne podatke, ki se predložijo ali zavarujejo na podlagi sporazuma, ne glede na naravo ali vrsto organa, ki predloži zahtevo (na primer zvezni organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter tisti na ravni posameznih zveznih držav v ZDA), tako da je treba enakovredno zaščito zagotoviti v vseh primerih. Vendar pa so organi Združenega kraljestva pojasnili tudi, da pogovori o podrobnostih konkretnega izvajanja zaščitnih ukrepov za varstvo podatkov med Združenim kraljestvom in ZDA še potekajo. V okviru pogovorov s službami Evropske komisije glede tega sklepa so organi Združenega kraljestva potrdili, da bodo začetek veljavnosti sporazuma omogočili le, ko bodo prepričani, da je njegovo izvrševanje skladno s pravnimi obveznostmi v njem, vključno z jasnostjo glede zagotavljanja skladnosti s standardi varstva podatkov glede katerih koli podatkov, ki se zahtevajo na podlagi sporazuma. Ker bi morebiten začetek veljavnosti sporazuma lahko vplival na raven varstva, ki se ocenjuje s tem sklepom, bi moralo Združeno kraljestvo Evropski komisiji posredovati vse informacije in prihodnja pojasnila glede tega, kako bodo ZDA izpolnjevale svoje obveznosti na podlagi sporazuma, takoj, ko so na voljo, v vsakem primeru pa pred začetkom veljavnosti sporazuma, da se zagotovi ustrezno spremljanje tega sklepa, v skladu s členom 45(4) Uredbe (EU) 2016/679. Posebna pozornost bo namenjena uporabi in prilagoditvi zaščit posebnih vrst prenosov iz krovnega sporazuma, kot so urejene v sporazumu med Združenim kraljestvom in ZDA.

(156) Splošneje, vsak zadevni dogodek v zvezi z začetkom veljavnosti in uporabo sporazuma bo ustrezno upoštevan v okviru stalnega spremljanja izvajanja tega sklepa, tudi glede potrebnih posledic v primeru kakršnih koli indicev, da v osnovi enakovredna raven varstva ni več zagotovljena.

3.2.3 *Nadzor*

(157) Različni organi zagotavljajo nadzor nad uporabo pooblastil, odvisno od pooblastil pristojnih organov pri obdelavi osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (na podlagi zakona o varstvu podatkov iz leta 2018 ali na podlagi zakona o preiskovalnih pooblastilih iz leta 2016). Informacijski pooblaščenec nadzira obdelavo osebnih podatkov, če ta spada na področje dela 3 zakona o varstvu podatkov iz leta

([219]) Člen 1(14) sporazuma.
([220]) Člen 5(2) sporazuma.
([221]) Člen 5(1) sporazuma.
([222]) Člen 4(5) sporazuma. Glede prestrezanja v realnem času se uporablja dodaten strožji standard: odredbe morajo biti časovno omejene, in sicer le na obdobje, ki je razumno potrebno za dosedanje namena odredbe; prav tako jih je mogoče izdati le, če istih informacij ne bi bilo razumno mogoče pridobiti z manj intruzivnimi metodami (člen 5(3) sporazuma).
([223]) Sporazum med Združenimi državami Amerike in Evropsko unijo o varstvu osebnih podatkov pri preprečevanju, preiskovanju, odkrivanju in pregonu kaznivih dejanj (UL L 336, 10.12.2016, str. 3, na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.
([224]) Člen 9(1) sporazuma.
([225]) Člen 9(1) sporazuma.

2018 ([226]). Neodvisen in sodni nadzor uporabe preiskovalnih pooblastil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 zagotavlja urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil (Investigatory Powers Commissioner's Office (IPCO)) ([227]) (ta del je obravnavan v uvodnih izjavah (250) do (255)). Dodaten nadzor zagotavljajo parlament ter drugi organi.

3.2.3.1 Nadzor nad delom 3 zakona o varstvu podatkov iz leta 2018

(158) Splošne naloge informacijskega pooblaščenca (katerega neodvisnost in organizacija sta pojasnjeni v uvodni izjavi (87)) v zvezi z obdelavo osebnih podatkov, ki spadajo na področje dela 3 zakona o varstvu podatkov iz leta 2018, so določene v dodatku 13 k zakonu o varstvu podatkov iz leta 2018. Glavne naloge urada informacijskega pooblaščenca so spremljanje in izvrševanje dela 3 zakona o varstvu podatkov iz leta 2018, ozaveščanje javnosti ter svetovanje parlamentu, vladi in drugim institucijam in organom. Informacijski pooblaščenec zaradi vzdrževanja neodvisnosti sodstva ne sme izvajati nalog v zvezi z obdelavo osebnih podatkov, ki jo izvaja posameznik ali sodišče v okviru svoje sodne pristojnosti. V takih okoliščinah bi nadzorne naloge izvajali drugi organi, kot je pojasnjeno v uvodnih izjavah (99) do (103).

(159) Informacijski pooblaščenec ima splošna preiskovalna in popravljalna pooblastila, pooblastila v zvezi z odobritvami in svetovalne pristojnosti, ki se nanašajo na obdelavo osebnih podatkov, za katero se uporablja del 3. Informacijski pooblaščenec lahko obvešča upravljavca ali obdelovalca o domnevnih kršitvah dela 3 zakona o varstvu podatkov iz leta 2018, izdaja opozorila ali opomine upravljavcem ali obdelovalcem, ki kršijo določbe dela 3 navedenega zakona, ter na lastno pobudo ali na zahtevo izdaja mnenja parlamentu, vladi ali drugim institucijam in organom ter javnosti o vseh vprašanjih, ki se nanašajo na varstvo podatkov ([228]).

(160) Informacijski pooblaščenec lahko tudi izdaja obvestila o predložitvi informacij ([229]), obvestila o preverjanju ([230]) in obvestila o izvršitvi ([231]), ima pa tudi pravico do dostopa do dokumentov upravljavcev in obdelovalcev ter do njihovih prostorov ([232]) in lahko izdaja upravne globe v obliki obvestil o plačilnem nalogu ([233]). Politika urada informacijskega pooblaščenca o regulativnih ukrepih (Regulatory Action Policy) določa okoliščine, v katerih urad izdaja obvestila o predložitvi informacij, preverjanju, izvršitvi in plačilnem nalogu ([234]) (glej tudi uvodno izjavo (93) in uvodni izjavi 101 in 102 Direktive (EU) 2016/680, ki se nanašata na sklepe o ustreznosti).

(161) Iz zadnjih letnih poročil informacijskega pooblaščenca (2018–2019 ([235]), 2019–2020 ([236])) je razvidno, da je izvedel več preiskav in sprejel izvršilne ukrepe glede obdelave podatkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Oktobra 2019 je na primer izvedel preiskavo in objavil mnenje v zvezi z uporabo tehnologije za prepoznavanje obrazov na javnih mestih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Preiskava je bila usmerjena zlasti na uporabo zmogljivosti prepoznavanja obrazov v živo pri policiji južnega Walesa in londonski policiji (Metropolitan Police Service). Informacijski pooblaščenec je preiskoval tudi „Gangs matrix" (matriko tolp) ([237]) londonske policije in ugotovil vrsto resnih kršitev zakonodaje o varstvu podatkov, ki bi lahko omajale zaupanje javnosti v matriko in uporabo podatkov. Novembra 2018 je informacijski pooblaščenec izdal obvestilo o izvršitvi, londonska policija pa je nato sprejela ukrepe, potrebne za povečanje varnosti in odgovornosti ter zagotovitev sorazmerne uporabe

([226]) Člen 116 zakona o varstvu podatkov iz leta 2018.
([227]) Glej zakon o preiskovalnih pooblastilih iz leta 2016 in zlasti poglavje 1 dela 8.
([228]) Točka 2 dodatka 13 k zakonu o varstvu podatkov iz leta 2018.
([229]) Odredba upravljavcu in obdelovalcu (ter v določenih okoliščinah kateri koli drugi osebi), naj predloži potrebne informacije (člen 142 zakona o varstvu podatkov iz leta 2018).
([230]) Omogoča izvedbo preiskav in revizij, na podlagi katerih mora upravljavec ali obdelovalec morda dovoliti informacijskemu pooblaščencu vstop v določene prostore, pregled ali proučitev dokumentov ali opreme in razgovore z osebami, ki obdelujejo osebne podatke v imenu upravljavca (člen 146 zakona o varstvu podatkov iz leta 2018).
([231]) Omogoča izvrševanje popravljalnih pooblastil, na podlagi katerih mora upravljavec/obdelovalec določen ukrep izvesti ali se ga vzdržati (člen 149 zakona o varstvu podatkov iz leta 2018).
([232]) Člen 154 zakona o varstvu podatkov iz leta 2018.
([233]) Člen 155 zakona o varstvu podatkov iz leta 2018.
([234]) Politika urada informacijskega pooblaščenca o regulativnih ukrepih, opomba 96.
([235]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2018–2019, opomba 101.
([236]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2019–2020, opomba 82.
([237]) Zbirka podatkov, v kateri so bili evidentirani obveščevalni podatki v zvezi z domnevnimi člani tolp in žrtvami kaznivih dejanj, povezanih s tolpami.

podatkov. Drug primer izvršilnega ukrepa na tem področju je globa v višini 325000 GBP, ki jo je informacijski pooblaščenec maja 2018 naložil državnemu tožilstvu zaradi izgube nešifriranega DVD-ja s posnetki informativnih razgovorov pri policiji. Informacijski pooblaščenec je izvajal tudi preiskave širših tem, na primer v prvi polovici leta 2020 o uporabi pridobivanja podatkov iz mobilnih telefonov za policijske namene ter obdelavi podatkov žrtev s strani policije. Poleg tega informacijski pooblaščenec trenutno preiskuje zadevo, ki se nanaša na dostop organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj do podatkov, ki jih hrani subjekt zasebnega prava, Clearview AI Inc ([238]).

(162) Poleg pooblastil informacijskega pooblaščenca za izvrševanje, navedenih v uvodnih izjavah (160) in (161), se nekatere kršitve zakonodaje o varstvu podatkov štejejo za kazniva dejanja, zato so lahko zanje izrečejo kazenske sankcije (člen 196 zakona o varstvu podatkov iz leta 2018). To se na primer nanaša na pridobivanje, razkritje ali hrambo osebnih podatkov brez privolitve upravljavca ter zagotovitev razkritja osebnih podatkov drugi osebi brez privolitve upravljavca ([239]); ponovno identifikacijo informacij v primeru anonimizacije osebnih podatkov brez privolitve upravljavca, ki je odgovoren za anonimizacijo osebnih podatkov ([240]); namerno oviranje informacijskega pooblaščenca pri izvrševanju njegovih pooblastil v zvezi s preverjanjem osebnih podatkov v skladu z mednarodnimi obveznostmi ([241]), dajanje neresničnih izjav v odgovor na obvestilo o predložitvi informacij ali uničenje informacij v zvezi z obvestilom o predložitvi informacij ali obvestilom o preverjanju ([242]).

3.2.3.2 Drugi nadzorni organi na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

(163) Poleg informacijskega pooblaščenca na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj obstaja več nadzornih organov s posebnimi pooblastili glede varstva podatkov. Med njimi so na primer pooblaščenec za hrambo in uporabo biometričnih podatkov (Commissioner for the Retention and Use of Biometric Material; v nadaljnjem besedilu: pooblaščenec za biometrične podatke) ([243]) in pooblaščenec za uporabo nadzornih kamer (Surveillance Camera Commissioner) ([244]).

3.2.3.3 Parlamentarni nadzor na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj

(164) Parlamentarni odbor za notranje zadeve (Home Affairs Select Committee (HASC)) zagotavlja parlamentarni nadzor na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj Sestavlja ga 11 poslancev iz treh največjih političnih strank. Naloga odbora je preverjati izdatke, upravljanje in politiko ministrstva za notranje zadeve ter zadevnih javnih organov, tj. tudi policije in nacionalne agencije za boj proti kriminalu (NCA), katerih delo lahko odbor posebej nadzira ([245]).

([238]) Izjava urada informacijskega pooblaščenca je na voljo na povezavi: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

([239]) Člen 170 zakona o varstvu podatkov iz leta 2018.

([240]) Člen 171 zakona o varstvu podatkov iz leta 2018.

([241]) Člen 119(6) zakona o varstvu podatkov iz leta 2018.

([242]) V poslovnem letu od 1. aprila 2019 do 31. marca 2020 so bila na podlagi preiskav urada informacijskega pooblaščenca izdana štiri opozorila in osem predlogov za pregon. V navedenih zadevah je bil pregon izveden na podlagi člena 55 zakona o varstvu podatkov iz leta 1998, člena 77 zakona o dostopu do informacij javnega značaja iz leta 2000 (Freedom of Information Act 2000) ter člena 170 zakona o varstvu podatkov iz leta 2018. V 75 % zadev so se obdolženci izrekli za krive, s čimer so se izognili dolgotrajnim sodnim postopkom in s tem povezanim stroškom (Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2019–2020, opomba 87, stran 40).

([243]) Funkcija pooblaščenca za biometrične podatke je bila ustanovljena na podlagi zakona o varstvu svoboščin iz leta 2012 (Protection of Freedoms Act 2012, glej: https://www.legislation.gov.uk/ukpga/2012/9/contents). Med drugim se pooblaščenec za biometrične podatke odloči, ali lahko policija hrani evidenco profilov DNK in prstne odtise, pridobljene od prijetih posameznikov, ki niso obtoženi kaznivega dejanja (člen 63G zakona o policiji in kazenskih evidencah iz leta 1984). Poleg tega je pooblaščenec za biometrične podatke na splošno odgovoren za spremljanje hrambe in uporabe DNK in prstnih odtisov ter hrambo iz razlogov nacionalne varnosti (člen 20(2) zakona o varstvu svoboščin iz leta 2012). Pooblaščenec za biometrične podatke se imenuje v skladu s kodeksom za javna imenovanja (Code for Public Appointments), na voljo na naslednji povezavi: https://www.gov.uk/government/publications/governance-code-for-public-appointments, pogoji za imenovanje pa jasno določajo, da ga lahko razreši samo minister za notranje zadeve v natančno določenih okoliščinah, ki vključujejo neizpolnjevanje nalog v obdobju treh mesecev, obsodbo za kaznivo dejanje ali nespoštovanje pogojev za imenovanje.

([244]) Pooblaščenec za uporabo nadzornih kamer je bil ustanovljen na podlagi zakona o varstvu svoboščin iz leta 2012, njegova naloga pa je spodbujati zagotavljanje skladnosti s kodeksom ravnanja glede uporabe nadzornih kamer (Surveillance Camera Code of Practice), preverjanje delovanja navedenega kodeksa in svetovanje ministrom o tem, ali bi bilo treba navedeni kodeks spremeniti. Pooblaščenec se imenuje v skladu z enakimi pravili kot pooblaščenec za biometrične podatke in ima podobne pristojnosti, sredstva in zaščito pred razrešitvijo.

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

(165) V okviru svojih pristojnosti lahko odbor sam izbere predmet obravnave, tudi posamezne zadeve, pod pogojem, da vprašanje ni predmet sodnega postopka. Odbor lahko zahteva tudi pisna ali ustna dokazila od različnih zadevnih skupin in posameznikov. O svojih ugotovitvah sestavi poročilo ter izdaja priporočila vladi ([246]). Vlada se mora na vsako priporočilo iz poročila odzvati v 60 dneh ([247]).

(166) V zvezi z obveščevalno dejavnostjo je odbor izdal tudi poročilo o zakonu o urejanju preiskovalnih pooblastil iz leta 2000 ([248]), v katerem je bilo ugotovljeno, da navedeni zakon ne ustreza svojemu namenu. Navedeno poročilo je bilo upoštevano pri nadomeščanju pomembnih delov zakona o urejanju preiskovalnih pooblastil iz leta 2000 z zakonom o preiskovalnih pooblastilih iz leta 2016. Celoten seznam preiskav je na voljo na spletišču odbora ([249]),

(167) Na Škotskem naloge parlamentarnega odbora za notranje zadeve opravlja pravosodni pododbor za področje policije (Justice Subcommittee on Policing), na Severnem Irskem pa odbor za pravosodje (Committee for Justice) ([250]).

3.2.4 *Pravna sredstva*

(168) V vezi z obdelavo podatkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj so mehanizmi pravnih sredstev opredeljeni v delu 3 zakona o varstvu podatkov iz leta 2018, zakonu o preiskovalnih pooblastilih iz leta 2016 ter zakonu o človekovih pravicah iz leta 1998.

(169) Ti mehanizmi posameznikom, na katere se nanašajo osebni podatki, zagotavljajo učinkovita upravna in sodna pravna sredstva, ki jim omogočajo zlasti uveljavljanje pravic, vključno s pravico do dostopa do svojih osebnih podatkov, njihovega popravka ali izbrisa.

(170) Prvič, na podlagi člena 165 zakona o varstvu podatkov iz leta 2018 ima posameznik, na katerega se nanašajo osebni podatki, pravico vložiti pritožbo pri informacijskem pooblaščencu, če meni, da je v zvezi z osebnimi podatki, ki se nanašajo nanj, prišlo do kršitve dela 3 zakona o varstvu podatkov iz leta 2018 ([251]). Informacijski pooblaščenec lahko preveri, kako upravljavec in obdelovalec zagotavljata skladnost z zakonom o varstvu podatkov iz leta 2018, od njiju zahteva, da v primeru neskladnosti sprejmeta potrebne ukrepe, ter naloži globe.

([246]) Za odbore, vključno s parlamentarnim odborom za notranje zadeve, veljajo poslovniki spodnjega doma parlamenta. Poslovniki (Standing Orders) so pravila, ki jih sprejme spodnji dom parlamenta in ki urejajo način poslovanja parlamenta. Odbori imajo široke pristojnosti, saj poslovnik št. 152(1) določa, da se „odbori oblikujejo z namenom preverjanja izdatkov, upravljanja in politik glavnih ministrstev, kot je določeno v točki 2 tega poslovnika, in zadevnih javnih organov“. Na podlagi tega lahko parlamentarni odbor za notranje zadeve obravnava vsako politiko ministrstva za notranje zadeve, vključno s politikami (in zadevno zakonodajo) o preiskovalnih pooblastilih. Poslovnik št. 152(4) tudi jasno določa, da imajo odbori razne pristojnosti, med drugim lahko od oseb zahtevajo predložitev dokazil ali dokumentov o posameznem vprašanju ali predložitev poročil. Trenutne in pretekle preiskave odbora so na voljo na povezavi: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Pristojnosti parlamentarnega odbora za notranje zadeve v Angliji in Walesu so določene v poslovnikih spodnjega doma parlamenta, ki so na voljo na povezavi: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Na voljo na povezavi: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) Na voljo na povezavi: https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Pravila pravosodnega pododbora za področje policije na Škotskem so na voljo na povezavi: https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, pravila odbora za pravosodje na Severnem Irskem pa na povezavi: http://www.niassembly.gov.uk/assembly-business/standing-orders/].

([251]) Zadnje letno poročilo urada informacijskega pooblaščenca vsebuje razčlembo vrst prejetih in zaključenih pritožb. Število prejetih pritožb, ki se nanašajo na „delovanje policije in kazenske evidence“, znaša 6 % skupnega števila prejetih pritožb (kar je 1 % več kot v predhodnem poslovnem letu). Iz letnega poročila tudi izhaja, da se največ pritožb nanaša na zahteve posameznikov za dostop (46 % vseh pritožb, kar je 8 % več kot v predhodnem poslovnem letu; letno poročilo urada informacijskega pooblaščenca za obdobje 2019–2020, stran 55; opomba 88).

(171) Drugič, zakon o varstvu podatkov iz leta 2018 določa pravico do pravnega sredstva zoper informacijskega pooblaščenca, če ta ne obravnava ustrezno pritožbe posameznika, na katerega se nanašajo osebni podatki. Natančneje, če informacijski pooblaščenec ne obravnava ([252]) pritožbe posameznika, na katerega se nanašajo osebni podatki, lahko pritožnik zahteva sodno presojo, saj se lahko pritoži pri sodišču prve stopnje ([253]) in zahteva, naj se informacijskemu pooblaščencu odredi ustrezna obravnava pritožbe ali pa naj se pritožnika obvešča o obravnavi pritožbe ([254]). Poleg tega se lahko vsakdo, ki mu informacijski pooblaščenec izda katerega koli od navedenih obvestil (o predložitvi informacij, o preverjanju, o izvršitvi ali o plačilnem nalogu), pritoži pri sodišču prve stopnje. Če sodišče ugotovi, da odločba informacijskega pooblaščenca ni v skladu s pravom ali da bi moral informacijski pooblaščenec odločiti drugače, mora sodišče pritožbo dovoliti ali obvestilo oziroma odločbo informacijskega pooblaščenca nadomestiti z drugo ([255]).

(172) Tretjič, posamezniki lahko pravna sredstva zoper upravljavce in obdelovalce uveljavljajo neposredno pred sodišči. Natančneje, na podlagi člena 167 zakona o varstvu podatkov iz leta 2018 lahko posameznik, na katerega se nanašajo osebni podatki, vloži vlogo pri sodišču zaradi kršitve svojih pravic na podlagi zakonodaje o varstvu podatkov, sodišče pa lahko z odločbo od upravljavca zahteva, da sprejme (ali se vzdrži) kakršnih koli ukrepov v zvezi z obdelavo, da se zagotovi skladnost z zakonom o varstvu podatkov iz leta 2018. Poleg tega lahko v skladu s členom 169 zakona o varstvu podatkov iz leta 2018 vsaka oseba, ki je utrpela škodo zaradi kršitve zahteve iz zakonodaje o varstvu podatkov (vključno z delom 3 zakona o varstvu podatkov iz leta 2018), razen na podlagi UK GDPR, upravičena do odškodnine za škodo, ki jo je povzročil upravljavec ali obdelovalec, razen če upravljavec ali obdelovalec dokaže, da nikakor ni odgovoren za dogodek, na podlagi katerega je nastala škoda. Škoda vključuje finančno in nefinančno izgubo, kot je na primer stiska.

(173) Nazadnje, vsaka oseba, ki meni, da je kateri koli javni organ kršil njene pravice, vključno s pravico do zasebnosti in varstva podatkov, lahko vloži pravno sredstvo pri sodišču Združenega kraljestva na podlagi zakona o človekovih pravicah iz leta 1998 ([256]); ko izkoristi vsa notranja pravna sredstva, pa lahko oseba, nevladna organizacija in skupina posameznikov vloži pravno sredstvo pri Evropskem sodišču za človekove pravice zaradi kršitve pravic, zagotovljenih na podlagi Evropske konvencije o varstvu človekovih pravic ([257]) (glej uvodno izjavo (111)).

3.2.4.1 Mehanizmi pravnih sredstev, ki so na voljo na podlagi zakona o preiskovalnih pooblastilih iz leta 2016

(174) Posamezniki lahko zaradi kršitev zakona o preiskovalnih pooblastilih iz leta 2016 vložijo pravna sredstva pri sodišču, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal). Pravna sredstva, ki so na voljo na podlagi zakona o preiskovalnih pooblastilih iz leta 2016, so opisana tudi v uvodnih izjavah (263)–(269) below.

([252]) Člen 166 zakona o varstvu podatkov iz leta 2018 se nanaša predvsem na naslednje okoliščine: (a) če informacijski pooblaščenec ne sprejme ustreznih ukrepov v odgovor na pritožbo; (b) če informacijski pooblaščenec pritožnika ne obvesti o stanju zadeve ali odločitvi o pritožbi v treh mesecih od dne, ko informacijski pooblaščenec prejme pritožbo; ali (c) če informacijski pooblaščenec v navedenem roku ne odloči o pritožbi in pritožnika ne obvesti o tem v nadaljnjih treh mesecih.

([253]) Sodišče prve stopnje je pristojno za obravnavo pritožb zoper odločitve vladnih regulativnih organov. Pristojni senat za obravnavo odločitev informacijskega pooblaščenca je splošni regulativni senat (General Regulatory Chamber), ki je pristojen za celotno Združeno kraljestvo.

([254]) Člen 166 zakona o varstvu podatkov iz leta 2018. Primera uspešne pritožbe pri sodišču zoper urad informacijskega pooblaščenca sta zadeva, v kateri je urad informacijskega pooblaščenca potrdil prejetje pritožbe posameznika, na katerega se nanašajo osebni podatki, vendar ga ni obvestil, kako namerava ukrepati, zato mu je bilo naloženo, naj v 21 dneh potrdi, ali bo pritožbo obravnaval, ter če jo bo, naj pritožnika najpozneje vsakih 21 koledarskih dni obvešča o napredovanju obravnave (sodba še ni bila objavljena); ter zadeva, v kateri je sodišče prve stopnje menilo, da ni jasno, ali odgovor urada informacijskega pooblaščenca pritožniku pomeni tudi „rezultat“ pritožbe (glej zadevo Susan Milne v The Information Commissioner [2020], ki je na voljo na povezavi: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) Člena 162 in 163 zakona o varstvu podatkov iz leta 2018.

([256]) Glej na primer zadevo Brown v Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, pri kateri je bila na podlagi zakona o varstvu podatkov iz leta 1998 in zakona o človekovih pravicah iz leta 1998 dosojena odškodnina v višini 9000 GBP zaradi nezakonite pridobitve in zlorabe osebnih podatkov, ter zadevo R (on the application of Bridges) v Chief Constable of South Wales [2020] EWCA Civ 1058, pri kateri je sodišče Court of Appeal ugotovilo, da je uporaba sistema za prepoznavanje obrazov s strani valižanske policije nezakonita, saj krši člen 8 EKČP, ocena učinka v zvezi z varstvom podatkov, ki jo je predložil upravljavec, pa ni bila skladna z zakonom o varstvu podatkov iz leta 2018.

([257]) Člen 34 Evropske konvencije o varstvu človekovih pravic določa, da „[s]odišče lahko sprejme pritožbo od katerekoli osebe, nevladne organizacije ali skupine posameznikov, ki zatrjujejo, da so žrtve kršitev pravic, priznanih s Konvencijo in njenimi protokoli, s strani katerekoli Visoke pogodbene stranke. Visoke pogodbene stranke se zavezujejo, da na noben način ne bodo ovirale dejanskega izvajanja te pravice.“

3.3 **Dostop in uporaba s strani javnih organov Združenega kraljestva za namene nacionalne varnosti**

(175) V pravnem redu Združenega kraljestva velja, da so iz razlogov nacionalne varnosti, v okoliščinah, pomembnih za oceno ustreznosti, naslednje obveščevalne službe pristojne za zbiranje elektronskih podatkov, ki jih hranijo upravljavci ali obdelovalci: varnostna služba (Security Service, MI5) ([258]), tajna obveščevalna služba (Secret Intelligence Service, SIS) ([259]) in vladna obveščevalna služba (Government Communications Headquarters ([260]), GCHQ) ([261]).

3.3.1 *Pravna podlaga, omejitve in zaščitni ukrepi*

(176) V Združenem kraljestvu so pooblastila obveščevalnih služb opredeljena v zakonu o preiskovalnih pooblastilih iz leta 2016 in v zakonu o urejanju preiskovalnih pooblastil iz leta 2000, ki skupaj z zakonom o varstvu podatkov iz leta 2018 določata materialno in osebno področje uporabe teh pooblastil ter omejitve in zaščitne ukrepe za njihovo uporabo. Navedena pooblastila ter omejitve in zaščitni ukrepi, ki se nanašajo nanje, so podrobneje ocenjena v oddelkih v nadaljevanju.

3.3.1.1 Preiskovalna pooblastila, ki se izvršujejo v okviru nacionalne varnosti

(177) Zakon o preiskovalnih pooblastilih iz leta 2016 določa pravni okvir za uporabo preiskovalnih pooblastil, tj. pooblastil za prestrezanje komunikacijskih podatkov, dostop do njih in poseganje v opremo. Navedeni zakon uvaja splošno prepoved in določa, da je uporaba tehnik, ki omogočajo dostop do vsebine komunikacij, dostop do komunikacijskih podatkov ali poseganje v opremo brez zakonitega pooblastila kaznivo dejanje ([262]). To se odraža v dejstvu, da je uporaba teh preiskovalnih pooblastil zakonita le, če se izvaja na podlagi odredbe ali pooblastila ([263]).

(178) Zakon o preiskovalnih pooblastilih iz leta 2016 določa podrobna pravila, ki urejajo področje uporabe in uporabo posameznih preiskovalnih pooblastil ter njihove omejitve in zaščitne ukrepe. Uporabljajo se različna pravila, odvisno od vrste preiskovalnih pooblastil (prestrezanje komunikacij, pridobivanje in hramba komunikacijskih podatkov ter poseganje v opremo), pa tudi od tega, ali se pooblastilo izvršuje na specifičnem

([258]) Varnostna služba MI5 deluje pod vodstvom ministra za notranje zadeve. Njene naloge določa zakon o varnostnih službah iz leta 1989: zaščita nacionalne varnosti (vključno z zaščito pred grožnjami vohunjenja, terorizma in sabotaže, dejavnostmi agentov tujih sil ter dejavnostmi, katerih namen je zrušiti ali spodkopati parlamentarno demokracijo s političnimi, gospodarskimi ali nasilnimi sredstvi), zaščita gospodarske blaginje Združenega kraljestva pred zunanjimi grožnjami ter podpora dejavnostim policije in drugih agencij za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj pri preprečevanju in odkrivanju hudih kaznivih dejanj.

([259]) Tajna obveščevalna služba (SIS) deluje pod vodstvom ministra za zunanje zadeve, njene naloge pa so opredeljene v zakonu o obveščevalnih službah iz leta 1994. Njene naloge so pridobivanje in zagotavljanje informacij o dejavnostih ali namenih oseb zunaj Britanskega otočja ter izvajanje drugih nalog v zvezi z dejanji ali nameni takih oseb. Te naloge se lahko izvajajo le v interesu nacionalne varnosti, v interesu gospodarske blaginje Združenega kraljestva ali za preprečevanje oziroma odkrivanje hudih kaznivih dejanj.

([260]) Vladna obveščevalna služba GCHQ deluje pod vodstvom ministra za zunanje zadeve, njene naloge pa so opredeljene v zakonu o obveščevalnih službah iz leta 1994. Te so: (a) spremljanje, uporaba elektromagnetnih in drugih emisij in opreme, ki take emisije oddaja, ali poseganje vanje, pridobivanje in zagotavljanje informacij, ki izhajajo iz takih emisij ali opreme in iz šifriranega gradiva ali ki se nanje nanaša; (b) zagotavljanje nasvetov in pomoči pri uporabi jezika, vključno s terminologijo, ki se uporablja za tehnične zadeve in kriptografijo ter druge zadeve v zvezi z varstvom informacij za oborožene sile, vlado ali druge organizacije ali osebe, za katere se šteje, da so ustrezne. Te naloge se lahko izvajajo le v interesu nacionalne varnosti, v interesu gospodarske blaginje Združenega kraljestva, v zvezi z dejavnostmi ali nameni oseb zunaj Britanskega otočja, ali za preprečevanje oziroma odkrivanje hudih kaznivih dejanj.

([261]) Drugi javni organi, ki izvajajo naloge v zvezi z nacionalno varnostjo, so obrambna obveščevalna služba (Defence Intelligence (DI)), nacionalni varnostni svet in sekretariat (National Security Council and Secretariat), skupna obveščevalna organizacija (Joint Intelligence Organisation) in skupni obveščevalni odbor (Joint Intelligence Committee). Vendar pa skupni obveščevalni odbor in skupna obveščevalna organizacija na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 nimata preiskovalnih pooblastil, obrambna obveščevalna služba pa ima omejena pooblastila.

([262]) Prepoved se nanaša na javna in zasebna komunikacijska omrežja ter na javno poštno službo, kadar se prestrezanje izvaja v Združenem kraljestvu. Prepoved pa se ne uporablja za upravljavca zasebnega omrežja, če je upravljavec izrecno ali tiho privolil v izvajanje prestrezanja (člen 3 zakona o preiskovalnih pooblastilih iz leta 2016).

([263]) V nekaterih omejenih primerih je mogoče tudi zakonito prestrezanje brez odredbe, npr. kadar se prestrezanje izvaja na podlagi privolitve pošiljatelja ali prejemnika (člen 44 zakona o preiskovalnih pooblastilih iz leta 2016), za omejene upravne ali izvršilne namene (členi 45 do 48 zakona o preiskovalnih pooblastilih iz leta 2016), v nekaterih posebnih ustanovah (členi 49 do 51 zakona o preiskovalnih pooblastilih iz leta 2016) ter v skladu z zahtevami iz tujine (člen 52 zakona o preiskovalnih pooblastilih iz leta 2016).

cilju ([264]) ali v večjem obsegu. Podrobnosti o področju uporabe, zaščitnih ukrepih in omejitvah vsakega ukrepa iz zakona o preiskovalnih pooblastilih iz leta 2016 so navedene v posebnem oddelku v nadaljevanju.

(179) Poleg tega Zakon o preiskovalnih pooblastilih iz leta 2016 dopolnjuje več zakonskih kodeksov ravnanja, ki jih je izdal pristojni minister, odobrila pa oba domova parlamenta ([265]); uporabljajo se v vsej državi in zagotavljajo dodatne smernice glede uporabe navedenih pooblastil ([266]). Medtem ko se lahko posamezniki, na katere se nanašajo osebni podatki, pri uveljavljanju svojih pravic sklicujejo neposredno na določbe zakona o preiskovalnih pooblastilih iz leta 2016, točka 5 dodatka 7 k navedenemu zakonu določa, da je kodeks ravnanja dopusten kot dokaz v civilnih in kazenskih postopkih, sodišče ali nadzorni organ pa lahko vsako neskladnost s kodeksom upošteva pri obravnavi zadevnih vprašanj v sodnih postopkih ([267]). V okviru ocene „kakovosti zakonodaje“ prejšnje zakonodaje Združenega kraljestva na področju nadzora, tj. zakona o urejanju preiskovalnih pooblastil iz leta 2000, je veliki senat Evropskega sodišča za človekove pravice izrecno priznal pomembnost kodeksa ravnanja Združenega kraljestva in sprejel, da bi se njegove določbe lahko upoštevale pri ocenjevanju predvidljivosti zakonodaje, ki dovoljuje nadzor ([268]).

(180) Opozoriti je treba, da so ciljna pooblastila (ciljno prestrezanje ([269]), pridobivanje komunikacijskih podatkov ([270]), hramba komunikacijskih podatkov ([271]) in ciljno poseganje v opremo ([272])) na voljo agencijam za nacionalno varnost in nekaterim organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ([273]), vendar pa lahko le obveščevalne službe navedena pooblastila izvršujejo neciljno (torej prestrezanje v večjem obsegu ([274]), pridobivanje komunikacijskih podatkov v večjem obsegu ([275]), poseganje v opremo v večjem obsegu ([276]) in nabori osebnih podatkov v večjem obsegu ([277])).

(181) Pri odločanju o tem, katera preiskovalna pooblastila naj se uporabijo, mora obveščevalna agencija zagotoviti skladnost s „splošnimi obveznostmi glede zasebnosti“ iz člena 2(2)(a) zakona o preiskovalnih pooblastilih iz leta 2016, ki vključujejo preskus potrebnosti in sorazmernosti. Natančneje, na podlagi te določbe mora javni organ, ki namerava uporabiti preiskovalno pooblastilo, preveriti, (i) ali bi bilo tisto, kar se želi doseči na podlagi odredbe,

([264]) Kar zadeva na primer področje uporabe takih ukrepov, je v delih 3 in 4 (hramba in pridobivanje komunikacijskih podatkov) področje uporabe ukrepa strogo povezano z opredelitvijo „telekomunikacijskih operaterjev“, katerih podatki uporabnikov so predmet ukrepa. Drug primer je uporaba pooblastil v večjem obsegu. V tem primeru je uporaba teh pooblastil omejena na „komunikacije, ki jih pošljejo ali prejmejo posamezniki zunaj Britanskega otočja“.

([265]) Dodatek 7 k zakonu o preiskovalnih pooblastilih iz leta 2016 določa področje uporabe kodeksov, postopek, ki ga je treba upoštevati pri njihovi izdaji, pravila glede njihovega spreminjanja in njihove učinke.

([266]) Kodeks ravnanja na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 je na voljo na povezavi: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Sodišča uporabljajo kodekse ravnanja pri oceni zakonitosti ravnanja organov. Glej na primer: zadevo Dias v Cleveland Police, [2017] UKIPTrib15_586-CH, v kateri se je sodišče, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal), sklicevalo na posamezne dele besedila kodeksa ravnanja glede uporabe komunikacijskih podatkov (Code of Practice on Communication Data), ko je ugotavljalo pomen razloga „preprečevanja ali odkrivanja kaznivih dejanj ali preprečevanja nemirov“, ki se uporablja za pridobivanje komunikacijskih podatkov. Kodeks je bil vključen v obrazložitev v zvezi z vprašanjem, ali je bil navedeni razlog pravilno uporabljen. Sodišče je nato ugotovilo, da je bilo sporno ravnanje nezakonito. Sodišča so ocenjevala tudi raven zaščitnih ukrepov, ki jih omogoča kodeks, glej na primer zadevo Just for Law Kids v Secretary of State for the Home Department [2019] EWHC 1772 (Admin), pri kateri je sodišče High Court ugotovilo, da primarna in sekundarna zakonodaja ter mednarodne smernice zagotavljajo zadostne zaščitne ukrepe, ali zadevo R (National Council for Civil Liberties) v Secretary of State for the Home Department & Others [2019] EWHC 2057 (Admin), pri kateri je ugotovilo, da zakon o preiskovalnih pooblastilih iz leta 2016 in kodeks ravnanja glede poseganja v opremo vsebujeta zadostne določbe glede tega, kako specifične morajo biti odredbe.

([268]) V zadevi Big Brother Watch je veliki senat Evropskega sodišča za človekove pravice ugotovil, da je „kodeks o prestrezanju komunikacij javni dokument, ki ga potrdita oba domova parlamenta in ki ga vlada objavi na spletu in v tiskani obliki ter ki ga morajo upoštevati osebe, ki opravljajo naloge prestrezanja, in sodišča (glej točki 93 in 94 zgoraj). Zato se Sodišče strinja, da bi se njegove določbe lahko upoštevale pri ocenjevanju predvidljivosti zakona o urejanju preiskovalnih pooblastil (glej zgoraj navedeno sodbo Kennedy, točka 157). V skladu s tem se Sodišče strinja, da je bilo notranje pravo ustrezno ‚dostopno‘.“ (Glej sodbo Evropskega sodišča za človekove pravice (veliki senat) v zadevi Big Brother Watch and others v United Kingdom, zadeve št. 58170/13, 62322/14 in 24960/15, z dne 25. maja 2021, točka 366).

([269]) Del 2 zakona o preiskovalnih pooblastilih iz leta 2016.

([270]) Del 3 zakona o preiskovalnih pooblastilih iz leta 2016.

([271]) Del 4 zakona o preiskovalnih pooblastilih iz leta 2016.

([272]) Del 5 zakona o preiskovalnih pooblastilih iz leta 2016.

([273]) Glede seznama zadevnih organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki lahko uporabljajo ciljna preiskovalna pooblastila na podlagi zakona o preiskovalnih pooblastilih iz leta 2016, glej opombo (139).

([274]) Člen 136 zakona o preiskovalnih pooblastilih iz leta 2016.

([275]) Člen 158 zakona o preiskovalnih pooblastilih iz leta 2016.

([276]) Člen 176 zakona o preiskovalnih pooblastilih iz leta 2016.

([277]) Člen 199 zakona o preiskovalnih pooblastilih iz leta 2016.

odobritve ali obvestila, razumno mogoče doseči z drugimi, manj intruzivnimi sredstvi; (ii) ali je raven varstva, ki se uporablja v zvezi s katerim koli pridobivanjem informacij na podlagi odredbe, odobritve ali obvestila, višja zaradi posebne občutljivosti navedenih informacij; (iii) javni interes v zvezi s celovitostjo in varnostjo telekomunikacijskih sistemov in poštnih storitev ter (iv) vse druge vidike javnega interesa v zvezi z varstvom zasebnosti ([278]).

(182) V zadevnem kodeksu ravnanja je podrobneje določeno, kako je treba uporabiti navedena merila in kako se ocenjuje zagotavljanje skladnosti z njimi, kot del odobritve uporabe takih pooblastil s strani pristojnega ministra in neodvisnega pravosodnega pooblaščenca (Judicial Commissioner). Natančneje, uporaba katerega koli od navedenih preiskovalnih pooblastil mora vedno biti „sorazmerna s ciljem, ki vključuje tehtanje stopnje posega v zasebnost (in druge preudarke iz člena 2(2)) na eni strani ter potrebe po izvedbi dejavnosti v preiskovalnem in operativnem smislu ter v smislu zmogljivosti na drugi strani“. To predvsem pomeni, da „bi morala obstajati realna možnost doseganja pričakovane koristi in da ne bi smela biti nesorazmerna ali samovoljna“ ter „da se noben poseg v zasebnost ne more šteti za sorazmernega, če bi bilo razumno mogoče iskane informacije pridobiti z manj intruzivnimi sredstvi“ ([279]). Natančneje, skladnost z načelom sorazmernosti je treba presojati glede na ta merila: „(i) obseg predlaganega posega v zasebnost v primerjavi s ciljem posega; (ii) kako in zakaj bodo uporabljene metode čim manj posegale v osebo in druge; (iii) ali dejavnost pomeni ustrezno uporabo zakona in ali je uporaba razumna, ob upoštevanju vseh razumnih drugih možnosti, kako doseči cilj; (iv) katere druge metode, kot je ustrezno, niso bile uporabljene ali so bile uporabljene, vendar so bile ocenjene kot nezadostne za dosego ciljev operacije, brez uporabe predlaganih preiskovalnih pooblastil“ ([280]).

(183) V skladu s pojasnili organov Združenega kraljestva v praksi to zagotavlja, da obveščevalna agencija najprej opredeli operativne cilje (s čimer opredeli zbiranje, npr. za namene boja proti mednarodnemu terorizmu na določenem geografskem območju), nato pa na podlagi teh operativnih ciljev določi, katera tehnična možnost (npr. ciljno prestrezanje ali prestrezanje v večjem obsegu, ciljni poseg v opremo ali poseg v opremo v večjem obsegu, ali ciljno pridobivanje komunikacijskih podatkov oziroma njihovo pridobivanje v večjem obsegu) je najustreznejša (npr. najmanj posega v zasebnost, v skladu s členom 2(2) zakona o preiskovalnih pooblastilih) glede na cilj in jo je torej mogoče odobriti na podlagi ene od razpoložljivih pravnih podlag.

(184) Pomembno je poudariti, da je tako sklicevanje na standarde potrebnosti in sorazmernosti omenil in pozdravil tudi posebni poročevalec Združenih narodov za pravico do zasebnosti, Joseph Cannataci, ki je glede sistema, vzpostavljenega z zakonom o preiskovalnih pooblastilih iz leta 2016, navedel, da „je videti, da postopki, vzpostavljeni pri obveščevalnih službah in agencijah za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, sistematično zahtevajo preverjanje potrebnosti in sorazmernosti obveščevalnega ukrepa ali operacije, preden se ta predlaga v odobritev, ter njeno preverjanje iz istih razlogov“ ([281]). Navedel je tudi, da mu je bilo na sestanku s predstavniki agencij za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter agencij za nacionalno varnost „soglasno predstavljeno mnenje, da je treba pri vseh odločitvah glede obveščevalnih ukrepov upoštevati pravico do zasebnosti. Vsi so razumeli in upoštevali potrebnost in sorazmernost kot glavni načeli, ki ju je treba upoštevati“.

([278]) Kodeks ravnanja glede prestrezanja komunikacij (Code of Practice on Interception of Communications) določa, da so drugi elementi preskusa sorazmernosti: „(i) obseg predlaganega posega v zasebnost v primerjavi s ciljem posega; (ii) kako in zakaj bodo uporabljene metode čim manj posegale v osebo in druge; (iii) ali dejavnost pomeni ustrezno uporabo zakona in ali je uporaba razumna, ob upoštevanju vseh razumnih drugih možnosti, kako doseči cilj; (iv) katere druge metode, kot je ustrezno, niso bile uporabljene ali so bile uporabljene, vendar so bile ocenjene kot nezadostne za dosego ciljev operacije, brez uporabe predlaganih preiskovalnih pooblastil“. Kodeks ravnanja glede prestrezanja komunikacij, točka 4.16, je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Glej kodeks ravnanja glede prestrezanja komunikacij, točki 4.12 in 4.15, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Glej kodeks ravnanja glede prestrezanja komunikacij, točka 4.16.

([281]) Zaključek izjave o opravljeni misiji posebnega poročevalca za pravico do zasebnosti ob zaključku njegove misije v Združenem kraljestvu Velika Britanija in Severna Irska, ki je na voljo na povezavi: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, točka 1.a.

(185) Posamezna merila za izdajo raznih odredb ter omejitve in zaščitni ukrepi iz zakona o preiskovalnih pooblastilih iz leta 2016 glede vsakega preiskovalnega pooblastila so podrobneje navedeni v uvodnih izjavah (186) do (243).

3.3.1.1.1 Ciljno prestrezanje in pregledovanje

(186) Obstajajo tri vrste odredb za ciljno prestrezanje: odredba o ciljnem prestrezanju ([282]), odredba o ciljnem pregledovanju in odredba na podlagi medsebojne pomoči ([283]). Pogoji za pridobitev takih odredb in relevantni zaščitni ukrepi so določeni v poglavju 1 dela 2 zakona o preiskovalnih pooblastilih iz leta 2016.

(187) Odredba o ciljnem prestrezanju omogoča prestrezanje komunikacij, navedenih v odredbi, med njihovim prenosom ter pridobivanje drugih podatkov, ki so pomembni za navedeno komunikacijo ([284]), vključno s sekundarnimi podatki ([285]). Odredba o ciljnem pregledovanju omogoča osebi, da med prestreženo vsebino, pridobljeno na podlagi odredbe o prestrezanju v večjem obsegu ([286]), izbere tisto, ki bo pregledana.

(188) Vsako odredbo na podlagi dela 2 zakona o preiskovalnih pooblastilih iz leta 2016 lahko izda pristojni minister ([287]), odobri pa jo pravosodni pooblaščenec ([288]). V vseh primerih je trajanje katere koli vrste ciljne odredbe omejeno na 6 mesecev ([289]), glede njene spremembe ([290]) ali podaljšanja ([291]) pa se uporabljajo posebna pravila.

(189) Pristojni minister mora pred izdajo odredbe izvesti oceno potrebnosti in sorazmernosti ([292]). Natančneje, glede odredbe o ciljnem prestrezanju in odredbe o ciljnem pregledovanju mora pristojni minister preveriti, ali je ukrep potreben iz enega od teh razlogov: za namene nacionalne varnosti; za preprečevanje ali odkrivanje hudih kaznivih dejanj ali v interesu gospodarske blaginje Združenega kraljestva ([293]), če je ta interes relevanten tudi za nacionalno varnost ([294]). Po drugi strani pa je odredbo na podlagi medsebojne pomoči (glej uvodno izjavo (139) above) mogoče izdati le, če pristojni minister meni, da obstajajo okoliščine, ki so enakovredne tistim, v katerih bi izdal odredbo za namene preprečevanja in/ali odkrivanja hudih kaznivih dejanj ([295]).

(190) Pristojni minister bi moral tudi oceniti, ali je ukrep sorazmeren s ciljem ([296]). Pri oceni sorazmernosti zahtevanih ukrepov je treba upoštevati splošne obveznosti glede zasebnosti iz člena 2(2) zakona o preiskovalnih pooblastilih iz leta 2016, predvsem, ali je cilj, ki se želi doseči z odredbo, odobritvijo ali obvestilom, mogoče razumno doseči

([282]) Člen 15(2) zakona o preiskovalnih pooblastilih iz leta 2016.
([283]) Člen 15(4) zakona o preiskovalnih pooblastilih iz leta 2016.
([284]) Člen 15(2) zakona o preiskovalnih pooblastilih iz leta 2016.
([285]) Sekundarni podatki so podatki, ki so priključeni prestreženi komunikaciji ali so z njo logično povezani, če jih je mogoče od nje logično ločiti in ob taki ločitvi ne razkrivajo ničesar, kar bi se razumno lahko štelo za (kakršen koli) pomen komunikacije. Med primeri sekundarnih podatkov so nastavitve usmerjevalnika ali požarnega zidu ali obdobje aktivnosti usmerjevalnika v omrežju, kadar so del prestrežene komunikacije, če so ji priključeni ali so z njo logično povezani. Več podrobnosti o tem vsebujeta opredelitev v členu 16 zakona o preiskovalnih pooblastilih iz leta 2016 in točka 2.19 kodeksa ravnanja glede prestrezanja komunikacij; opomba 278.
([286]) Ta pregled se izvaja kot izjema od člena 152(4) zakona o preiskovalnih pooblastilih iz leta 2016, ki določa prepoved poskusa identifikacije komunikacij posameznikov, ki so na Britanskem otočju. Glej uvodno izjavo (229).
([287]) Škotski minister odobri odredbo, kadar se ta nanaša na hudo kriminalno dejavnost na Škotskem (glej člena 21 in 22 zakona o preiskovalnih pooblastilih iz leta 2016); kadar je videti, da se bo prestrezanje nanašalo na osebo ali lokacijo zunaj Združenega kraljestva, lahko pristojni minister pooblasti višjega uslužbenca za izdajo odredbe na podlagi medsebojne pomoči (člen 40 zakona o preiskovalnih pooblastilih iz leta 2016).
([288]) Člena 19 in 23 zakona o preiskovalnih pooblastilih iz leta 2016.
([289]) Člen 32 zakona o preiskovalnih pooblastilih iz leta 2016.
([290]) Člen 39 zakona o preiskovalnih pooblastilih iz leta 2016. Nekatere osebe lahko na podlagi pogojev iz zakona o preiskovalnih pooblastilih iz leta 2016 omejeno spreminjajo odredbe. Oseba, ki je odredbo izdala, jo lahko kadar koli prekliče. To mora storiti, če odredba ni več potrebna iz katerega koli relevantnega razloga, ali če ravnanje, odobreno z odredbo, ni več sorazmerno s ciljem.
([291]) Člen 33 zakona o preiskovalnih pooblastilih iz leta 2016. Odločitev o podaljšanju odredbe mora odobriti pravosodni pooblaščenec.
([292]) Člen 19 zakona o preiskovalnih pooblastilih iz leta 2016.
([293]) Glede koncepta „interes gospodarske blaginje Združenega kraljestva, če je tak interes tudi pomemben za nacionalno varnost“, je veliki senat Evropskega sodišča za človekove pravice v točki 371 sodbe v zadevi Big Brother Watch and others v United Kingdom (glej opombo 268 zgoraj) navedel, da je ta pojem dovolj osredotočen na nacionalno varnost. Čeprav je bila ugotovitev Sodišča v tej zadevi povezana z uporabo tega koncepta v zakonu o urejanju preiskovalnih pooblastil iz leta 2000, se isti koncept uporablja tudi v zakonu o preiskovalnih pooblastilih iz leta 2016.
([294]) Člen 20(2) zakona o preiskovalnih pooblastilih iz leta 2016.
([295]) Člen 20(3) zakona o preiskovalnih pooblastilih iz leta 2016.
([296]) Člen 19(1)(b), (2)(b) in (3)(b) zakona o preiskovalnih pooblastilih iz leta 2016.

z drugimi manj intruzivnimi sredstvi in ali je raven varstva, ki se uporablja v zvezi s kakršnim koli pridobivanjem informacij na podlagi odredbe, višja zaradi posebno občutljive narave takih informacij (glej uvodno izjavo (181) above).

(191) Zato mora pristojni minister upoštevati vse elemente zahteve organa, zlasti tiste glede oseb, na katere se nanaša prestrezanje, in pomen ukrepa za preiskavo. Ti elementi so navedeni v kodeksu ravnanj glede prestrezanja komunikacij in morajo biti opisani z določeno mero natančnosti ([297]). Poleg tega člen 17 zakona o preiskovalnih pooblastilih iz leta 2016 določa, da mora biti v vsaki odredbi, izdani na podlagi poglavja 2 navedenega zakona, navedeno ime ali opis posamezne osebe ali skupine oseb, organizacije ali lokacije, na katero se nanaša prestrezanje (tako imenovana tarča). V primeru odredbe o ciljnem prestrezanju ali odredbe o ciljnem pregledovanju se to lahko nanaša tudi na skupino oseb, več kot eno osebo ali organizacijo ali več kot eno lokacijo (tudi tako imenovana tematska odredba) ([298]). V takih primerih mora biti v odredbi naveden namen ali dejavnost, ki je skupna skupini oseb ali operaciji/preiskavi, navedenih ali opisanih pa mora biti čim več takih oseb/organizacij ali lokacij, kot je razumno mogoče ([299]). Nazadnje, v vseh odredbah, izdanih na podlagi dela 2 zakona o preiskovalnih pooblastilih iz leta 2016, morajo biti navedeni naslovi, številke, oprema, dejavniki ali kombinacije dejavnikov, ki bodo uporabljeni za opredeljevanje komunikacij ([300]). V zvezi s tem kodeks ravnanja glede prestrezanja komunikacij določa, da je treba v primeru odredbe o ciljnem prestrezanju in odredbe o ciljnem pregledovanju „v odredbi opredeliti (ali opisati) dejavnike ali kombinacijo dejavnikov, ki bodo uporabljeni pri opredeljevanju komunikacij. Če bodo komunikacije (na primer) opredeljene glede na telefonsko številko, mora biti številka navedena v celoti. Kadar pa se bodo za opredeljevanje komunikacij uporabili zelo zapleteni ali stalno se spreminjajoči spletni izbirniki, je treba te opisati, kolikor je mogoče natančno“ ([301]).

(192) Pomemben zaščitni ukrep v tem smislu je, da mora oceno pristojnega ministra glede izdaje odredbe odobriti neodvisni pravosodni pooblaščenec ([302]), ki preverja predvsem, ali je odločitev o izdaji odredbe skladna z načeli potrebnosti in sorazmernosti ([303]) (glede statusa in vloge pravosodnih pooblaščencev glej uvodne izjave (251) do (256) below). Zakon o preiskovalnih pooblastilih iz leta 2016 tudi določa, da mora pravosodni pooblaščenec pri takem preverjanju uporabiti ista načela, kot bi jih sodišče na podlagi zahteve za sodno presojo ([304]). Na ta način se zagotavlja, da neodvisni organ sistematično preverja skladnost z načelom potrebnosti in sorazmernosti v vsakem primeru posebej in še preden se omogoči dostop do podatkov.

(193) Zakon o preiskovalnih pooblastilih iz leta 2016 določa nekaj posebnih in strogo opredeljenih izjem za izvajanje ciljnega prestrezanja brez odredbe. Omejeni primeri so podrobno opredeljeni v zakonu ([305]) in razen tistega, ki temelji na „soglasju“ pošiljatelja/prejemnika, jih izvajajo osebe (zasebni ali javni organi), ki niso nacionalne agencije za varnost. Poleg tega se ta vrsta prestrezanja izvaja za namene, ki se razlikujejo od zbiranja za namene obveščevalnih služb ([306]), in v nekaterih primerih je zelo malo verjetno, da bi se zbiranje lahko izvajalo v okviru prenosa (na primer v primeru prestrezanja v psihiatrični bolnišnici ali zaporu). Glede na naravo organa, na katerega

([297]) Zahtevane informacije vključujejo podatke o ozadju (opis oseb/organizacij/lokacij, komunikacij, ki se bodo prestrezale) in kako bo pridobitev teh podatkov koristila preiskavi, ter opis ravnanja, ki potrebuje odobritev. Če oseb/organizacij/lokacij ni mogoče opisati, je treba priložiti pojasnilo, zakaj to ni bilo mogoče oziroma zakaj je predložen le splošen opis (kodeks ravnanja glede prestrezanja komunikacij, točki 5.32 in 5.34, opomba 278).

([298]) Člen 17(2) zakona o preiskovalnih pooblastilih iz leta 2016. Glej tudi kodeks ravnanja glede prestrezanja komunikacij, točka 5.11 in naslednje, opomba 278.

([299]) Člen 31(4) in (5) zakona o preiskovalnih pooblastilih iz leta 2016.

([300]) Člen 31(8) zakona o preiskovalnih pooblastilih iz leta 2016.

([301]) Kodeks ravnanja glede prestrezanja komunikacij, točki 5.37 in 5.38, opomba 278.

([302]) Odobritev pravosodnega pooblaščenca ni potrebna, če pristojni minister meni, da je treba odredbo nujno izdati (člen 19(1) zakona o preiskovalnih pooblastilih). Vendar pa je treba pravosodnega pooblaščenca v kratkem obvestiti, saj mora odločiti o odobritvi odredbe. Če je ne odobri, odredba ne velja več (člena 24 in 25 zakona o preiskovalnih pooblastilih iz leta 2016).

([303]) Člen 23(1) zakona o preiskovalnih pooblastilih iz leta 2016.

([304]) Člen 23(2) zakona o preiskovalnih pooblastilih iz leta 2016.

([305]) Glej člene 44–51 zakona o preiskovalnih pooblastilih iz leta 2016 in člen 12 kodeksa ravnanja glede prestrezanja komunikacij (glej opombo 278).

([306]) To na primer velja, kadar je potrebno prestrezanje v zaporu ali psihiatrični bolnišnici, da se preveri ravnanje pridržane osebe ali pacienta, ali pri poštnem ali telekomunikacijskem operaterju, da se na primer odkrijejo neprimerne vsebine.

se ti posebni primeri nanašajo (razen agencij za nacionalno varnost), se bodo uporabljali vsi zaščitni ukrepi iz dela 2 zakona o varstvu podatkov iz leta 2018 in UK GDPR, vključno z nadzorom urada informacijskega pooblaščenca in razpoložljivimi mehanizmi pravnih sredstev. Poleg zaščitnih ukrepov, določenih v zakonu o varstvu podatkov iz leta 2018, v nekaterih primerih tudi zakon o preiskovalnih pooblastilih iz leta 2016 določa naknadni nadzor, ki ga izvaja urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil ([307]).

(194) Pri prestrezanju se uporabljajo dodatne omejitve in zaščitni ukrepi glede na specifičen status osebe, katere osebni podatki se prestrezajo ([308]). Prestrezanje komunikacij, za katere velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko, je na primer dovoljeno le v izrednih in prepričljivih okoliščinah, pri čemer mora oseba, ki izda odredbo, upoštevati javni interes v zvezi z zaupnostjo takih komunikacij, veljati pa morajo posebne zahteve glede ravnanja s takim gradivom, njegove hrambe in razkritja ([309]).

(195) Nadalje, zakon o preiskovalnih pooblastilih iz leta 2016 določa posebne zaščitne ukrepe v zvezi z varstvom, hrambo in razkritjem, ki jih mora pristojni minister upoštevati pred izdajo ciljne odredbe ([310]). Člen 53(5) zakona o preiskovalnih pooblastilih iz leta 2016 določa, da je treba vsako kopijo katerega koli gradiva, zbranega na podlagi odredbe, varno shraniti in uničiti, takoj ko ne obstajajo več upoštevni razlogi za njegovo hrambo; člen 53(2) navedenega zakona pa določa, da je treba osebe, ki se jim gradivo razkrije, da na voljo ali kopira, omejiti le na tiste, za katere je to iz zakonskih razlogov potrebno.

(196) Nazadnje, če je treba gradivo, prestreženo na podlagi odredbe o ciljnem prestrezanju ali odredbe na podlagi medsebojne pomoči, izročiti tretji državi („razkritje v tujino“), zakon o preiskovalnih pooblastilih iz leta 2016 določa, da mora pristojni minister zagotoviti ustrezne ukrepe, s katerimi se zagotovi, da v navedeni tretji državi veljajo podobni zaščitni ukrepi glede varstva, hrambe in razkritja ([311]). Poleg tega člen 109(2) zakona o varstvu podatkov iz leta 2018 določa, da lahko obveščevalne službe prenesejo osebne podatke z ozemlja Združenega kraljestva le, če je prenos nujen in sorazmeren ukrep, ki se izvede za namene zakonskih nalog upravljavca ali za drug namen iz člena 2(2)(a) zakona o varnostnih službah iz leta 1989 oziroma člena 2(2)(a) in 4(2)(a) zakona o obveščevalnih službah iz leta 1994 ([312]). Pomembno je, da se te zahteve uporabljajo tudi v primerih, ko se sklicuje na izjemo glede nacionalne varnosti v skladu s členom 110 zakona o varstvu podatkov iz leta 2018, saj v členu 110 zakona o varstvu podatkov iz leta 2018 ni naveden člen 109 zadevnega zakona kot ena od določb, ki se ne uporabijo, če je zaradi zaščite nacionalne varnosti potrebno izvzetje iz nekaterih določb.

3.3.1.1.2 Ciljno pridobivanje in hramba komunikacijskih podatkov

(197) Zakon o preiskovalnih pooblastilih iz leta 2016 pristojnemu ministru omogoča, da od telekomunikacijskih operaterjev zahteva hrambo komunikacijskih podatkov za namene ciljnega dostopa več javnih organov, vključno z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in obveščevalnimi agencijami. Del 4 zakona o preiskovalnih pooblastilih iz leta 2016 ureja hrambo komunikacijskih podatkov, del 3 pa ciljno pridobivanje komunikacijskih podatkov. Dela 3 in 4 zakona o preiskovalnih pooblastilih iz leta 2016 določata tudi posebne omejitve glede uporabe teh pooblastil in opredeljujeta posebne zaščitne ukrepe.

([307]) Glej, *a contrario*, člen 229(4) zakona o preiskovalnih pooblastilih.

([308]) Členi 26 do 29 zakona o preiskovalnih pooblastilih iz leta 2016 določajo omejitve glede pridobivanja odredb o ciljnem prestrezanju in ciljnem pregledovanju, ki se nanašajo na prestrezanje komunikacij, ki jih pošlje poslanec katerega koli parlamenta v Združenem kraljestvu oziroma ki so namenjene takemu poslancu, prestrezanje informacij, za katere velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko, prestrezanje komunikacij, za katere organ, ki bi jih prestregel, meni, da bodo vsebovale zaupno novinarsko gradivo, ali kadar je namen odredbe identifikacija ali potrditev vira novinarskih informacij.

([309]) Člen 26 zakona o preiskovalnih pooblastilih iz leta 2016.

([310]) Člen 19(1) zakona o preiskovalnih pooblastilih iz leta 2016.

([311]) Člen 54 zakona o preiskovalnih pooblastilih iz leta 2016. Zaščitni ukrepi v zvezi z razkritjem gradiva tujim organom so podrobneje opredeljeni v kodeksu ravnanja: glej zlasti odstavek 9.26 in naslednje in odstavek 9.87 kodeksa ravnanja glede prestrezanja komunikacij ter odstavke 9.33 in naslednje in odstavek 9.41 kodeksa ravnanja glede poseganja v opremo (glej opombo 278).

([312]) Ti nameni so: v primeru varnostne službe preprečevanje ali odkrivanje hudih kaznivih dejanj ali kateri koli kazenski postopek (člen 2(2)(a) zakona o varnostnih službah iz leta 1989), v primeru obveščevalne službe nacionalna varnost, preprečevanje ali odkrivanje hudih kaznivih dejanj ali kateri koli kazenski postopek (člen 2(2)(a) zakona o obveščevalnih službah iz leta 1994), v primeru službe GCHQ pa kateri koli kazenski postopek (člen 4(2)(a) zakona o obveščevalnih službah iz leta 1994). Glej tudi pojasnila o zakonu o varstvu podatkov iz leta 2018, ki so na voljo na naslednji povezavi: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Izraz „komunikacijski podatki“ se nanaša na elemente „kdo“, „kdaj“, „kje“ in „kako“, ne pa na vsebino, tj. ne na to, kaj je bilo rečeno ali napisano. Za razliko od prestrezanja, cilj pridobivanja in hrambe komunikacijskih podatkov ni pridobivanje vsebine komunikacij, ampak pridobivanje informacij, kot so, kdo je naročnik telefonske storitve, ali specifikacija računa. To lahko vključuje čas in trajanje komunikacije, številko ali elektronski naslov pošiljatelja ali prejemnika, včasih pa tudi lokacijo naprave, ki je bila uporabljena ([313]).

(199) Poudariti je treba, da se hramba in pridobivanje komunikacijskih podatkov običajno ne nanašata na osebne podatke posameznikov iz EU, na katere se nanašajo podatki, ki se prenašajo v Združeno kraljestvo na podlagi tega sklepa. Obveznost hrambe ali razkritja komunikacijskih podatkov na podlagi dela 3 in 4 zakona o preiskovalnih pooblastilih iz leta 2016 se nanaša na podatke, ki jih zbirajo telekomunikacijski operaterji v Združenem kraljestvu neposredno od uporabnikov telekomunikacijskih storitev ([314]). Te vrste obdelava, ki je usmerjena v stranke, običajno ne vključuje prenosov na podlagi tega sklepa, tj. prenosov od upravljavca/obdelovalca v EU k upravljavcu/obdelovalcu v Združenem kraljestvu.

(200) Vendar pa so zaradi celovitosti pogoji in zaščitni ukrepi, ki se uporabljajo za navedene ureditve pridobivanja in hrambe, analizirani v naslednjih uvodnih izjavah.

(201) Opozoriti je treba, da sta hramba in ciljno pridobivanje komunikacijskih podatkov na voljo tako agencijam za nacionalno varnost kot tudi nekaterim organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ([315]). Pogoji za zahtevo po hrambi in/ali pridobitvi komunikacijskih podatkov se lahko razlikujejo glede na razlog za zahtevo za ukrep, tj. zaradi nacionalne varnosti ali preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

(202) Medtem ko je nova ureditev uvedla splošno zahtevo po predhodni odobritvi s strani neodvisnega organa, ki se bo uporabljala v vseh primerih, ko se komunikacijski podatki hranijo in/ali pridobijo (za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali nacionalne varnosti), so bili po sodbi Sodišča v zadevi Tele2/Watson ([316]) uvedeni posebni zaščitni ukrepi, kadar se ukrep zahteva za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Kadar se hramba ali pridobitev komunikacijskih podatkov zahteva za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, mora predhodno dovoljenje vedno dati pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil. To ne velja vedno, kadar se ukrep zahteva za namene nacionalne varnosti, saj lahko, kot je opisano v nadaljevanju, tako vrsto ukrepov v nekaterih primerih odobri drug „posameznik, ki izda odobritev“. Poleg tega je nova ureditev prag, za katerega se lahko dovolita hramba in pridobivanje komunikacijskih podatkov, dvignila na „huda kazniva dejanja“ ([317]).

([313]) Komunikacijski podatki so opredeljeni v členu 261(5) zakona o preiskovalnih pooblastilih iz leta 2016. Komunikacijski podatki so razdeljeni v „podatke o dogodkih“ (vsi podatki, na podlagi katerih je mogoče opredeliti ali opisati dogodek, ne glede na to, ali se navede tudi lokacija ali ne, z uporabo telekomunikacijskega sistema, pri čemer dogodek pomeni enega ali več subjektov, ki sodelujejo pri določeni dejavnosti ob določenem času) ter „podatke o subjektu“ (vsi podatki, (a) ki se nanašajo na (i) subjekt, (ii) povezavo med telekomunikacijsko storitvijo in subjektom, ali (iii) povezavo med katerim koli delom telekomunikacijskega sistema in subjektom, (b) ki so sestavljeni iz podatkov ali vsebujejo podatke, na podlagi katerih je mogoče identificirati ali opisati subjekt (glede na njegovo lokacijo ali brez nje), in (c) pri katerih ne gre za podatke o dogodku).

([314]) To izhaja iz opredelitve komunikacijskih podatkov iz člena 261(5) zakona o preiskovalnih pooblastilih iz leta 2016, v skladu s katero komunikacijske podatke hrani ali pridobi telekomunikacijski operater, nanašajo pa se na uporabnika telekomunikacijske storitve in zagotavljanje te storitve ali pa so del komunikacije, vključeni vanjo, priloženi komunikaciji ali z njo logično povezani (glej tudi kodeks ravnanja glede komunikacijskih podatkov, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, točke 2.22 do 2.33). Opredelitev telekomunikacijskega operaterja iz člena 261(10) zakona o preiskovalnih pooblastilih iz leta 2016 tudi določa, da je telekomunikacijski operater oseba, ki ponuja ali zagotavlja telekomunikacijske storitve osebam v Združenem kraljestvu ali ki nadzoruje oziroma zagotavlja telekomunikacijski sistem, ki je (v celoti ali delno) v Združenem kraljestvu ali se nadzoruje iz Združenega kraljestva. Iz teh opredelitev jasno izhaja, da obveznosti iz zakona o preiskovalnih pooblastilih iz leta 2016 ni mogoče naložiti telekomunikacijskih operaterjem, ki nimajo opreme v Združenem kraljestvu ali ki svoje opreme ne nadzorujejo iz Združenega kraljestva, in ki ne ponujajo ali zagotavljajo storitev osebam v Združenem kraljestvu (glej tudi kodeks ravnanja glede komunikacijskih podatkov, točka 2.1). Če naročniki iz EU (ki so v EU ali v Združenem kraljestvu) uporabljajo storitve v Združenem kraljestvu, vse komunikacije v zvezi z zagotavljanjem te storitve zbira neposredno ponudnik storitve v Združenem kraljestvu in niso predmet prenosa iz EU.

([315]) Zadevni organi so navedeni v dodatku 4 k zakonu o preiskovalnih pooblastilih iz leta 2016, vključujejo pa policijo, obveščevalne službe, nekatera ministrstva in vladne službe, nacionalno agencijo za boj proti kriminalu, davčno in carinsko upravo, organ za konkurenco in trge, informacijskega pooblaščenca, službe za nujno medicinsko pomoč in gasilce ter druge organe, na primer na področju zdravja in varnosti hrane.

([316]) Sodba z dne 21. decembra 2016, Tele2 Sverige, združeni zadevi C-203/15 in C-698/15, EU:C:2016:970.

([317]) Za pridobitev komunikacijskih podatkov glej člen 61.7(b), za hrambo komunikacijskih podatkov pa člen 87.10A.

(i) *Pooblastilo za pridobitev komunikacijskih podatkov*

(203) V skladu z delom 3 zakona o preiskovalnih pooblastilih iz leta 2016 lahko zadevni javni organi pridobivajo komunikacijske podatke od telekomunikacijski operaterjev ali katere koli osebe, ki jih lahko pridobi in razkrije. Pooblastilo ne sme omogočati prestrezanja vsebine komunikacij ([318]) in preneha veljati po enem mesecu ([319]), lahko pa se podaljša na podlagi novega pooblastila ([320]). Za pridobitev komunikacijskih podatkov je potrebna odobritev pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil ([321]) (glede njegovega statusa in pooblastil glej uvodne izjave (250) do (251) below). To velja vedno, kadar za pridobitev komunikacijskih podatkov zaprosi relevantni organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Vendar pa člen 61 zakona o preiskovalnih pooblastilih iz leta 2016 določa, da kadar se podatki pridobivajo v interesu nacionalne varnosti ali gospodarske blaginje Združenega kraljestva, če je to relevantno za nacionalno varnost, ali če zahtevek predloži član obveščevalne agencije na podlagi člena 61(7)(b) ([322]), lahko pridobitev odobri tudi ([323]) pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil ali pooblaščeni višji uslužbenec ([324]). Pooblaščeni uslužbenec mora biti neodvisen od zadevne preiskave ter imeti ustrezno znanje o načelih in zakonodaji s področja človekovih pravic, zlasti o načelih potrebnosti in sorazmernosti ([325]). Odločitev pooblaščenega uslužbenca naknadno preveri pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil (več informacij o naknadnem nadzoru navedenega pooblaščenca je navedenih v uvodni izjavi (254) below v nadaljevanju).

(204) Pooblastilo za uporabo komunikacijskih podatkov temelji na oceni potrebnosti in sorazmernosti ukrepa. Natančneje, potrebnost ukrepa se ocenjuje glede na razloge, navedene v zakonodaji ([326]). Glede na ciljno naravo tega ukrepa mora biti ta potreben tudi za posamezno preiskavo ali operacijo ([327]). Več zahtev glede ocene potrebnosti ukrepov je navedenih v kodeksu ravnanja glede uporabe komunikacijskih podatkov ([328]). Navedeni kodeks določa zlasti, da morajo biti v vlogi, ki jo predloži organ prosilec, opredeljeni trije minimalni elementi za utemeljitev potrebnosti take zahteve: (i) preiskovani dogodek, na primer kaznivo dejanje ali lokacija ranljive pogrešane osebe; (ii) oseba, katere podatki se zahtevajo, na primer osumljenec, priča ali pogrešana oseba, ter kako je povezana z dogodkom, in (iii) zahtevani komunikacijski podatki, na primer telefonska številka ali naslov IP, ter kako se ti podatki nanašajo na osebo in dogodek ([329]).

(205) Pridobivanje komunikacijskih podatkov mora biti sorazmerno s ciljem ([330]). Kodeks ravnanja glede uporabe komunikacijskih podatkov pojasnjuje, da mora posameznik, ki izdaja odobritev, pri izvajanju take ocene uravnotežiti „intenzivnost posega v pravice in svoboščine posameznika ter specifično korist za preiskavo ali operacijo, ki jo v javnem interesu izvaja zadevni javni organ“ ter da ob upoštevanju vseh okoliščin posameznega primera „morda poseg v pravice posameznika kljub temu ni upravičen, ker bi bil škodljiv vpliv na pravice drugega

([318]) Člen 60A(6) zakona o preiskovalnih pooblastilih iz leta 2016.

([319]) To obdobje se skrajša na tri dni, kadar je odobritev izdana v nujnem primeru (člen 65(3)A zakona o preiskovalnih pooblastilih iz leta 2016).

([320]) V skladu s členom 65 zakona o preiskovalnih pooblastilih iz leta 2016 podaljšanje odobritve velja en mesec od datuma, ko predhodna odobritev poteče. Oseba, ki izda odobritev, jo lahko kadar koli prekliče, če meni, da zahteve niso več izpolnjene.

([321]) Člen 60A(1) zakona o preiskovalnih pooblastilih iz leta 2016. V imenu informacijskega pooblaščenca opravlja to funkcijo urad za izdajo dovoljenj za pridobivanje komunikacijskih podatkov (glej kodeks ravnanja glede uporabe komunikacijskih podatkov, odstavek 5.6).

([322]) Uporaba na podlagi člena 61(7)(b) zakona o preiskovalnih pooblastilih iz leta 2016 je namenjena „obravnavi kaznivih dejanj“, kar v skladu s členom 61(7)A navedenega zakona pomeni: „če gre pri komunikacijskih podatkih v celoti ali delno za podatke o dogodkih, za namene preprečevanja ali odkrivanja hudih kaznivih dejanj, v vseh drugih primerih pa za namene preprečevanja ali odkrivanja kaznivih dejanj ali preprečevanja nemirov“.

([323]) Kodeks ravnanja glede uporabe komunikacijskih podatkov določa, da „kadar je mogoče vlogo, ki se nanaša na nacionalno varnost, predložiti na podlagi člena 60A in člena 61, odločitev o tem, kateri način odobritve je v posameznem primeru ustreznejši, sprejme posamezni javni organ. Javni organi, ki želijo uporabiti način odobritve pooblaščenega višjega uslužbenca, morajo imeti vzpostavljene jasne smernice o tem, kdaj je ta način odobrite ustrezen (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 5.19, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) Člen 70(3) zakona o preiskovalnih pooblastilih iz leta 2016 vsebuje opredelitev pojma „pooblaščeni uslužbenec“, ki je odvisna od posameznega javnega organa (kot je določeno v dodatku 4 k zakonu o preiskovalnih pooblastilih iz leta 2016).

([325]) Dodatne podrobnosti o neodvisnosti imenovanega višjega uslužbenca so na voljo v kodeksu ravnanja glede uporabe komunikacijskih podatkov (odstavki 4.12–4.17, glej opombo 323).

([326]) Razlogi so: (i) nacionalna varnost; (ii) preprečevanje ali odkrivanje kaznivih dejanj ali preprečevanje nemirov (v primeru podatkov o dogodkih le v primeru hudih kaznivih dejanj); (iii) interes gospodarske blaginje Združenega kraljestva, če je navedeni interes tudi relevanten za nacionalno varnost; (iv) javna varnost; (v) za namene preprečevanja smrti ali poškodbe ali druge škode za telesno ali duševno zdravje osebe ali za zmanjšanje škodljivih posledic poškodbe ali škode za telesno ali duševno zdravje osebe; (vi) v pomoč pri preiskavah domnevnih nepravilnosti v postopku ali (vii) za identifikacijo mrtve osebe ali osebe, ki se iz določenih razlogov ne more sama identificirati (člen 61(7) zakona o preiskovalnih pooblastilih iz leta 2016).

([327]) Člen 60A(1)(b) zakona o preiskovalnih pooblastilih iz leta 2016.

([328]) Kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 3.3 in naslednje, opomba 323.

([329]) Kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 3.13, opomba 323.

([330]) Člen 60(1)(c) zakona o preiskovalnih pooblastilih iz leta 2016.

posameznika ali skupine posameznikov prevelik“. Za oceno sorazmernosti ukrepa kodeks navaja več elementov, ki jih mora organ prosilec navesti v svoji vlogi ([331]). Ob tem je treba posebno pozornost nameniti vrsti komunikacijskih podatkov, ki naj bi se pridobili (ali gre za podatke o subjektu ali za podatke o dogodku ([332])), prednost pa je treba dati uporabi manj intruzivnih vrst podatkov ([333]). Kodeks ravnanja glede uporabe komunikacijskih podatkov vsebuje tudi specifična navodila glede odobritev, ki vključujejo komunikacijske podatke oseb v določenih poklicih (na primer zdravnikov, odvetnikov, novinarjev, poslancev ali duhovnikov) ([334]), za katere veljajo dodatni zaščitni ukrepi ([335]).

(ii) *Obvestilo o hrambi komunikacijskih podatkov*

(206) Del 4 zakona o preiskovalnih pooblastilih iz leta 2016 določa pravila o hrambi komunikacijskih podatkov in merila, na podlagi katerih lahko pristojni minister izda obvestilo o hrambi ([336]). Zaščitni ukrepi iz zakona o preiskovalnih pooblastilih so enaki, če se podatki hranijo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali če se uporabljajo za namene nacionalne varnosti.

(207) Namen izdaje takih obvestil o hrambi podatkov je zagotoviti, da telekomunikacijski operaterji za največ 12 mesecev hranijo relevantne komunikacijske podatke, ki bi bili drugače izbrisani, ko ne bi bili več potrebni za poslovne namene ([337]). Hranjeni podatki morajo ostati na voljo v zahtevanem obdobju, če bi jih javni organ morda pozneje potreboval na podlagi odobritve ciljne pridobitve komunikacijskih podatkov iz dela 3 zakona o preiskovalnih pooblastilih iz leta 2016, kot je opisano v uvodnih izjavah (203) do (205).

(208) Za izvajanje pooblastila, da se zahteva hramba nekaterih podatkov, veljajo številne omejitve in zaščitni ukrepi. Pristojni minister lahko izda obvestilo o hrambi podatkov enemu ali več operaterjem ([338]) samo, če meni, da je zahteva po hrambi podatkov nujna za enega od zakonskih namenov ([339]) in sorazmerna s tem, kar se želi doseči ([340]). Kot je pojasnjeno v zakonu o preiskovalnih pooblastilih iz

([331]) Informacije, ki jih je treba vključiti, so: (i) razlaga, kako bo pridobitev podatkov koristila preiskavi ali operaciji; (ii) pojasnilo zahtevanega obdobja, vključno s tem, zakaj je navedeno obdobje sorazmerno z dogodkom, ki se preiskuje; (iii) utemeljitev stopnje posega, ob upoštevanju koristi podatkov za preiskavo (taka utemeljitev mora vključevati premislek, ali bi za dosego ciljev zadoščala manj intruzivna preiskava); (iv) premislek o pravicah posameznika (zlasti pravice do zasebnosti in v zadevnih primerih svobode izražanja) ter uravnoteženje pravic in koristi preiskave; (v) podatki o morebitnih postranskih posegih in kako zahtevano časovno obdobje vpliva na postranske posege (kodeks ravnanja glede uporabe komunikacijskih podatkov, točke 3.22 do 3.26, opomba 323).

([332]) Glej opombo 313.

([333]) Kodeks določa, da je v primerih, ko se zahteva dostop do komunikacijskih podatkov, ki bolj posega v pravice posameznika (na primer v podatke o dogodkih), ustrezneje najprej pridobiti podatke o subjektih, podatke o dogodku pa neposredno pridobiti le v omejenih, posebno nujnih primerih (kodeks ravnanja glede uporabe komunikacijskih podatkov, točke 6.10 do 6.14, opomba 323).

([334]) Kodeks ravnanja glede uporabe komunikacijskih podatkov, točke 8.8 do 8.44, opomba 323.

([335]) Kodeks ravnanja določa, da „mora posameznik, ki izda odobritev, take vloge skrbno proučiti, vključno s premislekom o tem, ali lahko pride do nenačrtovanih posledic takih vlog ter ali so vloge v korist javnosti“ (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 8.8). Nadalje, glede te vrste vlog je treba voditi evidenco, ob naslednjem pregledu pa jih predložiti v pregled pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 8.10, opomba 323).

([336]) Členi 87 do 89 zakona o preiskovalnih pooblastilih iz leta 2016.

([337]) Na podlagi člena 90 zakona o preiskovalnih pooblastilih iz leta 2016 lahko telekomunikacijski operater, ki mu je izdano obvestilo o hrambi podatkov, zahteva, da pristojni minister, ki ga je izdal, obvestilo še enkrat prouči.

([338]) V skladu s členom 87(2)(a) zakona o preiskovalnih pooblastilih iz leta 2016 se lahko obvestilo o hrambi nanaša na „posameznega operaterja ali kakršen koli opis operaterjev“.

([339]) Razlogi so: (i) nacionalna varnost; (ii) zadevni namen v zvezi s kaznivimi dejanji (kot je opredeljeno v členu 87.10A zakona o preiskovalnih pooblastilih iz leta 2016); (iii) interes gospodarske blaginje Združenega kraljestva, če je navedeni interes tudi relevanten za nacionalno varnost; (iv) javna varnost; (v) preprečevanje smrti ali poškodbe ali druge škode za telesno ali duševno zdravje osebe ali zmanjšanje škodljivih posledic poškodbe ali škode za telesno ali duševno zdravje osebe ali (vi) pomoč pri preiskavi domnevnih nepravilnosti v postopku (člen 87 zakona o preiskovalnih pooblastilih).

([340]) Člen 87 zakona o preiskovalnih pooblastilih iz leta 2016. Nadalje, v skladu z zadevnim kodeksom ravnanja se pri ocenjevanju sorazmernosti obvestila o hrambi podatkov uporabljajo merila iz člena 2(2) zakona o preiskovalnih pooblastilih iz leta 2016, predvsem zahteva, da se oceni, ali bi bilo razumno mogoče cilje obvestila doseči z manj intruzivnimi sredstvi. Podobno kot glede ocene sorazmernosti pridobivanja komunikacijskih podatkov kodeks ravnanja glede uporabe komunikacijskih podatkov pojasnjuje, da taka ocena vključuje „uravnoteženje intenzivnosti posega v pravico posameznika do spoštovanja njegovega zasebnega življenja in specifične koristi za preiskavo“ (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 16.3, opomba 323).

leta 2016 ([341]), mora pristojni minister v ta namen pred izdajo obvestila o hrambi podatkov upoštevati: predvidene koristi obvestila ([342]); opis telekomunikacijskih storitev; ustreznost omejevanja podatkov, ki naj se shranijo, glede na lokacijo ali opise oseb, ki se jim zagotavljajo telekomunikacijske storitve ([343]); predvideno število uporabnikov katere koli telekomunikacijske storitve, na katero se nanaša obvestilo (če je znano) ([344]); tehnično izvedljivost izvršitve obvestila; predvidene stroške izvršitve obvestila in vse druge učinke obvestila na telekomunikacijskega operaterja (ali opis operaterjev), na katerega se nanaša ([345]). Kot je podrobneje pojasnjeno v poglavju 17 kodeksa ravnanja glede uporabe komunikacijskih podatkov, morajo biti v vseh obvestilih o hrambi podatkov opredeljene vse vrste podatkov, ki naj se shranijo, in pojasnjeno mora biti, zakaj jih je treba shraniti.

(209) V vseh primerih (za namene nacionalne varnosti ter namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj) mora odločitev pristojnega ministra, da izda obvestilo o hrambi, odobriti neodvisni pravosodni pooblaščenec v okviru tako imenovanega „postopka z dvojnim varovalom“; ta mora zlasti preveriti, ali je obvestilo o hrambi zadevnih komunikacijskih podatkov potrebno in sorazmerno za enega ali več zakonskih namenov ([346]).

3.3.1.1.3 Poseganje v opremo

(210) Poseganje v opremo vključuje več tehnik, ki se uporabljajo za pridobivanje raznih podatkov iz opreme ([347]), na primer z računalnika, tablice in pametnega telefona ter s kablov, žic in naprav za shranjevanje ([348]). Poseganje v opremo omogoča pridobivanje vsebine komunikacij in podatkov o opremi ([349]).

(211) V skladu s členom 13(1) zakona o preiskovalnih pooblastilih iz leta 2016 mora obveščevalna služba za poseg v opremo pridobiti odobritev v obliki odredbe na podlagi postopka z dvojnim varovalom iz zakona o preiskovalnih pooblastilih iz leta 2016, če obstaja „povezava z Britanskim otočjem“ ([350]). Iz pojasnil organov Združenega kraljestva

([341]) Glej člen 88 zakona o preiskovalnih pooblastilih iz leta 2016.

([342]) Koristi so lahko obstoječe ali predvidene, morajo pa upoštevati zakoniti namen, za katerega se podatki lahko hranijo (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 17.17, opomba 323).

([343]) To vključuje presojo, ali je celoten geografski doseg obvestila o hrambi podatkov potreben in sorazmeren ter ali je potrebno in sorazmerno vključiti oziroma izključiti posamezne opise oseb (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 17.17, opomba 323).

([344]) To je pristojnemu ministru v pomoč pri presoji intenzivnosti posega v pravice strank ter potencialne koristi shranjenih podatkov (kodeks ravnanja glede uporabe komunikacijskih podatkov, točka 17.17, opomba 323).

([345]) Člen 88 zakona o preiskovalnih pooblastilih iz leta 2016.

([346]) Člen 89 zakona o preiskovalnih pooblastilih iz leta 2016.

([347]) Na podlagi člena 135(1) in člena 198(1) zakona o preiskovalnih pooblastilih iz leta 2016 „oprema“ pomeni opremo, ki ustvarja elektromagnetne, akustične ali druge emisije, ter vsako napravo, ki jo je mogoče uporabiti v zvezi s tako opremo.

([348]) Kodeks ravnanja glede poseganja v opremo je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, točka 2.2.

([349]) Podatki o opremi so opredeljeni v členu 100 zakona o varstvu podatkov iz leta 2016, in sicer kot sistemski podatki in podatki, ki (a) so del komunikacije, vključeni vanjo, priloženi komunikaciji ali z njo logično povezani (prek pošiljatelja ali kako drugače), ali kateri koli drug del informacije; (b) jih je mogoče logično ločiti od preostale komunikacije ali dela informacije in (c) se ob taki ločitvi z njimi ne bi razkrilo nič, kar bi se razumno lahko štelo za (kateri koli) pomen komunikacije ali dela informacije.

([350]) Člen 13(1) zakona o preiskovalnih pooblastilih iz leta 2016 določa, da je odredba obvezna, kadar ravnanje obveščevalne službe pomeni enega ali več kaznivih dejanj na podlagi členov 1 do 3A zakona o zlorabi računalnikov iz leta 1990 (Computer Misuse Act 1990), kar se zgodi v veliki večini okoliščin, glej kodeks ravnanja glede poseganja v opremo, točke 3.32 in 3.6 do 3.9. V skladu s členom 13(2) zakona o preiskovalnih pooblastilih iz leta 2016 obstaja „povezava z Britanskim otočjem“, če (a) kateri koli del ravnanja poteka na Britanskem otočju (ne glede na lokacijo opreme, v katero se ali bi se lahko posegalo), (b) obveščevalna služba meni, da je ali bi lahko bil kateri koli del opreme, v katero se ali bi se lahko posegalo, med poseganjem na Britanskem otočju, ali (c) je namen poseganja pridobiti (i) komunikacijo, ki jo pošlje ali prejme oseba, ki je v takem trenutku na Britanskem otočju ali za katero obveščevalna služba domneva, da je na Britanskem otočju, (ii) zasebne informacije, ki se nanašajo na posameznika, ki je v takem trenutku na Britanskem otočju ali za katerega obveščevalna služba domneva, da je na Britanskem otočju, ali (iii) podatke o opremi, ki so del komunikacije ali zasebnih informacij iz pododstavka (i) ali (ii) oziroma so povezani z njimi.

izhaja, da kadar se podatki prenašajo iz Evropske unije v Združeno kraljestvo v okviru tega sklepa, vedno obstaja „povezava z Britanskim otočjem“, zato je treba za vsak poseg v opremo, ki se nanaša na take podatke, pridobiti obvezno odredbo v skladu s členom 13(1) zakona o preiskovalnih pooblastilih iz leta 2016 ([351]).

(212) Pravila glede odredb o ciljnem poseganju v opremo so določena v delu 5 zakona o preiskovalnih pooblastilih iz leta 2016. Podobno kot ciljno prestrezanje se mora tudi ciljno poseganje v opremo nanašati na specifično „tarčo“, ki jo je treba v odredbi opredeliti ([352]). Opredelitev „tarče“ je odvisna od zadeve in vrste opreme, v katero se posega. Zlasti člen 115(3) zakona o preiskovalnih pooblastilih določa elemente, ki jih je treba vključiti v odredbo (na primer ime osebe ali organizacije, opis lokacije), odvisno na primer od tega, ali se poseg nanaša na opremo, ki pripada določeni osebi ali organizaciji ali skupini oseb, ali na opremo, ki jo taka oseba, organizacija ali skupina uporablja ali jo ima v posesti, ter ali je taka oprema na zadevni lokaciji itd. ([353]). Nameni, za katere se lahko izda odredba o ciljnem poseganju v opremo, so odvisni od javnega organa, ki zanjo zaprosi ([354]).

(213) Tako kot pri ciljnem prestrezanju mora organ izdajatelj proučiti, ali je ukrep potreben za doseganje specifičnega namena in ali je sorazmeren s ciljem ([355]). Proučiti mora tudi, ali obstajajo zaščitni ukrepi glede varstva, hrambe in razkritja ter glede „razkritja v tujino“ ([356]) (glej uvodno izjavo (196)).

(214) Odredbo mora odobriti pravosodni pooblaščenec, razen če gre za nujno zadevo ([357]). V slednjem primeru je treba pravosodnega pooblaščenca obvestiti o izdaji odredbe, ta pa jo mora nato v treh delovnih dneh odobriti. Če pravosodni pooblaščenec odobritev zavrne, odredba ne učinkuje več in je ni mogoče podaljšati ([358]). Poleg tega lahko pravosodni pooblaščenec zahteva, da se vsi podatki, pridobljeni na podlagi odredbe, izbrišejo ([359]). Dejstvo, da je bila odredba izdana nujno, ne vpliva na naknadni nadzor (glej uvodne izjave (244) do (255)) ali na možnosti posameznikov, da vložijo pravno sredstvo (glej uvodne izjave (260) do (270)). Posamezniki se lahko v zvezi s kakršnim koli domnevnim ravnanjem na običajen način pritožijo pri uradu informacijskega pooblaščenca ali vložijo zahtevek pri sodišču, ki obravnava preiskovalna pooblastila. V vseh primerih je preskus, ki ga pravosodni pooblaščenec uporablja pri odločanju, ali se odredba odobri, preskus potrebnosti in sorazmernosti, kot se uporablja za zahtevke za ciljno prestrezanje ([360]) (glej uvodno izjavo (192) above).

([351]) Zaradi celovitosti je treba poudariti, da tudi kadar ne obstaja „povezava z Britanskim otočjem“ in za poseganje v opremo ni potrebna obvezna odredba na podlagi člena 13(1) zakona o preiskovalnih pooblastilih iz leta 2016, mora obveščevalna služba, ki namerava izvajati dejavnost, pri kateri lahko pridobi odredbo o poseganju v opremo v večjem obsegu, tako odredbo tudi pridobiti (glej kodeks ravnanja glede poseganja v opremo, točka 3.24). Tudi kadar odredba o poseganju v opremo na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 ni zakonsko potrebna ali se praviloma ne zahteva, za ravnanje obveščevalnih služb velja več pogojev in omejitev na podlagi člena 7 zakona o obveščevalnih službah iz leta 1994. To vključuje predvsem zahtevo po odobritvi pristojnega ministra, ki se mora prepričati, da noben ukrep ne presega tistega, kar je potrebno za ustrezno opravljanje nalog obveščevalne službe.

([352]) Člen 115 zakona o preiskovalnih pooblastilih iz leta 2016 ureja vsebino odredbe in določa, da mora vsebovati ime ali opis oseb, organizacij, lokacijo ali skupino oseb, ki se šteje za „tarčo“, opis narave preiskave ter opis dejavnosti, za katere se oprema uporablja. Opisati je treba tudi vrsto opreme in ravnanje, ki ga mora opraviti oseba, ki se ji odredba izda.

([353]) Glej tudi kodeks ravnanja glede poseganja v opremo, točka 5.7, opomba 348.

([354]) Agencije za nacionalno varnost lahko zaprosijo za izdajo odredbe za poseganje v opremo, kadar je to potrebno za namene nacionalne varnosti, za namene odkrivanja hudih kaznivih dejanj in/ali v interesu gospodarske blaginje Združenega kraljestva, če je tak interes tudi pomemben za nacionalno varnost (člena 102 in 103 zakona o preiskovalnih pooblastilih iz leta 2016). Odvisno od agencije je mogoče za odredbo o poseganju v opremo zaprositi za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če je to potrebno za odkrivanje ali preprečevanje hudih kaznivih dejanj ali za namene preprečevanja smrti ali kakršne koli poškodbe ali škode za telesno ali duševno zdravje osebe ali za zmanjšanje poškodbe ali škode za telesno ali duševno zdravje osebe (glej člen 106(1) in (3) zakona o varstvu podatkov iz leta 2016).

([355]) Člen 102(1) zakona o preiskovalnih pooblastilih iz leta 2016.

([356]) Členi 129 do 131 zakona o preiskovalnih pooblastilih iz leta 2016.

([357]) Člen 109 zakona o preiskovalnih pooblastilih iz leta 2016.

([358]) Člen 109(4) zakona o preiskovalnih pooblastilih iz leta 2016.

([359]) Člen 110(3)(b) zakona o preiskovalnih pooblastilih iz leta 2016. V skladu s točko 5.67 kodeksa ravnanja glede poseganja v opremo se nujnost določi glede na to, ali bi bilo v času, ki je na voljo za izpolnitev operativnih ali preiskovalnih potreb, smiselno zaprositi za soglasje pravosodnega pooblaščenca za izdajo odredbe. Nujne odredbe bi morale spadati v eno ali obe od naslednjih kategorij: (i) neposredno ogrožanje življenja ali resna škoda – na primer, če je bila oseba ugrabljena in se ocenjuje, da je njeno življenje v neposredni nevarnosti, ali (ii) zbiranje obveščevalnih podatkov ali možnost za preiskavo z omejenim časom za ukrepanje – na primer, v Združeno kraljestvo bo kmalu vstopila pošiljka drog razreda A in organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj hočejo podatke o storilcih, da bi lahko izvedli aretacije. Glej opombo 348.

([360]) Člen 108 zakona o preiskovalnih pooblastilih iz leta 2016.

(215) Nazadnje, posebni zaščitni ukrepi, ki se uporabljajo glede ciljnega prestrezanja, se uporabljajo tudi glede poseganja v opremo, na primer glede trajanja, podaljševanja in spremembe odredbe ter glede prestrezanja podatkov poslancev, podatkov, za katere velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko, in prestrezanje novinarskega gradiva (več o tem je navedeno v uvodni izjavi 193).

3.3.1.1.4 Izvrševanje pooblastil v večjem obsegu

(216) Izvrševanje pooblastil v večjem obsegu je urejeno v delu 6 zakona o preiskovalnih pooblastilih iz leta 2016. Ob tem kodeks ravnanja vsebuje več podrobnosti o uporabi pooblastil v večjem obsegu. Čeprav v zakonodaji Združenega kraljestva ni opredelitve pojma „pooblastila v večjem obsegu“, je ta pojem v okviru zakona o preiskovalnih pooblastilih iz leta 2016 opisan kot zbiranje in hramba večjih količin podatkov, ki jih vlada pridobi na različne načine (na primer pooblastilo za prestrezanje v večjem obsegu, pridobivanje v večjem obsegu, poseganje v opremo v večjem obsegu in nabori osebnih podatkov v večjem obsegu), do katerih imajo organi posledično dostop. Ta opis je natančneje opredeljen z naštevanjem, kaj pooblastila v večjem obsegu niso; ne gre na primer za množičen nadzor brez omejitev ali zaščitnih ukrepov. Nasprotno, kot je pojasnjeno v nadaljevanju, veljajo omejitve in zaščitni ukrepi, vzpostavljeni z namenom, da se prepreči nekritičen ali neupravičen dostop do podatkov ([361]). Pooblastila v večjem obsegu je mogoče uporabiti le, če je vzpostavljena povezava med tehničnim ukrepom, ki ga namerava uporabiti nacionalna obveščevalna agencija, in operativnim ciljem, za katerega se tak ukrep zahteva.

(217) Nadalje, pooblastila v večjem obsegu so na voljo le obveščevalnim agencijam in zanje je vedno potrebna odredba pristojnega ministra ter odobritev pravosodnega pooblaščenca. Pri izbiri načina zbiranja podatkov je treba proučiti, ali je mogoče zadevni cilj doseči z „manj intruzivnimi sredstvi“ ([362]). Ta pristop izhaja iz zakonodajnega okvira, ki temelji na načelu sorazmernosti in zato daje prednost ciljnemu zbiranju pred zbiranjem v večjem obsegu.

3.3.1.1.4.1 Prestrezanje v večjem obsegu in poseganje v opremo v večjem obsegu

(218) Prestrezanje v večjem obsegu je urejeno v poglavju 1 dela 6 zakona o varstvu podatkov iz leta 2016, poglavje 3 istega dela pa ureja poseganje v opremo v večjem obsegu. Navedeni ureditvi sta vsebinsko enaki, zato so pogoji in dodatni zaščitni ukrepi, ki se uporabljajo glede takih odredb, analizirani skupaj.

(i) *Pogoji in merila za izdajo odredbe*

(219) Odredba o prestrezanju v večjem obsegu je omejena na prestrezanje komunikacij med njihovim prenosom, kadar jih pošlje ali prejme posameznik, ki ni na Britanskem otočju ([363]) (tako imenovana „komunikacija, povezana s tujino“ ([364])), ter drugih zadevnih podatkov, vključuje pa tudi nadaljnjo izbiro za pregled

([361]) Iz poročila o pooblastilih v večjem obsegu, ki ga je pred odobritvijo zakona o preiskovalnih pooblastilih iz leta 2016 pripravil Lord David Anderson, neodvisni pregledovalec zakonodaje o terorizmu, izhaja, da „je treba jasno navesti, da zbiranje in hramba podatkov v večjem obsegu ne pomeni tako imenovanega ‚množičnega nadzora‘. Vsak pravni sistem, ki je vreden tega naziva, bo vključil omejitve in zaščitne ukrepe, ki so namenjeni temu, da se prepreči neselektiven ali neupravičen dostop do shranjenih občutljivih podatkov. Take omejitve so v predlog zakona nedvomno vključene.“ Lord David Anderson, Report of the bulk power review, avgust 2016, točka 1.9 (poudarek dodan), na voljo na naslednji povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) Člen 2.2 zakona o preiskovalnih pooblastilih iz leta 2016. Glej na primer kodeks ravnanja glede pridobivanja komunikacijskih podatkov v večjem obsegu, točka 4.11, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) Izraz „Britansko otočje“ pomeni Združeno kraljestvo, Kanalske otoke in Otok Man, opredeljen pa je v dodatku 1 k zakonu o razlagi iz leta 1978 (Interpretation Act 1978), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) V skladu s členom 136 zakona o preiskovalnih pooblastilih iz leta 2016 izraz „komunikacija, povezana s tujino“ pomeni: (i) komunikacijo, ki jo pošljejo posamezniki, ki so zunaj Britanskega otočja, ali (ii) komunikacijo, ki jo prejmejo posamezniki, ki so zunaj Britanskega otočja. Kot so potrdili organi Združenega kraljestva, ta ureditev vključuje tudi komunikacijo med dvema osebama, ki sta obe zunaj Britanskega otočja. Veliki senat Evropskega sodišča za človekove pravice je v točki 376 sodbe v zadevi Big Brother Watch and others v United Kingdom (glej opombo 279 zgoraj) za podobno omejitev (v zvezi z „zunanjimi komunikacijami“) komunikacij, ki jih je mogoče v skladu z zakonom o urejanju preiskovalnih pooblastil iz leta 2000 zajeti s prestrezanjem v večjem obsegu, navedel, da je dovolj omejena in predvidljiva.

prestreženega gradiva ([365]). Odredba o poseganju v opremo v večjem obsegu ([366]) naslovniku omogoča poseg v katero koli opremo za namene pridobivanja komunikacij, povezanih s tujino (vključno z vsem, kar je sestavljeno iz govora, glasbe, zvokov, vizualnih podob ali katerih koli podatkov), podatkov o opremi (podatkov, ki omogočajo ali lajšajo izvajanje poštnih storitev, telekomunikacijskega sistema, telekomunikacijskih storitev) ali katerih koli drugih informacij ([367]).

(220) Pristojni minister lahko odredbo o ukrepih v večjem obsegu izda le na podlagi vloge vodje obveščevalne službe ([368]). Odredba o odobritvi prestrezanja v večjem obsegu ali poseganja v opremo v večjem obsegu se lahko izda le, če je to potrebno za nacionalno varnost ter za namen preprečevanja ali odkrivanja hudih kaznivih dejanj, ali v interesu gospodarske blaginje Združenega kraljestva, če je to pomembno za nacionalno varnost ([369]). Člen 142(7) zakona o preiskovalnih pooblastilih iz leta 2016 določa še, da mora biti odredba o prestrezanju v večjem obsegu natančno opredeljena in da ne zadošča zgolj sklicevanje na „interese nacionalne varnosti“, „ekonomsko blaginjo Združenega kraljestva“ ter „preprečevanje hudih kaznivih dejanj in boj zoper njih“, temveč mora biti vzpostavljena povezava med zahtevanim ukrepom in enim ali več operativnimi nameni, ki jih je treba vključiti v odredbo.

(221) Izbira operativnega namena je rezultat večplastnega postopka. Člen 142(4) določa, da morajo biti operativni nameni, ki so opredeljeni v odredbi, opredeljeni tudi v seznamu operativnih namenov, ki ga vodijo vodje obveščevalnih služb in za katere menijo, da so lahko podlaga za izbiro prestrežene vsebine ali sekundarnih podatkov, pridobljenih na podlagi odredbe o prestrezanju v večjem obsegu, ki se nato pregledajo. Seznam operativnih namenov mora odobriti pristojni minister. Ta lahko tako odobritev izda le, če se prepriča, da je operativni namen opredeljen podrobneje kot le na podlagi splošnih razlogov za odobritev odredbe (nacionalna varnost ali nacionalna varnost in gospodarska blaginja ali preprečevanje hudih kaznivih dejanj) ([370]). Ob koncu vsakega zadevnega trimesečnega obdobja mora pristojni minister predložiti kopijo seznama operativnih namenov parlamentarnemu odboru za obveščevalno in varnostno dejavnost. Nazadnje, predsednik vlade mora vsaj enkrat letno preveriti seznam operativnih namenov ([371]). Kot je navedlo sodišče High Court, „teh ne gre podcenjevati kot nepomembnih zaščitnih ukrepov, saj sestavljajo zapleteno mrežo odgovornosti, ki vključuje parlament in najvišje člane vlade“ ([372]).

(222) Taki operativni nameni tudi omejujejo obseg izbire prestreženega gradiva za pregled. Izbira gradiva za pregled, zbranega na podlagi odredbe o ukrepih v večjem obsegu, mora biti utemeljena glede na operativne namene. Kot so pojasnili organi Združenega kraljestva to pomeni, da mora pristojni minister oceniti praktično ureditev pregleda že ob izdaji odredbe, ko je treba navesti dovolj podrobnosti, da se izpolnijo zakonske obveznosti iz členov 152 in 193 zakona o preiskovalnih pooblastilih iz leta 2016 ([373]). Podrobnosti, ki se v zvezi s tako ureditvijo predložijo pristojnemu ministru, morajo vključevati na primer informacije o tem, kako se bo ureditev filtriranja morda spreminjala v času veljavnosti odredbe (če je ustrezno) ([374]). Več informacij o postopku in zaščitnih ukrepih, ki se uporabljajo v fazi filtriranja in pregleda, je na voljo v uvodni izjavi (229) below v nadaljevanju.

([365]) Člen 136(4) zakona o preiskovalnih pooblastilih iz leta 2016. V skladu s pojasnili vlade Združenega kraljestva se lahko prestrezanje v večjem obsegu uporabi na primer za identifikacijo predhodno neznanih groženj nacionalni varnosti Združenega kraljestva s filtriranjem in analizo prestreženega gradiva, da se identificira komunikacija z obveščevalno vrednostjo (UK Explanatory Framework section H: National security, str. 27 in 28, opomba 29). Kot so pojasnili organi Združenega kraljestva, je take instrumente mogoče uporabiti za vzpostavljanje povezav med znanimi sumljivimi subjekti ter za iskanje sledov dejavnosti posameznikov, ki morda še niso znani, vendar se pojavijo med preiskavo, ter za prepoznavanje vzorcev dejavnosti, ki lahko pomenijo grožnjo Združenemu kraljestvu.

([366]) V skladu s členom 13(1) zakona o preiskovalnih pooblastilih iz leta 2016 mora obveščevalna služba za poseganje v opremo pridobiti odobritev v obliki odredbe na podlagi navedenega zakona, če obstaja „povezava z Britanskim otočjem“, glej uvodno izjavo (211).

([367]) Člen 176 zakona o preiskovalnih pooblastilih iz leta 2016. Z odredbo o poseganju v opremo v večjem obsegu se ne sme odobriti ravnanja, ki bi pomenilo nezakonito prestrezanje (razen če je izvedeno z zakonitimi pooblastili; izjema je shranjena komunikacija). Iz obrazložitvenega okvira Združenega kraljestva izhaja, da so pridobljene informacije lahko potrebne za identifikacijo zanimivih subjektov in da gre običajno za ustrezne operacije večjega obsega (UK Explanatory Framework, section H: National security, str. 28, opomba 29).

([368]) Člena 138(1) in 178(1) zakona o preiskovalnih pooblastilih iz leta 2016.

([369]) Člena 138(2) in 178(2) zakona o preiskovalnih pooblastilih iz leta 2016.

([370]) V skladu s pojasnili organov Združenega kraljestva lahko operativni namen na primer omejuje obseg ukrepa na obstoj grožnje na določenem geografskem območju.

([371]) Člen 142(4) do (10) zakona o preiskovalnih pooblastilih iz leta 2016.

([372]) Sodišče High Court of Justice, zadeva Liberty, [2019] EWHC 2057 (Admin), točka 167.

([373]) Člena 152 in 193 zakona o preiskovalnih pooblastilih iz leta 2016 določata: (a) da je treba izbiro podatkov za pregled opraviti le v operativne namene, navedene v odredbi, (b) da mora biti izbira za pregled potrebna in sorazmerna v vseh okoliščinah, ter (c) da izbira za pregled ne sme kršiti prepovedi izbire gradiva in identifikacije komunikacij, ki so jih poslali posamezniki oziroma ki so namenjene posameznikom, za katere se ve, da so v zadevnem času na Britanskem otočju.

([374]) Glej kodeks ravnanja glede prestrezanja komunikacij, točka 6.6, opomba 278.

(223) Pooblastila v večjem obsegu se lahko odobrijo le, če so sorazmerna s ciljem ([375]). Kot je navedeno v kodeksu ravnanja glede prestrezanja, vsaka ocena sorazmernosti vključuje „presojo stopnje posega v zasebnost (in druge preudarke iz člena 2(2)) glede na potrebo po izvedbi dejavnosti v preiskovalnem ali operativnem smislu in smislu zmogljivosti. Odobreno ravnanje bi moralo omogočiti realne možnosti za dosego pričakovanih koristi in ne sme biti nesorazmerno ali arbitrarno“ ([376]). Kot je že bilo navedeno, v praksi to pomeni, da preskus sorazmernosti temelji na preskusu uravnoteženosti med ciljem („operativni namen(i)“) in razpoložljivimi tehničnimi možnostmi (na primer ciljno prestrezanje, poseganje v opremo, pridobivanje komunikacijskih podatkov, ali prestrezanje, poseganje v opremo, pridobivanje komunikacijskih podatkov v večjem obsegu), pri čemer je treba dati prednost najmanj intruzivnim sredstvom (glej uvodni izjavi (181) in (182) above). Kadar je glede na cilj primernih več ukrepov, je treba izbrati manj intruzivna sredstva.

(224) Dodaten zaščitni ukrep pri oceni sorazmernosti zahtevanega ukrepa je tudi dejstvo, da mora pristojni minister prejeti zadevne informacije, ki jih potrebuje za ustrezno izvedbo ocene. Natančneje, kodeks ravnanja glede prestrezanja in kodeks ravnanja glede poseganja v opremo določata, da morajo biti v vlogi, ki jo predloži zadevni organ, navedeni ozadje vloge, opis komunikacij, ki se bodo prestrezale, ter telekomunikacijski operaterji, ki bodo morali pri tem sodelovati, opis ravnanja, ki se odobri, operativni nameni in pojasnilo, zakaj je tako ravnanje potrebno in sorazmerno ([377]).

(225) Nazadnje je pomembno, da mora odločitev pristojnega ministra o izdaji odredbe odobriti neodvisni pravosodni pooblaščenec, ki oceni presojo potrebnosti in sorazmernosti predlaganega ukrepa ter pri tem uporabi enaka načela, kot bi jih uporabilo sodišče v postopku sodne presoje ([378]). Pravosodni pooblaščenec pregleda ugotovitve pristojnega ministra glede tega, ali je odredba potrebna in ali je ravnanje sorazmerno glede na načela iz člena 2(2) zakona o preiskovalnih pooblastilih iz leta 2016 (splošne obveznosti glede zasebnosti). Pravosodni pooblaščenec tudi preveri ugotovitve pristojnega ministra o tem, ali je vsak od operativnih namenov, navedenih v odredbi, eden od tistih, za katere je izbira potrebna ali bi lahko bila potrebna. Če pravosodni pooblaščenec zavrne odobritev odločitve o izdaji odredbe, lahko pristojni minister: (i) tako odločitev sprejme in ne izda odredbe ali (ii) zadevo preda v odločanje pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil (razen če je ta že sprejel prvotno odločitev) ([379]).

(ii) *Dodatni zaščitni ukrepi*

(226) Zakon o preiskovalnih pooblastilih iz leta 2016 uvaja nadaljnje omejitve glede trajanja, podaljšanja in spremembe odredb o ukrepih v večjem obsegu. Odredba lahko velja največ šest mesecev, vsako odločitev o podaljšanju ali spremembi odredbe (razen glede manjših sprememb) pa mora odobriti tudi pravosodni pooblaščenec ([380]). Kodeks ravnanja glede prestrezanja in kodeks ravnanja glede poseganja v opremo določata, da se sprememba operativnega namena odredbe šteje za večjo spremembo odredbe ([381]).

([375]) Člen 138(1)(b) in (c) ter člen 178(b) in (c) zakona o preiskovalnih pooblastilih iz leta 2016.

([376]) Kodeks ravnanja glede prestrezanja komunikacij, točka 4.10, opomba 278.

([377]) Kodeks ravnanja glede prestrezanja komunikacij, točka 6.20, opomba 278, in kodeks ravnanja glede poseganja v opremo, točka 6.13, opomba 348.

([378]) Člena 138(1)(g) in 178(1)(f) zakona o preiskovalnih pooblastilih iz leta 2016. Evropsko sodišče za človekove pravice je predhodno odobritev s strani neodvisnega organa opredelilo kot pomemben zaščitni ukrep proti zlorabam v okviru prestrezanja v večjem obsegu. Sodba Evropskega sodišča za človekove pravice (veliki senat) v zadevi Big Brother Watch and others v United Kingdom (glej opombo 269), točki 351 in 352. Upoštevati je treba, da se je ta sodba nanašala na prejšnji pravni okvir (zakon o urejanju preiskovalnih pooblastil iz leta 2000), ki ni vseboval nekaterih zaščitnih ukrepov (vključno s predhodno odobritvijo s strani neodvisnega pravosodnega pooblaščenca), ki so bili uvedeni z zakonom o preiskovalnih pooblastilih iz leta 2016.

([379]) Člen 159(3) in (4) zakona o preiskovalnih pooblastilih iz leta 2016.

([380]) Členi 143 do 146 in 184 do 188 zakona o preiskovalnih pooblastilih iz leta 2016. V primeru nujnih sprememb lahko pristojni minister odredbo spremeni brez odobritve, vendar mora pooblaščenca o tem obvestiti, ta pa mora sprejeti odločitev o odobritvi ali zavrnitvi spremembe (člen 147 zakona o preiskovalnih pooblastilih iz leta 2016). Odredbo je treba preklicati, kadar ni več potrebna ali sorazmerna, ali kadar pregled prestrežene vsebine, metapodatkov ali drugih podatkov, pridobljenih na podlagi odredbe, ni več potreben za nobenega od operativnih namenov, navedenih v odredbi (člena 148 in 189 zakona o preiskovalnih pooblastilih iz leta 2016).

([381]) Kodeks ravnanja glede prestrezanja komunikacij, točke 6.44 do 6.47, opomba 278, in kodeks ravnanja glede poseganja v opremo, točka 6.48, opomba 348.

(227) Podobno kot glede ciljnega prestrezanja, del 6 zakona o preiskovalnih pooblastilih iz leta 2016 določa, da mora pristojni minister zagotoviti zaščitne ukrepe glede hrambe in razkritja gradiva, pridobljenega na podlagi odredbe ([382]), ter glede razkritja v tujino ([383]). Zlasti člena 150(5) in 191(5) zakona o preiskovalnih pooblastilih iz leta 2016 določata, da je treba vsako kopijo katerega koli gradiva, zbranega na podlagi odredbe, varno hraniti in uničiti takoj, ko več ne obstajajo upoštevni razlogi za njegovo hrambo; člena 150(2) in 191(2) pa določata, da je treba število oseb, ki se jim gradivo razkrije, da na voljo ali kopira, omejiti na tiste, za katere je to iz zakonskih razlogov potrebno ([384]).

(228) Nazadnje, če je treba gradivo, prestreženo na podlagi odredbe o prestrezanju v večjem obsegu ali odredbe o poseganju v opremo v večjem obsegu, izročiti tretji državi („razkritje v tujino“), zakon o preiskovalnih pooblastilih iz leta 2016 določa, da mora pristojni minister zagotoviti ustrezne ukrepe, s katerimi se zagotovi, da v navedeni tretji državi veljajo podobni zaščitni ukrepi glede varstva, hrambe in razkritja ([385]). Poleg tega člen 109 zakona o varstvu podatkov iz leta 2018 določa posebne zahteve za mednarodne prenose osebnih podatkov s strani obveščevalnih služb v tretje države ali mednarodnim organizacijam in ne dovoljuje prenosa podatkov v državo ali na ozemlje zunaj Združenega kraljestva ali mednarodni organizaciji, razen če je prenos potreben in sorazmeren za namene zakonskih nalog upravljavca ali za drug namen iz člena 2(2)(a) zakona o varnostnih službah iz leta 1989 oziroma člena 2(2)(a) in 4(2)(a) zakona o obveščevalnih službah iz leta 1994 ([386]). Pomembno je, da se te zahteve uporabljajo tudi v primerih, ko se sklicuje na izjemo glede nacionalne varnosti v skladu s členom 110 zakona o varstvu podatkov iz leta 2018, saj v členu 110 zakona o varstvu podatkov iz leta 2018 ni naveden člen 109 zadevnega zakona kot ena od določb, ki se ne uporabijo, če je zaradi zaščite nacionalne varnosti potrebno izvzetje iz nekaterih določb.

(229) Ko je odredba odobrena in so podatki zbrani v večjem obsegu, se opravi izbira podatkov pred pregledom. Izbira in pregled se preverita z nadaljnjim preskusom sorazmernosti, ki ga opravi analitik; ta na podlagi operativnih namenov iz odredbe (in morebitne ureditve filtriranja) opredeli merila za izbiro. Kot je določeno v členih 152 in 193 zakona o preiskovalnih pooblastilih, mora pristojni minister pri izdaji odredbe zagotoviti, da se izbira gradiva opravi le za navedene operativne namene ter da je v vseh okoliščinah potrebna in sorazmerna. V tem smislu so organi Združenega kraljestva pojasnili, da se gradivo, prestreženo v večjem obsegu, najprej razvrsti prek samodejnega filtriranja, z namenom izločanja podatkov, za katere ni verjetno, da so koristni za nacionalno varnost. Filtri se s časom spreminjajo (v skladu s spremembami vzorcev spletnega prometa, vrst in protokolov), odvisni pa so od tehnologije in operativnega konteksta. Nato se lahko podatki izberejo za pregled le, če so relevantni za operativne namene, navedene v odredbi ([387]). Zaščitni ukrepi, ki jih določa zakon o preiskovalnih pooblastilih iz leta 2016 za proučevanje zbranega gradiva, se uporabljajo za vse vrste podatkov (prestrežene in sekundarne podatke) ([388]). Člena 152 in 193 zakona o preiskovalnih pooblastilih iz leta 2016 določata tudi splošno prepoved, da se za pregled izbere gradivo, ki se nanaša na pogovore, ki jih pošljejo posamezniki, ki so na Britanskem otočju, ali ki so namenjeni takim posameznikom. Če želijo organi pregledati tako gradivo, morajo vložiti zahtevo za izdajo odredbe o ciljnem pregledu na podlagi dela 2 in dela 4 zakona o preiskovalnih pooblastilih iz leta 2016, ki jo izda pristojni minister in odobri pravosodni pooblaščenec ([389]). Če oseba za pregled namenoma izbere prestreženo vsebino tako, da pri tem krši zahteve iz zakonodaje ([390]), stori kaznivo dejanje ([391]).

([382]) Člen 156 zakona o preiskovalnih pooblastilih iz leta 2016.

([383]) Člena 150 in 191 zakona o preiskovalnih pooblastilih iz leta 2016.

([384]) Sodba velikega senata Evropskega sodišča za človekove pravice v zadevi Big Brother Watch and others v United Kingdom (glej opombo 268) je potrdila sistem dodatnih zaščitnih ukrepov za hrambo, dostop in razkritje, ki je bil določen z zakonom o urejanju preiskovalnih pooblastil iz leta 2000, glej točke 392–394 in 402–405. Enak sistem zaščitnih ukrepov določa zakon o preiskovalnih pooblastilih iz leta 2016.

([385]) Člena 151 in 192 zakona o preiskovalnih pooblastilih iz leta 2016.

([386]) Za več informacij o teh namenih glej opombo 312.

([387]) Kodeks glede prestrezanja komunikacij glede tega določa, da „ti sistemi obdelave obdelujejo podatke iz komunikacijskih povezav ali signalov, ki jih za prestrezanje izbere organ. Nato se glede prometa na navedenih povezavah in signalih uporabi stopnja filtriranja, ki je namenjena izbiri vrste komunikacij, ki ima potencialno obveščevalno vrednost, završe pa se tista komunikacija, za katero je najmanj verjetno, da ima kakšno obveščevalno vrednost. Na podlagi takega filtriranja, ki se razlikuje glede na sistem obdelave, se velik delež komunikacij na teh povezavah in signalih samodejno završe. Nato se lahko izvedejo nadaljnja zapletena iskanja za odkrivanje komunikacij, pri katerih je najbolj verjetno, da bodo imele največjo obveščevalno vrednost glede na zakonske naloge agencije. Te komunikacije se nato lahko izberejo za pregled na podlagi enega ali več operativnih namenov, navedenih v odredbi, če so izpolnjeni pogoji glede potrebnosti in sorazmernosti. Za pregled pri pooblaščenih osebah so lahko potencialno izbrani le podatki, ki niso bili odstranjeni pri filtriranju“ (kodeks ravnanja glede prestrezanja komunikacij, točka 6.6, opomba 278).

([388]) Glej člen 152(1)(a) in (b) zakona o preiskovalnih pooblastilih iz leta 2016, v skladu s katerim je treba pregled obeh vrst podatkov (prestreženi in sekundarni podatki) opraviti le za določen namen ter mora biti v vseh okoliščinah potreben in sorazmeren.

([389]) Ta vrsta odredbe ni potrebna, kadar so podatki o posameznikih na Britanskem otočju „sekundarni podatki“ (glej člen 152(1)(c) zakona o preiskovalnih pooblastilih iz leta 2016).

([390]) Člena 152 in 193 zakona o preiskovalnih pooblastilih iz leta 2016.

([391]) Člena 155 in 196 zakona o preiskovalnih pooblastilih iz leta 2016.

(230) Oceno analitika glede izbire gradiva naknadno preveri pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil, ki oceni skladnost s posameznimi zaščitnimi ukrepi iz zakona o preiskovalnih pooblastilih iz leta 2016 v fazi pregleda ([392]) (glej tudi uvodno izjavo (229)). Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil mora preverjati (tudi z revizijami, inšpekcijskimi pregledi in preiskavami), kako javni organi izvršujejo preiskovalna pooblastila iz zakona o preiskovalnih pooblastilih iz leta 2016 ([393]). V zvezi s tem kodeks ravnanja glede prestrezanja in kodeks ravnanja glede poseganja v opremo določata, da morajo agencije voditi evidence z namenom naknadnega preverjanja in revizij, v evidencah pa mora biti naveden ustrezen operativni namen in zakaj je dostop do gradiva s strani pooblaščenih oseb potreben in sorazmeren ([394]). Urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil (IPCO) je v svojem letnem poročilu za leto 2018 ([395]) na primer ugotovil, da utemeljitve, ki jih glede pregleda nekaterega gradiva, zbranega v večjem obsegu, navajajo analitiki, ustrezajo zahtevanemu standardu sorazmernosti, saj je navedenih dovolj podrobnosti glede razlogov za poizvedbo glede na cilj ([396]). Urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil je v poročilu za leto 2019 v zvezi s pooblastili v večjem obsegu jasno navedel, da namerava še naprej preverjati prestrezanja v večjem obsegu, vključno s podrobnim pregledom izbirnikov in iskalnih meril ([397]). Prav tako bo za vsak primer posebej še naprej podrobno preverjal izbiro nadzornih ukrepov (ciljni oziroma v večjem obsegu), in sicer tako pri obravnavi vlog za izdajo odredbe na podlagi postopka z dvojnim varovalom kot tudi med preverjanji ([398]). To nadaljnje spremljanje se bo ustrezno upoštevalo v okviru spremljanja tega sklepa, ki ga bo izvajala Komisija in je opredeljeno v uvodnih izjavah (281)–(284).

3.3.1.1.4.2 Pridobivanje komunikacijskih podatkov v večjem obsegu

(231) Poglavje 2 dela 6 zakona o preiskovalnih pooblastilih iz leta 2016 ureja odredbe o pridobivanju podatkov v večjem obsegu, na podlagi katerih lahko naslovnik od telekomunikacijskega operaterja zahteva razkritje ali pridobitev katerih koli komunikacijskih podatkov, ki jih ima v posesti. Na podlagi teh odredb lahko organ prosilec tudi izbere podatke za nadaljnjo fazo pregleda. Tako kot pri ciljni hrambi in pridobivanju komunikacijskih podatkov (glej uvodno izjavo (199)) tudi pri pridobivanju komunikacijskih podatkov v večjem obsegu velja, da se običajno ne nanaša na osebne podatke posameznikov iz EU, na katere se nanašajo in ki so preneseni v Združeno kraljestvo na podlagi tega sklepa. Obveznost razkritja komunikacijskih podatkov na podlagi poglavja 2 dela 6 zakona o preiskovalnih pooblastilih iz leta 2016 se nanaša na podatke, ki jih zbirajo telekomunikacijski operaterji v Združenem kraljestvu neposredno od uporabnikov telekomunikacijskih storitev ([399]). Te vrste obdelava, ki je usmerjena v stranke, običajno ne vključuje prenosov na podlagi tega sklepa, tj. prenosov od upravljavca/obdelovalca v EU k upravljavcu/obdelovalcu v Združenem kraljestvu.

(232) Vendar pa so zaradi celovitosti v nadaljevanju opisani pogoji in zaščitni ukrepi, ki se uporabljajo za pridobivanje komunikacijskih podatkov v večjem obsegu.

([392]) Člena 152 in 193 zakona o preiskovalnih pooblastilih iz leta 2016.

([393]) Člen 229 zakona o preiskovalnih pooblastilih iz leta 2016.

([394]) Kodeks ravnanja glede prestrezanja komunikacij, točka 6.74, opomba 278, in kodeks ravnanja glede poseganja v opremo, točka 6.78, opomba 348.

([395]) Urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil je bil ustanovljen na podlagi člena 238 zakona o preiskovalnih pooblastilih iz leta 2016 in ima zagotovljeno potrebno osebje, prostore, opremo ter druge zmogljivosti in storitve, ki so potrebne za izvajanje njegovih nalog (glej uvodno izjavo (251))

([396]) V letnem poročilu urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2018 je navedeno, da utemeljitve, ki jih navajajo analitiki vladne obveščevalne službe GCHQ, „dosegajo zahtevane standarde, analitiki pa dovolj podrobno preverjajo sorazmernost svojih poizvedb, ki se nanašajo na podatke v večjem obsegu“. Annual Report of the Investigatory Powers Commissioner 2018, točka 6.22, opomba 464.

([397]) Annual Report of the Investigatory Powers Commissioner 2019, točka 7.6, opomba 463.

([398]) Annual Report of the Investigatory Powers Commissioner 2019, točka 10.22, opomba 463.

([399]) To izhaja iz opredelitve komunikacijskih podatkov iz člena 261(5) zakona o preiskovalnih pooblastilih iz leta 2016, v skladu s katero komunikacijske podatke hrani ali pridobi telekomunikacijski operater, podatki pa se nanašajo na uporabnika telekomunikacijske storitve in zagotavljanje te storitve ali pa so del komunikacije, vključeni vanjo, ji priloženi ali z njo logično povezani (glej tudi kodeks ravnanja glede pridobivanja komunikacijskih podatkov v večjem obsegu, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf točke 2.15 do 2.22). Opredelitev telekomunikacijskega operaterja iz člena 261(10) zakona o preiskovalnih pooblastilih iz leta 2016 tudi določa, da je telekomunikacijski operater oseba, ki ponuja ali zagotavlja telekomunikacijske storitve osebam v Združenem kraljestvu ali ki nadzoruje oziroma zagotavlja telekomunikacijski sistem, ki je (v celoti ali delno) v Združenem kraljestvu ali se nadzoruje iz Združenega kraljestva. Iz teh opredelitev jasno izhaja, da obveznosti iz zakona o preiskovalnih pooblastilih iz leta 2016 ni mogoče naložiti telekomunikacijskih operaterjem, ki nimajo opreme v Združenem kraljestvu ali ki svoje opreme ne nadzorujejo iz Združenega kraljestva, in ki ne ponujajo ali zagotavljajo storitev osebam v Združenem kraljestvu (glej tudi kodeks ravnanja glede pridobivanja komunikacijskih podatkov v večjem obsegu, točka 2.2). Če naročniki iz EU (ki so v EU ali v Združenem kraljestvu) uporabljajo storitve v Združenem kraljestvu, vse komunikacije v zvezi z zagotavljanjem te storitve zbira neposredno ponudnik storitve v Združenem kraljestvu in niso predmet prenosa iz EU.

(233) Zakon o preiskovalnih pooblastilih iz leta 2016 nadomešča zakonodajo glede pridobivanja komunikacijskih podatkov v večjem obsegu, ki je bila predmet sodbe Sodišča EU v zadevi Privacy International. Navedena zakonodaja je bila razveljavljena, nova ureditev pa zagotavlja posebne pogoje in zaščitne ukrepe, na podlagi katerih je mogoče tak ukrep odobriti.

(234) Razlika od prejšnje ureditve, na podlagi katere je imel pristojni minister prosto presojo glede odobritve ukrepa ([400]), je zlasti, da lahko pristojni minister na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 odredbo izda le, če je ukrep potreben in sorazmeren. V praksi to pomeni, da mora obstajati povezava med dostopom do podatkov in ciljem ([401]). Natančneje, pristojni minister mora proučiti obstoj povezave med zahtevanim ukrepom in enim ali več „operativnimi nameni", navedenimi v odredbi (glej uvodno izjavo 219). Glede presoje sorazmernosti zadevni kodeks ravnanja določa, da „mora pristojni minister upoštevati, ali bi bilo razumno mogoče cilj odredbe doseči z manj intruzivnimi sredstvi (člen 2(2)(a) zakona). Na primer s pridobitvijo zahtevanih informacij z manj intruzivnimi pooblastili, kot je ciljno pridobivanje komunikacijskih podatkov" ([402]).

(235) Pri izvajanju take ocene se mora pristojni minister zanesti na informacije, ki jih morajo v vlogi predložiti vodje obveščevalnih služb ([403]), kot so na primer razlogi, zakaj je ukrep potreben glede na enega od zakonskih razlogov, ter razlogi, zakaj cilja ni mogoče razumno doseči z drugimi, manj intruzivnimi sredstvi ([404]). Nadalje, operativni nameni omejujejo obseg podatkov, ki jih je na podlagi odredbe mogoče izbrati za pregled ([405]). Kot je navedeno v zadevnem kodeksu ravnanja, morajo operativni nameni opredeljevati jasno zahtevo in biti dovolj podrobno opredeljeni, da se pristojni minister lahko prepriča, da so lahko pridobljeni podatki izbrani za pregled le iz določenih razlogov ([406]). Pred odobritvijo odredbe mora pristojni minister zagotoviti ustrezno ureditev, ki zagotavlja, da se za pregled izbere le gradivo, ki ga je treba pregledati zaradi operativnih in zakonskih namenov, ter da je to v vseh okoliščinah sorazmerno in potrebno. Ta specifična zahteva, ki se odraža v členih 158 in 172 zakona o preiskovalnih pooblastilih iz leta 2016 ([407]) in se nanaša na predhodno oceno potrebnosti in sorazmernosti meril, ki se uporabljajo pri izbiri, je še ena pomembna novost ureditve, ki je bila uvedena z zakonom o preiskovalnih pooblastilih iz leta 2016, v primerjavi s predhodno ureditvijo.

(236) Zakon o preiskovalnih pooblastilih iz leta 2016 tudi uvaja obveznost pristojnega ministra, ki mora pred izdajo odredbe o pridobivanju komunikacijskih podatkov v večjem obsegu zagotoviti posebne omejitve glede varstva, hrambe in razkritja zbranih osebnih podatkov ([408]). V primeru razkritja v tujino se v tem smislu uporabljajo tudi zaščitni ukrepi, opisani v uvodni izjavi (227) glede prestrezanja v večjem obsegu in poseganja v opremo v večjem obsegu ([409]). Zakonodaja določa tudi nadaljnje omejitve glede trajanja ([410]), podaljševanja ([411]) in glede sprememb odredb o ukrepih v večjem obsegu ([412]).

(237) Pomembno je, da mora pristojni minister pred izdajo odredbe pridobiti odobritev pravosodna pooblaščenca, tako kot pri drugih pooblastilih v večjem obsegu ([413]). To je ključna značilnost ureditve, uvedene z zakonom o preiskovalnih pooblastilih iz leta 2016.

([400]) Člen 94(1) zakona o telekomunikacijah iz leta 1984 (Telecommunication Act 1984) določa, da lahko pristojni minister izda „splošna navodila, kot meni, da je potrebno ali smotrno v interesu nacionalne varnosti (...)" (opomba 451).

([401]) Glej zadevo Privacy International, točka 78

([402]) Glej kodeks ravnanja glede pridobivanja komunikacijskih podatkov v večjem obsegu, točka 4.11, (opomba 399414).

([403]) Izdajo odredbe o pridobivanju podatkov v večjem obsegu lahko zahtevajo le vodje obveščevalnih služb: (i) generalni direktor varnostne službe, (ii) vodja tajne obveščevalne službe ali (iii) direktor vladne obveščevalne službe GCHQ (glej člena 158 in 263 zakona o preiskovalnih pooblastilih iz leta 2016).

([404]) Kodeks ravnanja glede pridobivanja komunikacijskih podatkov v večjem obsegu, točka 4.5 (opomba 399).

([405]) Člen 161 zakona o preiskovalnih pooblastilih iz leta 2016 določa, da morajo biti operativni nameni, ki so opredeljeni v odredbi, navedeni tudi na seznamu namenov, ki ga vodijo vodje obveščevalnih služb („seznam operativnih namenov") in za katere menijo, da so operativni nameni, na podlagi katerih je mogoče komunikacijske podatke, pridobljene na podlagi odredb o pridobivanju podatkov v večjem obsegu, izbrati za pregled.

([406]) Kodeks ravnanja glede pridobivanja komunikacijskih podatkov v večjem obsegu, točka 6.6 (opomba 399).

([407]) Člen 172 zakona o preiskovalnih pooblastilih iz leta 2016 zahteva vzpostavitev posebnih zaščitnih ukrepov v fazi filtriranja komunikacij, pridobljenih v večjem obsegu, in njihove izbire za pregled. Poleg tega je nameren pregled v nasprotju s temi zaščitnimi ukrepi tudi kaznivo dejanje (glej člen 173 zakona o preiskovalnih pooblastilih iz leta 2016).

([408]) Člen 171 zakona o preiskovalnih pooblastilih iz leta 2016.

([409]) Člen 171(9) zakona o preiskovalnih pooblastilih iz leta 2016.

([410]) Člen 162 zakona o preiskovalnih pooblastilih iz leta 2016.

([411]) Člen 163 zakona o preiskovalnih pooblastilih iz leta 2016.

([412]) Členi 164 do 166 zakona o preiskovalnih pooblastilih iz leta 2016.

([413]) Člen 159 zakona o preiskovalnih pooblastilih iz leta 2016.

(238) Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil izvaja naknadni nadzor nad postopkom pregleda gradiva (komunikacijskih podatkov), pridobljenega v večjem obsegu (glej uvodno izjavo (254) below). V tem smislu je zakon o preiskovalnih pooblastilih iz leta 2016 uvedel zahtevo, da mora obveščevalni analitik, ki izvaja pregled, pred izbiro podatkov za pregled evidentirati razloge, zakaj je predlagani pregled potreben in sorazmeren za posamezni operativni namen ([414]). Glede prakse služb GCHQ in MI5 je bilo v letnem poročilu urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019 ugotovljeno, da „iz spisov, ki smo jih proučili, izhaja, da je bila pri več dejavnostih službe GCHQ ključna vloga komunikacijskih podatkov v večjem obsegu dobro pojasnjena. Proučili smo naravo zahtevanih podatkov in navedene obveščevalne zahteve ter ugotovili, da iz dokumentacije izhaja, da je bil njihov pristop potreben in sorazmeren“ ([415]). Evidentirane utemeljitve agencije MI5 so dosegale dobre standarde in so upoštevale načeli potrebnosti in sorazmernosti“ ([416]).

3.3.1.1.4.3 Hramba in pregled nabora osebnih podatkov v večjem obsegu

(239) Odredbe o naboru osebnih podatkov v večjem obsegu ([417]) obveščevalnim agencijam omogočajo hrambo in pregledovanje naborov podatkov, ki vsebujejo osebne podatke številnih posameznikov. V skladu s pojasnili organov Združenega kraljestva je lahko analiza takih naborov podatkov „edini način, da obveščevalna skupnost Združenega kraljestva izvede preiskave in identificira teroriste na podlagi zelo omejenih obveščevalnih indicev ali kadar namenoma prikrivajo svojo komunikacijo“ ([418]). Obstajata dve vrsti odredb. „Odredbe o kategorijah naborov osebnih podatkov v večjem obsegu“ ([419]) se nanašajo na določene kategorije naborov podatkov, tj. na tiste, ki so si podobni po vsebini in predlagani uporabi in sprožajo podobne pomisleke, na primer glede stopnje poseganja in občutljivosti ter sorazmernosti uporabe podatkov, zaradi česar lahko pristojni minister prouči potrebnost in sorazmernost pridobitve vseh podatkov v posamezni kategoriji naenkrat. Odredba o kategorijah naborov osebnih podatkov v večjem obsegu se lahko na primer nanaša na nabore podatkov o potovanju, ki se nanašajo na podobne poti ([420]). V nasprotju s tem se „odredbe o specifičnih naborih osebnih podatkov v večjem obsegu“ ([421]) nanašajo na en specifičen nabor podatkov, na primer na nabor podatkov o novi ali nenavadni vrsti informacij, ki ne spada v obstoječo odredbo o kategorijah naborov osebnih podatkov v večjem obsegu, ali nabor podatkov, ki se nanaša na posebno vrsto osebnih podatkov ([422]), zato je zanj treba zagotoviti dodatne zaščitne ukrepe ([423]). Določbe zakona o preiskovalnih pooblastilih iz leta 2016, ki se nanašajo na odredbe o naboru osebnih podatkov v večjem obsegu, omogočajo pregled in hrambo takih naborov podatkov le, kadar je to potrebno in sorazmerno ([424]), ter v skladu s splošnimi obveznostmi, ki se nanašajo na zasebnost ([425]).

(240) Odredba o naboru osebnih podatkov v večjem obsegu se izdaja v postopku z dvojnim varovalom: najprej oceno potrebnosti in sorazmernosti ukrepa opravi pristojni minister, nato pa še pravosodni pooblaščenec ([426]). Pristojni minister mora proučiti naravo in obseg vrste odredbe, katere izdaja se zahteva, vrsto zadevnih podatkov in število posameznih naborov osebnih podatkov v večjem obsegu, ki bodo najverjetneje vključeni v posebno vrsto odredbe ([427]). Kot je opredeljeno v kodeksu ravnanja glede hrambe in uporabe naborov osebnih podatkov v večjem obsegu s strani obveščevalnih služb, je treba tudi voditi podrobne evidence, ki jih preverja pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil ([428]). Hramba in pregledovanje naborov osebnih podatkov v večjem obsegu v nasprotju z omejitvami zakona o preiskovalnih pooblastilih iz leta 2016 je kaznivo dejanje ([429]).

([414]) Letno poročilo urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019, točka 8.6, glej opomba 463.
([415]) Letno poročilo urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019, točka 10.4, opomba 463.
([416]) Letno poročilo urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019, točka 8.37, opomba 463.
([417]) Člen 200 zakona o preiskovalnih pooblastilih iz leta 2016.
([418]) The UK Explanatory Framework for Adequacy Discussions, section H: National Security: Nacionalna varnost), stran 34, opomba 29.
([419]) Člen 204 zakona o preiskovalnih pooblastilih iz leta 2016.
([420]) Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets (Kodeks ravnanja glede hrambe in uporabe naborov osebnih podatkov v večjem obsegu s strani obveščevalnih služb), točka 4.7, na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) Člen 205 zakona o preiskovalnih pooblastilih iz leta 2016.
([422]) Kot so na primer občutljivi osebni podatki, glej člen 202 zakona o preiskovalnih pooblastilih iz leta 2016 in kodeks ravnanja glede hrambe in uporabe naborov osebnih podatkov v večjem obsegu s strani obveščevalnih služb, točki 4.21 in 4.12, opomba 469.
([423]) Vlogo za odredbo o specifičnih naborih osebnih podatkov v večjem obsegu mora posamično proučiti pristojni minister, torej glede na en specifični nabor podatkov. Na podlagi člena 205 zakona o preiskovalnih pooblastilih morajo obveščevalne službe v vlogo za izdajo odredbe o specifičnih naborih osebnih podatkov v večjem obsegu vključiti podrobno pojasnilo o naravi in obsegu zadevnega gradiva ter seznam „operativnih namenov“, za katere želi zadevna obveščevalna služba pregledati nabor osebnih podatkov v večjem obsegu (kadar obveščevalna služba prosi za izdajo odredbe za hrambo in pregled in ne samo za hrambo). V nasprotju s tem pri izdaji odredbe o kategorijah naborov osebnih podatkov v večjem obsegu pristojni minister prouči celotno kategorijo nabora podatkov hkrati.
([424]) Člena 204 in 205 zakona o preiskovalnih pooblastilih iz leta 2016.
([425]) Člen 2 zakona o preiskovalnih pooblastilih iz leta 2016.
([426]) Člena 204 in 205 zakona o preiskovalnih pooblastilih iz leta 2016.
([427]) Kodeks ravnanja glede hrambe in uporabe naborov osebnih podatkov v večjem obsegu s strani obveščevalnih služb, točka 5.2, opomba 420.
([428]) Kodeks ravnanja glede hrambe in uporabe naborov osebnih podatkov v večjem obsegu s strani obveščevalnih služb, točke 8.1 do 8.15, opomba 420.
([429]) The UK Explanatory Framework for Adequacy Discussions, section H: National Security, stran 34, opomba 29.

3.3.2 *Nadaljnja uporaba zbranih informacij*

(241) Osebni podatki, ki se obdelujejo na podlagi dela 4 zakona o varstvu podatkov iz leta 2018, se ne smejo obdelovati v nasprotju z namenom, za katerega so bili zbrani ([430]). Zakon o varstvu podatkov iz leta 2018 določa, da lahko upravljavec podatke obdeluje za drug namen od tistega, za katerega so bili zbrani, če je ta skladen s prvotnim namenom, če je upravljavec po zakonu pooblaščen za obdelavo podatkov in če je obdelava potrebna in sorazmerna ([431]). Poleg tega zakon o varnostnih službah iz leta 1989 (Security Services Act 1989) in zakon o obveščevalnih službah iz leta 1994 (Intelligence Services Act 1994) določata, da morajo vodje obveščevalnih agencij zagotoviti, da se informacije pridobijo ali razkrijejo le, če je to potrebno za ustrezno izvajanje nalog agencije ali za druge omejene in določene namene, navedene v ustreznih določbah ([432]).

(242) Poleg tega člen 109 zakona o varstvu podatkov iz leta 2018 določa posebne zahteve glede mednarodnega prenosa osebnih podatkov s strani obveščevalnih služb v tretje države ali mednarodne organizacije. V skladu s to določbo se osebni podatki se smejo prenašati v državo ali na ozemlje zunaj Združenega kraljestva ali k mednarodni organizaciji, razen če je prenos potreben in sorazmeren za namene zakonskih nalog upravljavca ali za drug namen iz člena 2(2)(a) zakona o varnostnih službah iz leta 1989 oziroma člena 2(2)(a) in 4(2)(a) zakona o obveščevalnih službah iz leta 1994 ([433]). Pomembno je, da se te zahteve uporabljajo tudi v primerih, ko se sklicuje na izjemo glede nacionalne varnosti v skladu s členom 110 zakona o varstvu podatkov iz leta 2018, saj v členu 110 zakona o varstvu podatkov iz leta 2018 ni naveden člen 109 zadevnega zakona kot ena od določb, ki se ne uporabijo, če je zaradi zaščite nacionalne varnosti potrebno izvzetje iz nekaterih določb.

(243) Prav tako, kot je urad informacijskega pooblaščenca poudaril v svojih smernicah o obdelavi s strani obveščevalnih služb, poleg zaščitnih ukrepov iz dela 4 zakona o varstvu podatkov iz leta 2018 za obveščevalne agencije pri posredovanju podatkov obveščevalnim organom tretje države veljajo tudi zaščitni ukrepi, ki jih določajo drugi zakonodajni ukrepi, ki se uporabljajo zanje, da se zagotovi, da se osebni podatki pridobijo, delijo in obdelujejo zakonito in odgovorno ([434]). Na primer, zakon o preiskovalnih pooblastilih iz leta 2016 določa nadaljnje zaščitne ukrepe glede prenosov gradiva, zbranega na podlagi ciljnega prestrezanja ([435]), ciljnega poseganja v opremo ([436]), prestrezanja v večjem obsegu ([437]), pridobivanja komunikacijskih podatkov v večjem obsegu ([438]) in poseganja v opremo v večjem obsegu ([439]) v tretje države (tako imenovana „razkritja v tujino“). Organ, ki izda odredbo mora predvsem zagotoviti, da tretja država, ki prejme podatke, omeji število oseb, ki vidijo gradivo, obseg razkritja in število kopij katerega koli gradiva, ki se izdelajo, in sicer le na toliko, kot je potrebno za odobrene namene iz zakona o preiskovalnih pooblastilih iz leta 2016 ([440]).

3.3.3 *Nadzor*

(244) Vladni dostop za namene nacionalne varnosti je pod nadzorom več različnih organov. Informacijski pooblaščenec nadzoruje obdelavo osebnih podatkov v smislu zakona o varstvu podatkov iz leta 2018 (več informacij o neodvisnosti, imenovanju, vlogi in pooblastilih informacijskega pooblaščenca je na voljo v uvodnih izjavah (85) do (98)), pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil pa izvaja neodvisen in pravosodni nadzor

([430]) Člen 87(1) zakona o varstvu podatkov iz leta 2018.

([431]) Člen 87(3) zakona o varstvu podatkov iz leta 2018. Čeprav lahko na podlagi člena 110 zakona o varstvu podatkov iz leta 2018 za upravljavce velja izjema od tega načela iz razloga nacionalne varnosti, pa je treba tako izjemo proučiti v vsakem primeru posebej, nanjo pa se je mogoče sklicevati le, če bi uporaba posamezne določbe imela negativne posledice za nacionalno varnost (glej uvodno izjavo (132)). Potrdila glede nacionalne varnosti za obveščevalne službe Združenega kraljestva (na voljo na povezavi: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) se ne nanašajo na člen 87(3) zakona o varstvu podatkov iz leta 2018. Glede na to, da mora za vsako obdelavo za drug namen obstajati pooblastilo v zakonu, morajo imeti obveščevalne službe tudi jasno pravno podlago za nadaljnjo obdelavo.

([432]) Za več informacij o teh namenih glej opombo 312.

([433]) Glej opombo 312.

([434]) Smernice urada informacijskega pooblaščenca o obdelavi s strani obveščevalnih služb (glej opombo 161).

([435]) Člen 54 zakona o preiskovalnih pooblastilih iz leta 2016.

([436]) Člen 130 zakona o preiskovalnih pooblastilih iz leta 2016.

([437]) Člen 151 zakona o preiskovalnih pooblastilih iz leta 2016.

([438]) Člen 171(9) zakona o preiskovalnih pooblastilih iz leta 2016.

([439]) Člen 192 zakona o preiskovalnih pooblastilih iz leta 2016.

([440]) Ureditev mora vključevati ukrepe, s katerimi se zagotovi, da se vsaka kopija katerega koli gradiva ves čas hrambe varno hrani. Gradivo, pridobljeno na podlagi odredbe, in vsako kopijo katerega koli takega gradiva je treba uničiti takoj, ko ni več upoštevnih razlogov za njihovo hrambo (glej člene 150(2), 150(5) in 151(2) zakona o preiskovalnih pooblastilih iz leta 2016). Opozoriti je treba, da je bilo za podobne zaščitne ukrepe, določene v prejšnjem pravnem okviru (zakon o urejanju preiskovalnih pooblastil iz leta 2000), ugotovljeno, da so skladni z zahtevami Evropskega sodišča za človekove pravice glede posredovanja gradiva, pridobljenega s prestrezanjem v večjem obsegu, tretjim državami ali mednarodnim organizacijam (Evropsko sodišče za človekove pravice (veliki senat), Big Brother Watch and others v United Kingdom (glej opombo 279), točke 362 in 399).

nad uporabo preiskovalnih pooblastil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016. Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil nadzoruje uporabo preiskovalnih pooblastil s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in organov za nacionalno varnost na podlagi zakona o preiskovalnih pooblastilih iz leta 2016. Politični nadzor izvaja parlamentarni odbor za obveščevalne službe.

3.3.3.1 Nadzor na podlagi dela 4 zakona o varstvu podatkov

(245) Obdelavo osebnih podatkov, ki jo izvajajo obveščevalne službe na podlagi dela 4 zakona o varstvu podatkov iz leta 2018, nadzoruje informacijski pooblaščenec ([441]).

(246) Splošne naloge informacijskega pooblaščenca v zvezi z obdelavo osebnih podatkov, ki jo izvajajo obveščevalne službe na podlagi dela 4 zakona o varstvu podatkov iz leta 2018, so določene v dodatku 13 k zakonu o varstvu podatkov iz leta 2018. Naloge med drugim vključujejo spremljanje in izvrševanje dela 4 zakona o varstvu podatkov iz leta 2018, ozaveščanje javnosti, svetovanje parlamentu, vladi in drugim institucijam o zakonodajnih in upravnih ukrepih, ozaveščanje upravljavcev in obdelovalcev o njihovih obveznostih, zagotavljanje informacij posameznikom, na katere se nanašajo osebni podatki, o uveljavljanju njihovih pravic, izvajanje preiskav itd.

(247) Kot je določeno v delu 3 zakona o varstvu podatkov iz leta 2018, je informacijski pooblaščenec pristojen za obveščanje upravljavcev o domnevnih kršitvah, izdajanje opozoril, da obdelava verjetno krši pravila, in izrekanje opominov ob potrditvi kršitve. Izdaja lahko tudi obvestila o izvršitvi in o plačilnem nalogu za kršitve nekaterih določb akta ([442]). Informacijski pooblaščenec pa v nasprotju z drugimi deli zakona o varstvu podatkov iz leta 2018 ne more izdati obvestila o preverjanju organu za nacionalno varnost ([443]).

(248) Poleg tega je v členu 110 zakona o varstvu podatkov iz leta 2018 določena izjema glede uporabe nekaterih pooblastil informacijskega pooblaščenca, ko je to potrebno zaradi zaščite nacionalne varnosti. To vključuje pristojnost informacijskega pooblaščenca, da lahko na podlagi zakona o varstvu podatkov izdaja obvestila vseh vrst (obvestilo o predložitvi informacij, obvestilo o preverjanju, obvestilo o izvršitvi in obvestilo o plačilnem nalogu), pristojnost za opravljanje inšpekcijskega nadzora v skladu z mednarodnimi obveznostmi, pristojnost za vstop in inšpekcijski pregled ter pravila o kaznivih dejanjih ([444]). Kot je pojasnjeno v uvodni izjavi (126), se te izjeme uporabljajo le, če je v vsakem primeru posebej to potrebno in sorazmerno.

(249) Urad informacijskega pooblaščenca in obveščevalne službe Združenega kraljestva so podpisale memorandum o soglasju ([445]), ki vzpostavlja okvir za sodelovanje o številnih vprašanjih, vključno z obvestili o kršitvi varstva podatkov in obravnavanjem pritožb posameznikov, na katere se nanašajo osebni podatki. V njem je zlasti določeno, da urad informacijskega pooblaščenca ob prejetju pritožbe preveri, ali je bila izjema zaradi nacionalne varnosti ustrezno uporabljena. Zadevna obveščevalna agencija mora odgovor na poizvedbo urada informacijskega pooblaščenca v zvezi s pritožbo posameznika poslati v 20 delovnih dneh, in sicer prek ustreznih varnih kanalov, če gre za zaupne informacije. Urad informacijskega pooblaščenca je od aprila 2018 do danes prejel 21 pritožb posameznikov glede obveščevalnih služb. Vsako pritožbo je proučil in rezultat sporočil posamezniku, na katerega se nanašajo osebni podatki ([446]).

([441]) Člen 116 zakona o varstvu podatkov iz leta 2018.

([442]) Upravljavcu ali obdelovalcu se lahko v skladu s točko 2 dodatka 13 k zakonu o varstvu podatkov iz leta 2018 izdajo obvestila o izvršitvi in o plačilnem nalogu za kršitve poglavja 2 dela 4 zakona o varstvu podatkov iz leta 2018 (načela obdelave), določbe dela 4 zakona o varstvu podatkov iz leta 2018 o priznanju pravic posamezniku, na katerega se nanašajo osebni podatki, zahteve o obveščanju informacijskega pooblaščenca o kršitvi varstva osebnih podatkov v skladu s členom 108 zakona o varstvu podatkov iz leta 2018 ter načel prenosa osebnih podatkov v tretje države, države, ki niso podpisnice konvencije, in mednarodne organizacije iz člena 109 zakona o varstvu podatkov iz leta 2018 (več informacij o obvestilu o izvršitvi in o plačilnem nalogu je na voljo v uvodni izjavi (92) zgoraj).

([443]) Informacijski pooblaščenec v skladu s členom 147(6) zakona o varstvu podatkov iz leta 2018 ne sme izdati obvestila o preverjanju organu iz člena 23(3) zakona o dostopu do informacij javnega značaja iz leta 2000. To vključuje varnostno službo (MI5), tajno obveščevalno službo (MI6) in vladno obveščevalno službo (GCHQ).

([444]) Določbe, pri katerih so dovoljene izjeme, so: člen 108 (obveščanje informacijskega pooblaščenca o kršitvi varstva osebnih podatkov), člen 119 (inšpekcijski nadzor v skladu z mednarodnimi obveznostmi), členi 142 do 154 in dodatek 15 (obvestila informacijskega pooblaščenca in pristojnost za vstop in inšpekcijski pregled) ter členi 170 do 173 (kazniva dejanja, povezana z osebnimi podatki). Poleg tega pa še tiste, ki se nanašajo na obdelavo s strani obveščevalnih služb iz točke 1(a) in (g) ter točke 2 dodatka 13 (druge splošne naloge informacijskega pooblaščenca).

([445]) Memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, opomba 165.

([446]) Urad informacijskega pooblaščenca je v sedmih od teh primerov pritožniku svetoval, naj se s pritožbo obrne na upravljavca podatkov (ko je posameznik pritožbo najprej vložil pri uradu informacijskega pooblaščenca, moral pa bi jo pri upravljavcu podatkov), v enem od teh primerov je urad upravljavcu podatkov zagotovil splošen nasvet (to se uporablja, kadar ukrepi upravljavca ne kršijo zakonodaje, vendar bi se lahko z boljšo prakso preprečilo vlaganje pritožb pri uradu), v preostalih 13 primerih pa ni bilo potrebno ukrepanje upravljavca podatkov (to se uporablja, kadar posamezniki izrazijo pomisleke, ki spadajo na področje uporabe zakona o varstvu podatkov iz leta 2018, ker se nanašajo na obdelavo osebnih informacij, vendar iz predloženih informacij ni razvidno, da bi upravljavec kršil zakonodajo).

3.3.3.2 Nadzor nad uporabo preiskovalnih pooblastil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016

(250) Na podlagi dela 8 zakona o preiskovalnih pooblastilih iz leta 2016 nadzor nad uporabo preiskovalnih pooblastil izvaja pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil. Pomagajo mu drugi pravosodni pooblaščenci, ki se skupaj imenujejo pravosodni pooblaščenci ([447]). Zakon o preiskovalnih pooblastilih iz leta 2016 določa jamstva, ki ščitijo neodvisnost pravosodnih pooblaščencev. Pravosodni pooblaščenci morajo imeti ali so imeli visoko sodno funkcijo (tj. biti morajo ali so bili člani najvišjih sodišč) ([448]) in so kot vsi člani sodstva neodvisni od vlade ([449]). V skladu s členom 227 zakona o preiskovalnih pooblastilih iz leta 2016 je predsednik vlade tisti, ki imenuje pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil in toliko pravosodnih pooblaščencev, kot se mu zdi potrebno. Vsi pooblaščenci, ne glede na to, ali so sedanji ali nekdanji člani sodstva, so lahko imenovani le na podlagi skupnega priporočila treh vodij sodstva Anglije in Walesa, Škotske in Severne Irske ter lorda kanclerja ([450]). Pristojni minister mora pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil zagotoviti osebje, prostore, opremo ter druge zmogljivosti in storitve ([451]). Pooblaščenec ima triletni mandat, po izteku katerega je lahko znova imenovan ([452]). Dodatno jamstvo za neodvisnost pravosodnih pooblaščencev je, da se lahko razrešijo s položaja le pod strogimi pogoji; odpokliče jih lahko predsednik vlade v posebnih okoliščinah, ki so izčrpno navedene v členu 228(5) zakona o preiskovalnih pooblastilih iz leta 2016 (na primer stečaj ali zaporna kazen), ali če oba domova parlamenta sprejmeta sklep o odpoklicu ([453]).

(251) Pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil in pravosodnim pooblaščencem pri delu pomaga urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil. Osebje navedenega urada vključuje skupino inšpektorjev, internih pravnih in tehničnih strokovnjakov ter tehnološki svetovalni odbor (Technology Advisory Panel), ki zagotavlja strokovne nasvete. Tudi neodvisnost urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil je zaščitena, tako kot neodvisnost pravosodnih pooblaščencev. Urad je samostojen organ (arm's-length body) v okviru ministrstva za notranje zadeve, kar pomeni, da prejema sredstva navedenega ministrstva, vendar svoje naloge opravlja neodvisno ([454]).

(252) Glavne naloge pravosodnih pooblaščencev so določene v členu 229 zakona o preiskovalnih pooblastilih iz leta 2016 ([455]). Pravosodni pooblaščenci imajo predvsem obsežna pooblastila v zvezi s predhodnimi odobritvami, kar je del zaščitnih ukrepov, uvedenih s pravnim okvirom Združenega kraljestva na podlagi zakona o preiskovalnih pooblastilih iz leta 2016. Pravosodni pooblaščenci morajo odobriti odredbe o ciljnem prestrezanju, poseganju v opremo, naborih osebnih podatkov v večjem obsegu, pridobivanju komunikacijskih podatkov v večjem obsegu ter obvestila o hrambi komunikacijskih podatkov ([456]). Poleg tega mora pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil vedno vnaprej odobriti pridobitev komunikacijskih podatkov za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([457]). Če pooblaščenec zavrne odobritev odredbe, se lahko pristojni minister pri pooblaščencu za nadzor pritoži nad izvajanjem preiskovalnih pooblastil, njegova odločitev pa je dokončna.

([447]) V skladu s členom 227(7) in (8) zakona o preiskovalnih pooblastilih iz leta 2016 se pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil šteje za pravosodnega pooblaščenca, skupaj z drugimi pravosodnimi pooblaščenci pa so skupaj imenovani pravosodni pooblaščenci. Trenutno je imenovanih 15 pravosodnih pooblaščencev.

([448]) V skladu s členom 60(2) dela 3 zakona o ustavnih reformah iz leta 2005 (Constitutional Reform Act 2005) izraz „visoka sodna funkcija" pomeni položaj sodnika pri katerem koli od teh sodišč: (i) sodišče Supreme Court, (ii) sodišče Court of Appeal v Angliji in Walesu, (iii) sodišče High Court v Angliji in Walesu, (iv) sodišče Court of Session, (v) sodišče Court of Appeal na Severnem Irskem, (vi) sodišče High Court na Severnem Irskem ali položaj Lord of Appeal in Ordinary.

([449]) Neodvisnost sodstva temelji na tradiciji, splošno priznana pa je od sprejetja zakona Act of Settlement iz leta 1701.

([450]) Člen 227(3) zakona o preiskovalnih pooblastilih iz leta 2016. Pravosodne pooblaščence mora priporočiti tudi pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil, člen 227(4)(e) zakona o preiskovalnih pooblastilih iz leta 2016.

([451]) Člen 238 zakona o preiskovalnih pooblastilih iz leta 2016.

([452]) Člen 227(2) zakona o preiskovalnih pooblastilih iz leta 2016.

([453]) Postopek odpoklica je enak odpoklicu drugih sodnikov v Združenem kraljestvu (glej na primer člen 11(3) zakona o višjih sodiščih iz leta 1981 (Senior Courts Act 1981) in člen 33 zakona o ustavnih reformah iz leta 2005, na podlagi katerih se prav tako zahteva sklep o odobritvi obeh domov parlamenta). Do danes ni bil odpoklican še noben pravosodni pooblaščenec.

([454]) Samostojen organ te vrste je organizacija ali agencija, ki prejema sredstva vlade, vendar lahko deluje neodvisno (več informacij in opredelitev takih organov je na voljo v priročniku kabineta vlade o razvrstitvi javnih organov (Handbook of the Cabinet Office on the classification of Public Bodies), ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf, ter v prvem poročilu zasedanja odbora spodnjega doma parlamenta za javno upravo v obdobju 2014–2015, ki je na voljo na povezavi: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) V skladu s členom 229 zakona o preiskovalnih pooblastilih iz leta 2016 ima pravosodni pooblaščenec obsežna pooblastila za nadzor, ki zajemajo tudi nadzor nad hrambo in razkritjem podatkov, ki jih zberejo obveščevalne agencije.

([456]) Odločitve o tem, ali naj se odobri odločitev pristojnega ministra o izdaji odredbe, sprejemajo pravosodni pooblaščenci sami. Če pooblaščenec zavrne odobritev odredbe, se lahko pristojni minister pri pooblaščencu za nadzor pritoži nad izvajanjem preiskovalnih pooblastil, njegova odločitev pa je dokončna.

([457]) Odobritev pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil je vedno potrebna, kadar se komunikacijski podatki pridobivajo za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (člen 60A zakona o preiskovalnih pooblastilih iz leta 2016). Kadar se komunikacijski podatki pridobivajo za namen nacionalne varnosti, lahko odobritev izda pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil ali imenovani višji uslužbenec zadevnega javnega organa (glej člena 61 in 61A zakona o preiskovalnih pooblastilih iz leta 2016 ter uvodno izjavo (203) zgoraj).

(253) Posebni poročevalec ZN za pravico do zasebnosti je pozdravil vzpostavitev funkcije pravosodnega pooblaščenca na podlagi zakona o preiskovalnih pooblastilih iz leta 2016, v skladu s katerim „morata vse bolj občutljive ali intruzivne zahteve za izvedbo nadzora odobriti višji minister in urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil“. Poudaril je zlasti, da je „ta element sodne presoje [v okviru vloge pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil], ob pomoči skupine inšpektorjev in strokovnjakov za tehnologijo, ki ima na voljo boljše zmogljivosti, eden najpomembnejših novih zaščitnih ukrepov, ki jih je uvedel zakon o preiskovalnih pooblastilih“, saj nadomešča predhodni razdrobljeni sistem organov za nadzor in dopolnjuje vlogo parlamentarnega odbora za obveščevalno in varnostno dejavnost (Intelligence and Security Committee) ter sodišča, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal)“ ([458]).

(254) Poleg tega je pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil pooblaščen za izvajanje naknadnega nadzora nad uporabo preiskovalnih pooblastil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 ([459]), tudi z revizijami, inšpekcijskimi pregledi in preiskavami, ima pa tudi nekatera druga pooblastila in naloge na podlagi ustrezne zakonodaje ([460]) Rezultati takega naknadnega nadzora se vključijo v poročilo, ki ga mora letno pripraviti pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil in ga predložiti predsedniku vlade ([461]), nato pa objaviti in predložiti parlamentu ([462]). Poročilo vsebuje relevantne statistične podatke in informacije o uporabi preiskovalnih pooblastil s strani obveščevalnih agencij in organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter o uporabi zaščitnih ukrepov v zvezi z informacijami, za katere velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko, v zvezi z zaupnim novinarskim gradivom in viri novinarskih informacij, v zvezi z informacijami o sprejeti ureditvi ter v zvezi z operativnimi nameni, ki se uporabljajo glede odredb o ukrepih večjem obsegu. V letnem poročilu urada je navedeno tudi, na katerih področjih so bila javnim organom dana priporočila in kako so jih ti obravnavali ([463]).

(255) V skladu s členom 231 zakona o preiskovalnih pooblastilih iz leta 2016 velja, da če pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil izve za kakršno koli napako, ki jo javni organ stori pri uporabi preiskovalnih pooblastil, mora o tem obvestiti zadevno osebo, če meni, da gre za hudo napako in da je obveščanje osebe v javnem interesu ([464]). Natančneje, člen 231 zakona o preiskovalnih pooblastilih iz leta 2016 določa, da kadar pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil osebo obvesti o napaki, jo mora obvestiti tudi o vseh pravicah, ki jih ima v zvezi s pritožbo pri sodišču, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal), ter zagotoviti vse informacije, ki se pooblaščencu zdijo potrebne za izvrševanje navedenih pravic, če obstaja javni interes za razkritje ([465]).

([458]) Zaključek izjave o opravljeni misiji posebnega poročevalca za pravico do zasebnosti ob zaključku njegove misije v Združenem kraljestvu Velika Britanija in Severna Irska (opomba 281).

([459]) Člen 229 zakona o preiskovalnih pooblastilih iz leta 2016. Preiskovalna in informacijska pooblastila pravosodnega pooblaščenca so določena v členu 235 zakona o preiskovalnih pooblastilih iz leta 2016.

([460]) To vključuje nadzorne ukrepe na podlagi zakona o urejanju preiskovalnih pooblastil iz leta 2000, ki se uporablja v Angliji, Walesu in na Severnem Irskem, izvajanje nalog na podlagi dela 3 zakona o policiji iz leta 1997 (Police Act 1997; odobritev ukrepa v zvezi s premoženjem) in izvrševanje nalog pristojnega ministra na podlagi členov 5 do 7 zakona o obveščevalnih službah iz leta 1994; odredbe o poseganju v brezžično telegrafijo, o vstopu in poseganju v premoženje) (člen 229 zakona o preiskovalnih pooblastilih iz leta 2016).

([461]) Člen 230 zakona o preiskovalnih pooblastilih iz leta 2016. Pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil lahko predsedniku vlade poroča tudi na lastno pobudo o vseh vprašanjih, ki se nanašajo na izvajanje njegovih nalog. Prav tako mora navedeni pooblaščenec predsedniku vlade poročati na njegovo zahtevo, predsednik vlade pa lahko pooblaščencu naroči pregled katerih koli nalog obveščevalnih služb.

([462]) Nekatere dele je mogoče izpustiti, če bi njihova objava škodila nacionalni varnosti.

([463]) V letnem poročilu urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019 (točka 6.38) je na primer navedeno, da je bilo službi MI5 izdano priporočilo, naj spremeni svojo politiko hrambe naborov osebnih podatkov v večjem obsegu, saj bi morala upoštevati sorazmernost hrambe vseh polj v naborih osebnih podatkov v večjem obsegu in vsakega nabora osebnih podatkov v večjem obsegu. Ob koncu leta 2018 urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil ni bil zadovoljen z upoštevanjem tega priporočila, v poročilu za leto 2019 pa je navedeno, da je služba MI5 uvedla nov postopek za upoštevanje te zahteve. V letnem poročilu za leto 2019 (točka 8.22) je navedeno tudi, da je bilo službi GHCQ izdanih več priporočil glede vodenja evidence sorazmernosti iskanj med podatki v večjem obsegu. Poročilo potrjuje, da se je ob koncu leta 2018 praksa na tem področju izboljšala. Letno poročilo urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019, na voljo na povezavi: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Poleg tega se vsako preverjanje javnega organa s strani urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil zaključi s poročilom, ki se predloži organu in vključuje vsa priporočila na podlagi tega pregleda. Urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil nato vsako naslednje preverjanje začne s pregledom priporočil iz zadnjega preverjanja in v novem poročilu o preverjanju navede, ali so bila prejšnja priporočila upoštevana ali se prenesejo naprej.

([464]) Šteje se, da gre za hudo napako, če pooblaščenec meni, da zadevno osebo resno ogroža ali da ji je povzročila večjo škodo (člen 231(2) zakona o preiskovalnih pooblastilih iz leta 2016). Leta 2018 je bilo sporočenih 22 napak, od katerih je bilo osem hudih in je bila zadevna oseba o njih obveščena. Glej letno poročilo urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2018, priloga C (https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). Leta 2019 je bilo hudih napak 14. Glej letno poročilo urada pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2019, priloga C, opomba 463.

([465]) Člen 231 zakona o preiskovalnih pooblastilih iz leta 2016 določa, da mora pooblaščenec za nadzor nad preiskovalnimi pooblastili pri obveščanju osebe o napaki tej zagotoviti tiste informacije, za katere meni, da so potrebne za izvrševanje njenih pravic, pri tem pa mora upoštevati, v kolikšnem obsegu bi bilo razkritje podrobnosti v nasprotju z javnim interesom ali bi ogrožalo preprečevanje oziroma odkrivanje hudih kaznivih dejanj, gospodarsko blaginjo Združenega kraljestva ali nadaljnje izvajanje nalog obveščevalnih služb.

3.3.3.3 Parlamentarni nadzor obveščevalnih služb

(256) Parlamentarni nadzor parlamentarnega odbora za obveščevalno in varnostno dejavnost temelji na zakonu o pravosodju in varnosti iz leta 2013 (Justice and Security Act 2013) ([466]). Z zakonom je bil ustanovljen odbor parlamenta Združenega kraljestva za obveščevalno in varnostno dejavnost. Odboru za obveščevalno in varnostno dejavnost so bila od leta 2013 podeljena večja pooblastila, vključno z nadzorom nad operativnimi dejavnostmi varnostnih služb. V skladu s členom 2 zakona o pravosodju in varnosti iz leta 2013 je naloga tega odbora nadzor nad odhodki, upravljanjem, politiko in operacijami agencij za nacionalno varnost. Zakon o pravosodju in varnosti iz leta 2013 določa, da lahko ta odbor izvaja preiskave o operativnih zadevah, kadar se te ne nanašajo na tekoče operacije ([467]). Memorandum o soglasju, sklenjen med predsednikom vlade ter odborom za obveščevalno in varnostno dejavnost ([468]) podrobno določa elemente, ki jih je treba upoštevati pri presoji, ali je dejavnost del tekoče operacije ([469]). Predsednik vlade lahko navedenemu odboru naroči tudi preiskavo tekočih operacij, poleg tega lahko odbor prouči informacije, ki jih agencije predložijo prostovoljno.

(257) Odbor za obveščevalno in varnostno dejavnost lahko v skladu z dodatkom 1 k zakonu o pravosodju in varnosti iz leta 2013 prosi vodjo katere koli od treh obveščevalnih služb, da razkrije informacije. Služba mora take informacije dati na voljo, razen če pristojni minister vloži veto ([470]). V skladu s pojasnili organov Združenega kraljestva se v praksi odboru za obveščevalno in varnostno dejavnost zelo redko odreče dostop do informacij ([471]).

(258) Odbor za obveščevalno in varnostno dejavnost sestavljajo poslanci zgornjega ali spodnjega doma parlamenta Združenega kraljestva, ki jih imenuje predsednik vlade po posvetovanju z vodjem opozicije ([472]). Pripraviti mora letno poročilo za parlament o izvajanju svojih nalog in druga poročila, ki se mu zdijo ustrezna ([473]). Poleg tega je odbor upravičen, da vsake tri mesece prejme seznam operativnih namenov, ki se uporabljajo za pregled gradiva, pridobljenega v večjem obsegu ([474]). Predsednik vlade odboru za obveščevalno in varnostno dejavnost predloži kopije preiskav, inšpekcijskih ali drugih pregledov pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, če se tema poročil nanaša na zakonska pooblastila odbora ([475]). Odbor lahko pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil tudi prosi, naj izvede preiskavo, pooblaščenec pa mora odbor obvestiti o tem, ali se je odločil izvesti tako preiskavo ali ne ([476]).

(259) Odbor za obveščevalno in varnostno dejavnost je zagotovil tudi vrsto predlogov glede osnutka zakona o preiskovalnih pooblastilih iz leta 2016, ki so bili upoštevani v nazadnje sprejetem besedilu navedenega zakona ([477]). Predlagal je krepitev varstva zasebnosti z uvedbo več zaščitnih ukrepov, ki se uporabljajo pri vseh

([466]) Kot so pojasnili organi Združenega kraljestva, so se z zakonom o pravosodju in varnosti razširile pristojnosti odbora za obveščevalno in varnostno dejavnost, tako da vključujejo tudi nadzor nad obveščevalno skupnostjo, ki presega te tri službe, in omogočajo naknadni nadzor nad operativnimi dejavnostmi služb v zvezi z vprašanji večjega nacionalnega interesa.

([467]) Člen 2 zakona o pravosodju in varnosti iz leta 2013.

([468]) Memorandum o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost je na voljo na povezavi: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Memorandum o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost, točka 14, opomba 468.

([470]) Pristojni minister lahko vloži veto na razkritje informacij le iz dveh razlogov: informacije so občutljive in odboru za obveščevalno in varnostno dejavnost ne smejo biti razkrite zaradi nacionalne varnosti ali je narava informacij taka, da bi se pristojnemu ministru, če bi bil zaprošen, da jih predstavi pred resornim odborom spodnjega doma parlamenta Združenega kraljestva (zaradi razlogov, ki niso omejeni na nacionalno varnost), zdelo ustrezno, da tega ne stori (točka 4(2) dodatka 1 k zakonu o pravosodju in varnosti iz leta 2013).

([471]) UK Explanatory Framework for Adequacy Discussions, section H: National Security, stran 43, opomba 31.

([472]) Člen 1 zakona o pravosodju in varnosti iz leta 2013. Ministri ne morejo biti člani. Člani opravljajo funkcije v odboru za obveščevalno in varnostno dejavnost do konca mandata parlamenta, v času katerega so bili imenovani. Odpoklicani so lahko, če to potrdi dom parlamenta, ki jih je imenoval, ali če prenehajo biti poslanci ali prevzamejo vlogo nižjega ministra. Član lahko tudi odstopi.

([473]) Poročila in izjave odbora so na voljo na povezavi: https://isc.independent.gov.uk/publications/. Odbor za obveščevalno in varnostno dejavnost je leta 2015 izdal poročilo z naslovom Privacy and Security: A modern and transparent legal framework (glej: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), v katerem je proučil pravni okvir za tehnike nadzora, ki jih uporabljajo obveščevalne službe, ter izdal vrsto priporočil, ki so bila nato proučena in vključena v osnutek predloga zakona o preiskovalnih pooblastilih, ki je bil pozneje sprejet kot zakon o preiskovalnih pooblastilih iz leta 2016. Odgovori vlade na navedeno poročilo so na voljo na povezavi: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) Členi 142, 161 in 183 zakona o preiskovalnih pooblastilih iz leta 2016.

([475]) Člen 234 zakona o preiskovalnih pooblastilih iz leta 2016.

([476]) Člen 236 zakona o preiskovalnih pooblastilih iz leta 2016.

([477]) Parlamentarni odbor za obveščevalno in varnostno dejavnost, Report on the draft Investigatory Powers Bill (poročilo o osnutku predloga zakona o preiskovalnih pooblastilih), na voljo na povezavi: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

preiskovalnih pooblastilih ([478]). Predlagal je tudi spremembe predlaganih zmogljivosti glede poseganja v opremo, naborov osebnih podatkov v večjem obsegu in komunikacijskih podatkov, ter zahteval druge specifične spremembe za krepitev omejitev in zaščitnih ukrepov pri uporabi preiskovalnih pooblastil ([479]).

3.3.4 *Pravna sredstva*

(260) V zvezi z dostopom vlade zaradi nacionalne varnosti morajo imeti posamezniki, na katere se nanašajo osebni podatki, možnost uveljavljanja pravnih sredstev pred neodvisnim in nepristranskim sodiščem, da si zagotovijo dostop do svojih osebnih podatkov ali da dosežejo popravo oziroma izbris takih podatkov ([480]). Tak pravosodni organ mora predvsem imeti pristojnost za sprejemanje zavezujočih odločitev glede obveščevalnih služb ([481]). Kot je pojasnjeno v uvodnih izjavah (261) do (271), je v Združenem kraljestvu posameznikom, na katere se nanašajo osebni podatki, na voljo več poti sodnega varstva, v okviru katerih lahko uveljavljajo taka pravna sredstva.

3.3.4.1 Mehanizmi pravnih sredstev, ki so na voljo na podlagi dela 4 zakona o varstvu podatkov

(261) Na podlagi člena 165 zakona o varstvu podatkov iz leta 2018 ima posameznik, na katerega se nanašajo osebni podatki, pravico vložiti pritožbo pri informacijskem pooblaščencu, če meni, da je v zvezi z osebnimi podatki, ki se nanašajo nanj, prišlo do kršitve dela 4 zakona o varstvu podatkov iz leta 2018. Informacijski pooblaščenec lahko preveri, kako upravljavec in obdelovalec zagotavljata skladnost z zakonom o varstvu podatkov iz leta 2018 in od njiju zahteva, da sprejmeta potrebne ukrepe. Poleg tega so posamezniki v skladu z delom 4 zakona o varstvu podatkov iz leta 2018 upravičeni, da pri sodišču High Court (ali sodišču Court of Session na Škotskem) vložijo predlog za izdajo odločbe, ki od upravljavca zahteva, da upošteva pravice do dostopa do podatkov ([482]), do ugovora obdelavi ([483]) in do popravka ali izbrisa ([484]).

(262) Posamezniki so prav tako upravičeni zahtevati odškodnino za škodo, ki nastane zaradi kršitve zahteve iz dela 4 zakona o varstvu podatkov iz leta 2018 s strani upravljavca ali obdelovalca ([485]). Škoda vključuje finančno in nefinančno izgubo, kot je na primer stiska ([486]).

3.3.4.2 Mehanizmi pravnih sredstev, ki so na voljo na podlagi zakona o preiskovalnih pooblastilih iz leta 2016

(263) Posamezniki lahko zaradi kršitev zakona o preiskovalnih pooblastilih iz leta 2016 vložijo pravna sredstva pri sodišču, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal).

(264) Navedeno sodišče je bilo vzpostavljeno na podlagi zakona o urejanju preiskovalnih pooblastil iz leta 2000 in je neodvisno od izvršilne veje oblasti ([487]). V skladu s členom 65 navedenega zakona člane tega sodišča imenuje kraljica za obdobje petih let. Člana tega sodišča lahko s funkcije razreši kraljica, na podlagi nagovora ([488]) obeh domov parlamenta ([489]).

([478]) Te splošne obveznosti v zvezi z zasebnostjo so zdaj določene v členu 2(2) zakona o preiskovalnih pooblastilih iz leta 2016, ki določa, da mora javni organ, ki deluje na podlagi navedenega zakona, upoštevati, ali bi bilo mogoče cilj odredbe, odobritve ali obvestila razumno doseči z drugimi, manj intruzivnimi sredstvi; ali se glede pridobivanja informacij na podlagi odredbe, odobritve ali obvestila uporablja višja raven varstva zaradi posebne občutljivosti informacij; javni interes glede celovitosti in varnosti telekomunikacijskih sistemov in poštnih storitev ter vse druge vidike javnega interesa v zvezi z varstvom zasebnosti.

([479]) V skladu z zahtevo odbora za obveščevalno in varnostno dejavnost se je na primer število dni veljavnosti „nujne“ odredbe, preden se jo predloži pravosodnemu pooblaščencu v odobritev, zmanjšalo s petih na tri delovne dni, odbor za obveščevalno in varnostno dejavnost pa je dobil pristojnost zadevo predložiti pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil v preiskavo.

([480]) Sodba v zadevi Schrems II, točka 194.

([481]) Sodba v zadevi Schrems II, točka 197.

([482]) Člen 94(11) zakona o varstvu podatkov iz leta 2018.

([483]) Člen 99(4) zakona o varstvu podatkov iz leta 2018.

([484]) Člen 100(1) zakona o varstvu podatkov iz leta 2018.

([485]) Člen 169 zakona o varstvu podatkov iz leta 2018 dopušča zahtevke „osebe, ki utrpi škodo zaradi kršitve zahteve iz zakonodaje o varstvu podatkov“. Iz informacij organov Združenega kraljestva izhaja, da se v praksi zahtevek ali pritožba zoper obveščevalno službo običajno vloži pri sodišču, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal), saj ima to široka pooblastila, lahko dodeli odškodnino, vložitev zahtevka pa ni povezana s stroški.

([486]) Člen 169(5) zakona o varstvu podatkov iz leta 2018.

([487]) V skladu z dodatkom 3 k zakonu o urejanju preiskovalnih pooblastil iz leta 2000 morajo imeti člani določene izkušnje v pravosodju in so lahko ponovno imenovani.

([488]) Nagovor (Address) je predlog, predložen parlamentu, katerega namen je monarha opozoriti na stališča parlamenta o posameznem vprašanju.

([489]) Točka 1(5) dodatka 3 k zakonu o urejanju preiskovalnih pooblastil iz leta 2000.

(265) V skladu s členom 65 zakona o urejanju preiskovalnih pooblastil iz leta 2000 je sodišče ustrezen pravosodni organ za vse pritožbe oseb, ki jih je prizadelo ravnanje na podlagi zakona o preiskovalnih pooblastilih iz leta 2016, zakona o urejanju preiskovalnih pooblastil iz leta 2000 ali katero koli ravnanje obveščevalnih služb ([490]).

(266) Da lahko posameznik vloži tožbo pri sodišču, ki obravnava preiskovalna pooblastila („procesno upravičenje"), mora biti v skladu s členom 65 zakona o urejanju preiskovalnih pooblastil iz leta 2000 prepričan ([491]), da je obveščevalna služba izvajala dejavnosti v zvezi z njim, njegovim premoženjem, komunikacijami, ki jih je poslal ali so mu bile poslane ali namenjene, ali njegovo uporabo poštnih storitev, telekomunikacijskih storitev ali telekomunikacijskega sistema ([492]). Poleg tega mora biti tožnik prepričan, da je bilo ravnanje izvedeno v „spornih okoliščinah" ([493]) ali „da ga je izvedla obveščevalna služba ali je bilo izvedeno v njenem imenu" ([494]). Ker se je zlasti ta standard prepričanja razlagal precej široko ([495]), se za predložitev zadeve navedenemu sodišču zahteva nizek prag procesnega upravičenja.

(267) Sodišče, ki obravnava preiskovalna pooblastila, mora pri obravnavanju vložene tožbe proučiti, ali so imele osebe, zoper katere je vložena tožba, odnos s tožnikom ter kako je ravnal organ, ki je domnevno vpleten v kršitve, in ali je bilo domnevno ravnanje storjeno ([496]). Kadar sodišče, ki obravnava preiskovalna pooblastila, vodi postopek, mora pri sprejemanju odločitve v tem postopku uporabiti ista načela, kot bi jih uporabilo sodišče na podlagi zahteve za sodno presojo ([497]). Poleg tega morajo naslovniki odredb ali obvestil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 ter vse druge osebe, ki imajo državno funkcijo, so zaposlene pri policiji ali pri pooblaščencu za obravnavo pritožb zoper policijo (Police Investigations and Review Commissioner), navedenemu sodišču razkriti ali predložiti vse dokumente in informacije, ki jih sodišče zahteva z namenom izvajanja svojih pristojnosti ([498]).

(268) Sodišče, ki obravnava preiskovalna pooblastila, mora tožnika obvestiti, ali je bila sprejeta odločitev v njegovo korist ali ne ([499]). Sodišče, ki obravnava preiskovalna pooblastila, lahko v skladu s členom 67(6) in (7) zakona o urejanju preiskovalnih pooblastil iz leta 2000 izdaja začasne odločbe in priznava odškodnine ali izdaja druge odločbe, ki se mu zdijo primerne. To lahko vključuje odločbo o razveljavitvi ali odpravi vsake odredbe ali pooblastila ter odločbo

([490]) Člen 65(5) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([491]) Glede standarda preskusa „prepričanja" glej zadevo Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH, točka 41. V tej zadevi je sodišče, ki obravnava preiskovalna pooblastila, s sklicevanjem na sodno prakso Evropskega sodišča za človekove pravice navedlo, da je treba preveriti, ali je zatrjevano prepričanje, da je obveščevalna služba storila ravnanje, ki spada v podčlen 68(5) zakona o urejanju preiskovalnih pooblastil iz leta 2000 oziroma je bilo storjeno v njenem imenu, res utemeljeno, tako da lahko posameznik na tej podlagi trdi, da je žrtev kršitve, ki jo povzroči že sam obstoj tajnih ukrepov ali zakonodaje, ki dovoljuje tajne ukrepe, le, če dokaže, da bi zaradi svojega osebnega položaja lahko bil izpostavljen takim ukrepom.

([492]) Člen 65(4)(a) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([493]) Take okoliščine se nanašajo na ravnanje javnih organov na podlagi pooblastila (npr. odredba, odobritev/obvestilo o pridobitvi podatkov o komunikacijah itd.) ali v primeru okoliščin (ne glede na to, ali tako pooblastilo obstaja ali ne), v katerih ravnanje ne bi bilo ustrezno brez pooblastila ali vsaj brez ustrezne proučitve, ali bi bilo tako pooblastilo potrebno. Ravnanje, ki ga odobri pravosodni pooblaščenec, se obravnava kot ravnanje, storjeno v spornih okoliščinah (člen 65(7ZA) zakona o urejanju preiskovalnih pooblastil iz leta 2000), medtem ko se za druga ravnanja, storjena z dovoljenjem osebe, ki opravlja sodno funkcijo, šteje, da niso bila storjena v spornih okoliščinah (člen 65(7) in (8) zakona o urejanju preiskovalnih pooblastil iz leta 2000).

([494]) Iz informacij organov Združenega kraljestva izhaja, da glede na nizek prag za vložitev tožbe ni nenavadno, da sodišče ugotovi, da javni organ dejansko ni nikoli preiskoval tožnika. V zadnjem statističnem poročilu sodišča, ki obravnava preiskovalna pooblastila, je navedeno, da je to sodišče leta 2016 prejelo 209 tožb, od katerih jih je bilo 52 % neresnih ali zlonamernih, pri 25 % pa ni bilo mogoče podati ugotovitve. Organi Združenega kraljestva so pojasnili, da to pomeni, da v zvezi s tožnikom niso bile uporabljene prikrite dejavnosti/pooblastila ali pa so bile uporabljene prikrite metode, vendar je sodišče ugotovilo, da so bile zakonite. Poleg tega je bilo v 11 % tožb ugotovljeno, da sodišče zanje ni pristojno, da so bile umaknjene ali da so neveljavne, 5 % tožb ni bilo vloženih pravočasno, v 7 % pa je bilo odločeno v korist tožnika. Statistično poročilo sodišča, ki obravnava preiskovalna pooblastila, iz leta 2016, je na voljo na povezavi: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Glej sodbo v zadevi Human Rights Watch v Secretary of State [2016] UKIPTrib15_165-CH. V tej zadevi je sodišče, ki obravnava preiskovalna pooblastila, s sklicevanjem na sodno prakso Evropskega sodišča za človekove pravice navedlo, da je treba preveriti, ali je zatrjevano prepričanje, da je obveščevalna služba storila ravnanje, ki spada v podčlen 68(5) zakona o urejanju preiskovalnih pooblastil iz leta 2000 oziroma je bilo storjeno v njenem imenu, res utemeljeno, tako da lahko posameznik na tej podlagi trdi, da je žrtev kršitve, ki jo povzroči že sam obstoj tajnih ukrepov ali zakonodaje, ki dovoljuje tajne ukrepe, le, če dokaže, da bi zaradi svojega osebnega položaja lahko bil izpostavljen takim ukrepom (glej zadevo Human Rights Watch v Secretary of State, točka 41).

([496]) Člen 67(3) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([497]) Člen 67(2) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([498]) Člen 68(6) in (7) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([499]) Člen 68(4) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

o uničenju vseh evidenc informacij, pridobljenih pri izvrševanju katerih koli pooblastil na podlagi odredbe, odobritve ali obvestila, ali informacij, ki jih ima o kateri koli osebi kateri koli javni organ na drugi podlagi ([500]). V skladu s členom 67A zakona o urejanju preiskovalnih pooblastil iz leta 2000 se je mogoče pritožiti zoper odločitev sodišča, ki obravnava preiskovalna pooblastila, in sicer na podlagi dovoljenja tega sodišča ali ustreznega pritožbenega sodišča.

(269) Treba je tudi omeniti, da se je o vlogi sodišča, ki obravnava preiskovalna pooblastila, večkrat razpravljalo v okviru tožb pred Evropskim sodiščem za človekove pravice, zlasti v zadevi Kennedy v. the United Kingdom ([501]) in nedavno v zadevi Big Brother Watch and others v. United Kingdom ([502]), v kateri je Sodišče navedlo, da je „sodišče, ki obravnava preiskovalna pooblastila, vsem, ki so sumili, da so obveščevalne službe prestregle njegovo komunikacijo, ponudilo zanesljiva pravna sredstva“ ([503]).

3.3.4.3 Drugi razpoložljivi mehanizmi pravnih sredstev

(270) Kot je pojasnjeno v uvodnih izjavah (109) do (111), so pravna sredstva na podlagi zakona o človekovih pravicah iz leta 1998 in Sodišča za človekove pravice ([504]) na voljo tudi na področju nacionalne varnosti. Na podlagi člena 65(2) zakona o urejanju preiskovalnih pooblastil iz leta 2000 je sodišče, ki obravnava preiskovalna pooblastila, izključno pristojno za obravnavo vseh zahtevkov na podlagi zakona o človekovih pravicah v zvezi z obveščevalnimi agencijami ([505]). Kot je navedlo sodišče High Court, to pomeni, da „lahko o tem, ali je bil na podlagi dejstev v posamezni zadevi kršen zakon o človekovih pravicah, načeloma odloča neodvisno sodišče, ki lahko ima dostop do vsega ustreznega gradiva, tudi tajnega. […] Pri tem upoštevamo tudi, da se je zoper odločitev sodišča, ki obravnava preiskovalna pooblastila, zdaj mogoče pritožiti pri ustreznem pritožbenem sodišču (v Angliji in Walesu je to sodišče Court of Appeal); sodišče Supreme Court pa je pred kratkim ugotovilo, da je načeloma mogoče zahtevati sodno presojo zoper odločitve sodišča, ki obravnava preiskovalna pooblastila: glej sodbo v zadevi R (Privacy International) v Investigatory Powers Tribunal [2019] UKSC 22, [2019] 2 WLR 1219“ ([506]).

(271) Iz zgoraj navedenega izhaja, da kadar organi Združenega kraljestva za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ali za nacionalno varnost izvajajo dostop do osebnih podatkov, ki spadajo na področje uporabe tega sklepa, tak dostop ureja zakonodaja, ki določa pogoje, na podlagi katerih je dostop mogoč, pri tem pa omejuje dostop in nadaljnjo uporabo podatkov na tisto, kar je potrebno in sorazmerno glede na cilj preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali nacionalne varnosti. Nadalje, za tak dostop je v več primerih potrebna predhodna odobritev pravosodnega organa v obliki odobritve odredbe ali odredbe o predložitvi dokazov, v vsakem primeru pa je podvržen neodvisnemu nadzoru. Ko javni organi pridobijo dostop do podatkov, za vso obdelavo, vključno z nadaljnjo izmenjavo in pošiljanjem, veljajo posebni zaščitni ukrepi glede varstva podatkov, in sicer glede obdelave s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj na podlagi dela 3 zakona o varstvu podatkov iz leta 2018, ki odražajo tiste iz Direktive (EU) 2016/680, in glede obdelave s strani obveščevalnih agencij na podlagi dela 4 zakona o varstvu podatkov iz leta 2018. Nazadnje, posamezniki, na katere se nanašajo osebni podatki, imajo na tem področju učinkovito upravno in sodno varstvo, vključno s pravico do dostopa do svojih podatkov ter pravico do popravka ali izbrisa podatkov.

(272) Glede na pomen takih pogojev, omejitev in zaščitnih ukrepov za namene tega sklepa bo Komisija pozorno spremljala uporabo in razlago pravil Združenega kraljestva, ki določajo vladni dostop do podatkov. To bo vključevalo ustrezen razvoj zakonodaje, predpisov in sodne prakse ter dejavnosti urada informacijskega pooblaščenca in drugih nadzornih organov na tem področju. Posebna pozornost bo namenjena tudi izvajanju

([500]) Primer uporabe takih pooblastil je zadeva Liberty & Others proti the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Sodišče je odločilo v korist obeh tožnikov, ker je v enem primeru hramba njune komunikacije presegala vzpostavljene omejitve, v drugem primeru pa, ker postopek pregleda ni bil izveden v skladu z notranjimi pravili službe GCHQ. V prvem primeru je sodišče obveščevalnim službam odredilo uničenje komunikacij, ki so bile hranjene dlje od zadevnega roka. V drugem primeru odločba o uničenju ni bila izdana, ker komunikacija ni bila shranjena.

([501]) Kennedy, opomba 129.

([502]) Sodba Evropskega sodišča za človekove pravice v zadevi Big Brother Watch and others v United Kingdom (glej opombo 268), točke 413–415.

([503]) Evropsko sodišče za človekove pravice, Big Brother Watch, točka 425.

([504]) Kot je na primer razvidno iz nedavne sodbe velikega senata Evropskega sodišča za človekove pravice v zadevi Big Brother Watch and others v United Kingdom (glej opombo 279), to omogoča učinkovit sodni nadzor – podoben tistemu, ki velja za države članice EU – s strani mednarodnega sodišča nad spoštovanjem temeljnih pravic s strani javnih organov pri dostopu do osebnih podatkov. Poleg tega je izvrševanje sodb Evropskega sodišča za človekove pravice pod posebnim nadzorom Sveta Evrope.

([505]) V zadevi Belhaj & others [2017] UKSC 3 je nezakonitost prestrezanja gradiva, za katerega velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko, temeljila neposredno na členu 8 EKČP (glej točko 11).

([506]) Sodišče High Court of Justice, zadeva Liberty, [2019] EWHC 2057 (Admin), točka 170.

relevantnih sodb Evropskega sodišča za človekove pravice s strani Združenega kraljestva, vključno z ukrepi, opredeljenimi v „akcijskih načrtih“ in „poročilih o ukrepih“, predloženih odboru ministrov v okviru nadzora nad spoštovanjem sodb Sodišča.

4. **SKLEPNA UGOTOVITEV**

(273) Komisija meni, da UK GDPR in zakon o varstvu podatkov iz leta 2018 zagotavljata raven varstva osebnih podatkov, ki se prenašajo iz Evropske unije, ki je v osnovi enakovredna ravni, ki jo zagotavlja Uredba (EU) 2016/679.

(274) Poleg tega Komisija meni, da gledano v celoti nadzorni mehanizmi in pravna sredstva v pravu Združenega kraljestva v praksi omogočajo, da se kršitve ugotovijo in kaznujejo, ter da so posameznikom, na katere se nanašajo osebni podatki, na voljo pravna sredstva, s katerimi lahko pridobijo dostop do osebnih podatkov, ki se nanašajo nanje, in po potrebi zagotovijo popravek ali izbris takih podatkov.

(275) Komisija glede na razpoložljive informacije o pravnem redu Združenega kraljestva nazadnje meni, da so vsi posegi v temeljne pravice posameznikov, katerih osebne podatke iz Evropske unije v Združeno kraljestvo prenašajo javni organi Združenega kraljestva v imenu javnega interesa, zlasti za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in namene nacionalne varnosti, omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, ter da obstaja učinkovita pravna zaščita zoper take posege.

(276) Zato bi bilo treba glede na ugotovitve iz tega sklepa odločiti, da Združeno kraljestvo zagotavlja ustrezno raven varstva v smislu člena 45 Uredbe (EU) 2016/679, kot se razlaga glede na Listino EU o temeljnih pravicah.

(277) Ta ugotovitev temelji na ustrezni nacionalni ureditvi Združenega kraljestva in njegovih mednarodnih zavezah, zlasti zavezanosti Evropski konvenciji o varstvu človekovih pravic ter priznanju pristojnosti Evropskega sodišča za človekove pravice. Nadaljnja zavezanost takim mednarodnim obveznostim je torej posebej pomemben element ocene, na kateri temelji ta sklep.

5. **UČINKI TEGA SKLEPA IN UKREPI ORGANOV ZA VARSTVO PODATKOV**

(278) Države članice in njihovi organi morajo sprejeti ukrepe, potrebne za zagotavljanje skladnosti z akti institucij Unije, saj se domneva, da so ti zakoniti in imajo pravne učinke, dokler njihova veljavnost ne poteče, dokler niso umaknjeni, razveljavljeni na podlagi izpodbojne tožbe ali razglašeni za neveljavne na podlagi predloga za sprejetje predhodne odločbe ali sklicevanja na nezakonitost.

(279) Zato je sklep Evropske komisije o ustreznosti varstva, sprejet na podlagi člena 45(3) Uredbe (EU) 2016/679, zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z njihovimi neodvisnimi nadzornimi organi. V obdobju uporabe tega sklepa prenosi med upravljavcem ali obdelovalcem v Evropski uniji in upravljavci ali obdelovalci v Združenem kraljestvu lahko potekajo, ne da bi bilo treba pridobiti nadaljnje dovoljenje.

(280) V skladu s členom 58(5) Uredbe (EU) 2016/679 in glede na pojasnila Sodišča EU v sodbi v zadevi Schrems ([507]) je treba opozoriti, da če ima nacionalni organ za varstvo podatkov, tudi po prejemu pritožbe, pomisleke o skladnosti sklepa Komisije o ustreznosti s temeljnimi pravicami posameznika do zasebnosti in varstva podatkov, mu mora nacionalno pravo zagotavljati pravno sredstvo za predložitev teh ugovorov nacionalnemu sodišču, od katerega se lahko zahteva, da v primeru dvomov prekine postopek in Sodišču EU predloži predlog za sprejetje predhodne odločbe ([508]).

([507]) Sodba v zadevi Schrems, točka 65.

([508]) Sodba v zadevi Schrems, točka 65. „V zvezi s tem mora nacionalni zakonodajalec določiti pravna sredstva, ki zadevnemu nacionalnemu nadzornemu organu omogočajo, da nacionalnim sodiščem predloži očitke, ki jih šteje za utemeljene, da lahko ta, če dvomijo o veljavnosti sklepa Komisije, sprožijo postopek predhodnega odločanja za preizkus veljavnosti navedenega sklepa.“

6. SPREMLJANJE, ZAČASNO ZADRŽANJE IZVAJANJA, RAZVELJAVITEV ALI SPREMEMBA TEGA SKLEPA

(281) Komisija v skladu s členom 45(4) Uredbe (EU) 2016/679 redno spremlja razvoj dogodkov v Združenem kraljestvu po sprejetju tega sklepa, da lahko presodi, ali še vedno zagotavlja v osnovi enakovredno raven varstva. Tako spremljanje je pomembno zlasti v tem primeru, saj bo Združeno kraljestvo upravljalo, uporabljalo in izvajalo novo ureditev varstva podatkov, za katero se ne uporablja več pravo Evropske unije in se bo morda spremenilo. V zvezi s tem bo posebna pozornost namenjena praktični uporabi pravil Združenega kraljestva o prenosu osebnih podatkov v tretje države in vplivu, ki ga lahko ima na raven varstva podatkov, prenesenih v skladu s tem sklepom, učinkovitost uveljavljanja pravic posameznikov, vključno z vsemi relevantnimi spremembami v zakonodaji in praksi v zvezi z izjemami ali omejitvami teh pravic (zlasti tiste, ki se nanaša na ohranjanje učinkovitega nadzora priseljevanja), ter spoštovanje omejitev in zaščitnih ukrepov v zvezi z vladnim dostopom. Spremljanje s strani Komisije bosta med drugim odvisna od razvoja sodne prakse in nadzora s strani urada informacijskega pooblaščenca in drugih neodvisnih organov.

(282) Da bi olajšali to spremljanje, bi morali organi Združenega kraljestva Komisijo nemudoma obvestiti o vseh bistvenih spremembah pravnega reda Združenega kraljestva, ki vplivajo na pravni okvir, ki je predmet tega sklepa, ter o razvoju praks v zvezi z obdelavo osebnih podatkov, ocenjenih v tem sklepu, in sicer tako glede obdelave osebnih podatkov s strani upravljavcev in obdelovalcev v skladu z UK GDPR kot tudi glede omejitev in zaščitnih ukrepov, ki se uporabljajo za dostop javnih organov do osebnih podatkov. To bi moralo vključevati razvoj elementov iz uvodne izjave (281).

(283) Poleg tega bi morale države članice Komisijo obveščati o vseh pomembnih ukrepih nacionalnih organov za varstvo podatkov, zlasti glede poizvedb ali pritožb posameznikov iz EU, na katere se nanašajo osebni podatki, v zvezi s prenosom osebnih podatkov iz Unije upravljavcem ali obdelovalcem v Združenem kraljestvu, da lahko Komisija učinkovito izvaja naloge spremljanja. Evropska komisija bi morala biti obveščena tudi o vseh indicih, da ukrepi javnih organov Združenega kraljestva, odgovornih za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj oziroma za nacionalno varnost, vključno z vsemi nadzornimi organi, ne zagotavljajo zahtevane ravni varnosti.

(284) Kadar razpoložljive informacije, zlasti informacije, ki izhajajo iz spremljanja tega sklepa ali ki jih zagotovijo organi Združenega kraljestva ali držav članic, pokažejo, da raven varstva, ki jo zagotavlja Združeno kraljestvo, morda ni več ustrezna, bi morala Komisija o tem nemudoma obvestiti pristojne organe Združenega kraljestva in zahtevati, da se sprejmejo ustrezni ukrepi v določenem roku, ki ne sme biti daljši od treh mesecev. Po potrebi se lahko to obdobje podaljša za določeno obdobje ob upoštevanju narave posamezne zadeve in/ali ukrepov, ki naj bi se sprejeli. Tak postopek bi se na primer sprožil v primerih, ko nadaljnji prenosi, tudi na podlagi novih predpisov o ustreznosti, ki jih sprejme pristojni minister, ali mednarodnih sporazumov, ki jih sklene Združeno kraljestvo, ne bi bili več izvedeni v okviru zaščitnih ukrepov, ki zagotavljajo neprekinjeno varstvo v smislu člena 44 Uredbe (EU) 2016/679.

(285) Če pristojni organi Združenega kraljestva ob preteku tega določenega roka ne sprejmejo navedenih ukrepov ali drugače zadovoljivo dokažejo, da ta sklep še temelji na ustrezni ravni varnosti, bo Komisija začela postopek iz člena 93(2) Uredbe (EU) 2016/679 za začasno zadržanje izvajanja ali za razveljavitev dela ali celotnega tega sklepa.

(286) Druga možnost je, da bo Komisija začela postopek za spremembo tega sklepa, in sicer uvedbo dodatnih pogojev za prenos podatkov ali z omejitvijo področja uporabe ugotovitve o ustreznosti varstva samo na prenose podatkov, za katere je še naprej zagotovljena ustrezna raven varstva.

(287) Komisija bo v nujnih ustrezno utemeljenih primerih uporabila možnost, da v skladu s postopkom iz člena 93(3) Uredbe (EU) 2016/679 sprejme izvedbene akte, ki se začnejo uporabljati takoj in s katerimi se začasno zadrži izvajanje tega sklepa oziroma se sklep razveljavi ali spremeni.

7. TRAJANJE IN PODALJŠANJE VELJAVNOSTI TEGA SKLEPA

(288) Komisija mora upoštevati, da bo Združeno kraljestvo ob izteku prehodnega obdobja, določenega v sporazumu o izstopu, in takoj po prenehanju uporabe začasne določbe iz člena 782 sporazuma o trgovini in sodelovanju med EU in Združenim kraljestvom uveljavilo, uporabljalo in izvajalo novo ureditev varstva podatkov, ne pa več ureditve, ki je bila vzpostavljena, ko ga je še zavezovalo pravo Evropske unije. To lahko vključuje zlasti dopolnitve ali spremembe okvira varstva podatkov, ki se ocenjuje v tem sklepu, ter druge spremembe.

(289) Zato je primerno določiti, da ta sklep velja štiri leta od začetka njegove veljavnosti.

(290) Kadar zlasti iz informacij, ki izhajajo iz spremljanja izvajanja tega sklepa, izhaja, da so ugotovitve, ki se nanašajo na ustreznost ravni varstva, ki se zagotavlja v Združenem kraljestvu, še vedno dejansko in pravno upravičene, bi morala Komisija najpozneje šest mesecev pred prenehanjem uporabe tega sklepa začeti postopek za spremembo tega sklepa, tako da se veljavnost načeloma podaljša za dodatna štiri leta. Vsak tak izvedbeni akt, ki spreminja ta sklep, mora biti sprejet v skladu s postopkom iz člena 93(2) Uredbe (EU) 2016/679.

8. **SKLEPNE UGOTOVITVE**

(291) Evropski odbor za varstvo podatkov je objavil svoje mnenje ([509]), ki je bilo upoštevano pri pripravi tega sklepa.

(292) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 93 Uredbe (EU) 2016/679 –

SPREJELA NASLEDNJI SKLEP:

Člen 1

1. Za namene člena 45 Uredbe (EU) 2016/679 se šteje, da Združeno kraljestvo zagotavlja ustrezno raven varstva osebnih podatkov, ki se v okviru področja Uredbe (EU) 2016/679 prenašajo iz Evropske unije v Združeno kraljestvo.

2. Ta sklep se ne nanaša na osebne podatke, ki se prenašajo za namene nadzora priseljevanja v Združeno kraljestvo ali ki sicer spadajo na področje uporabe izjeme glede nekaterih pravic posameznikov, na katere se nanašajo osebni podatki, za namene vzdrževanja učinkovitega nadzora priseljevanja v skladu z odstavkom 4(1) dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

Člen 2

Kadar pristojni nadzorni organi držav članic zaradi varstva posameznikov pri obdelavi njihovih osebnih podatkov izvajajo svoja pooblastila na podlagi člena 58 Uredbe (EU) 2016/679 v zvezi s prenosom podatkov, ki spadajo na področje uporabe iz člena 1, morajo zadevne države članice o tem brez odlašanja obvestiti Komisijo.

Člen 3

1. Komisija stalno spremlja uporabo pravnega okvira, na katerem temelji ta sklep, vključno s pogoji, pod katerimi se izvajajo nadaljnji prenosi in uveljavljajo individualne pravice ter pod katerimi imajo javni organi Združenega kraljestva dostop do podatkov, prenesenih na podlagi tega sklepa, da bi ocenila, ali Združeno kraljestvo še naprej zagotavlja ustrezno raven varstva v smislu člena 1.

2. Države članice in Komisija se medsebojno obveščajo o primerih, ko informacijski pooblaščenec ali kateri koli drug pristojni organ Združenega kraljestva ne zagotovi skladnosti s pravnim okvirom, na katerem temelji ta sklep.

3. Države članice in Komisija se medsebojno obveščajo o vseh indicih, da posegi javnih organov Združenega kraljestva v pravico posameznikov do varstva njihovih osebnih podatkov presegajo tisto, kar je nujno potrebno, ali da zoper take posege ni učinkovitega pravnega varstva.

4. Če Komisija utemeljeno sumi, da ustrezna raven varstva ni več zagotovljena, o tem obvesti pristojne organe Združenega kraljestva in lahko začasno zadrži izvajanje tega sklepa, ga razveljavi ali spremeni.

([509]) Mnenje 14/2021 o osnutku izvedbenega sklepa Evropske komisije v skladu z Uredbo (EU) 2016/679 o ustreznem varstvu osebnih podatkov v Združenem kraljestvu, ki je na voljo na naslednji povezavi: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komisija lahko začasno zadrži izvajanje tega sklepa, ga razveljavi ali spremeni tudi, če zaradi nesodelovanja vlade Združenega kraljestva ne more ugotoviti, ali obstaja vpliv na ugotovitev iz člena 1(1).

Člen 4

Ta sklep preneha veljati 27. junija 2025, razen če se podaljša v skladu s postopkom iz člena 93(2) Uredbe (EU) 2016/679.

Člen 5

Ta sklep je naslovljen na države članice.

V Bruslju, 28. junija 2021

Za Komisijo
Didier REYNDERS
Član Komisije

IZVEDBENI SKLEP KOMISIJE (EU) 2021/1773

z dne 28. junija 2021

v skladu z Direktivo (EU) 2016/680 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu

(notificirano pod dokumentarno številko C(2021) 4801)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ ([1]) in zlasti člena 36(3) Direktive,

ob upoštevanju naslednjega:

1. **UVOD**

(1) Direktiva (EU) 2016/680 določa pravila za prenos osebnih podatkov od pristojnih organov v Uniji v tretje države in mednarodne organizacije, če taki prenosi spadajo na področje uporabe navedene direktive. Pravila o mednarodnih prenosih podatkov s strani pristojnih organov so določena v poglavju V Direktive (EU) 2016/680, natančneje v členih 35 do 40. Čeprav je za učinkovito sodelovanje na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ključen pretok osebnih podatkov v države zunaj Evropske unije in iz njih, je treba zagotoviti, da s takimi prenosi ni ogrožena raven varstva osebnih podatkov, ki se zagotavlja v Evropski uniji ([2]).

(2) V skladu s členom 36(3) Direktive (EU) 2016/680 lahko Komisija z izvedbenim aktom sklene, da tretja država, ozemlje ali eden ali več določenih sektorjev v zadevni tretji državi ali mednarodna organizacija zagotavlja ustrezno raven varstva. Na podlagi tega pogoja se lahko prenosi osebnih podatkov v tretjo državo izvedejo, ne da bi bilo treba pridobiti dodatno dovoljenje (razen če mora druga država članica, iz katere so bili podatki pridobljeni, dati svoje soglasje za prenos), kot je določeno v členu 35(1) in uvodni izjavi 66 Direktive (EU) 2016/680.

(3) Kot je določeno v členu 36(2) Direktive (EU) 2016/680, mora sprejetje sklepa o ustreznosti temeljiti na celoviti analizi pravnega reda tretje države. Komisija mora v oceni opredeliti, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, zagotovljeni v Evropski uniji (uvodna izjava 67 Direktive (EU) 2016/680). Standard, po katerem se ocenjuje dejstvo, da je raven varstva „v osnovi enakovredna“, je določen v zakonodaji EU, zlasti v Direktivi (EU) 2016/680, in sodni praksi Sodišča Evropske unije ([3]). V tem pogledu je pomemben tudi referenčni dokument Evropskega odbora za varstvo podatkov o ustreznosti ([4]).

(4) Kot je pojasnilo Sodišče Evropske unije, v ta namen ni treba ugotavljati povsem enake ravni varstva ([5]). To pomeni zlasti, da lahko zadevna tretja država za varstvo osebnih podatkov uporablja drugačna sredstva od tistih, ki jih uporablja Evropska unija, če se v praksi izkaže, da so učinkovita pri zagotavljanju ustrezne ravni varstva ([6]). Standard ustreznosti torej ne zahteva dobesednega prepisa pravil Unije. Bolj kot to preskus temelji na proučitvi, ali tuji sistem kot celota prek vsebine pravic do zasebnosti ter njihovega učinkovitega izvajanja, nadzora in izvrševanja zagotavlja zahtevano raven varstva ([7]).

([1]) UL L 119, 4.5.2016, str. 89.

([2]) Glej uvodno izjavo 64 Direktive (EU) 2016/680.

([3]) Glej, nazadnje, sodbo v zadevi C-311/18, Maximillian Schrems/Data Protection Commissioner (v nadaljnjem besedilu: Schrems II), ECLI:EU:C:2020:559.

([4]) Glej Priporočila št. 01/2021 o referenčnem dokumentu o ustreznosti v skladu z direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj (Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive), sprejeta februarja 2021, ki so na voljo na povezavi: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_sl.

([5]) Sodba v zadevi C-362/14, Maximillian Schrems/Data Protection Commissioner (v nadaljnjem besedilu: Schrems), ECLI:EU:C:2015:650, točka 73.

([6]) Sodba v zadevi Schrems, točka 74.

([7]) Glej Sporočilo Komisije Evropskemu parlamentu in Svetu: Izmenjava in varstvo osebnih podatkov v globaliziranem svetu (COM (2017) 7, 10.1.2017, oddelek 3.1, str. 6), na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52017DC0007&from=SL.

(5) Komisija je pozorno analizirala ustrezno zakonodajo in prakso Združenega kraljestva. Na podlagi v nadaljevanju navedenih ugotovitev sklepa, da Združeno kraljestvo zagotavlja ustrezno raven varstva osebnih podatkov, ki se prenašajo od pristojnih organov v Uniji, kar spada na področje uporabe Direktive (EU) 2016/680, pristojnim organom v Združenem kraljestvu, kar spada na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 (Data Protection Act 2018) ([8]).

(6) Učinek tega sklepa je, da se taki prenosi lahko izvajajo za obdobje štirih let z morebitno možnostjo podaljšanja, ne da bi bilo potrebno dodatno dovoljenje in brez poseganja v pogoje iz člena 35 Direktive (EU) 2016/680.

2. PRAVILA, KI JIH PRISTOJNI ORGANI UPORABLJAJO ZA OBDELAVO PODATKOV ZA NAMENE PREPREČEVANJA, ODKRIVANJA IN PREISKOVANJA KAZNIVIH DEJANJ

2.1 Ustavni okvir

(7) Združeno kraljestvo je parlamentarna demokracija. Ima suveren parlament, ki je nad vsemi drugimi vladnimi institucijami, izvršilno vejo oblasti, ki izhaja iz parlamenta in je temu tudi odgovorna, ter neodvisno sodstvo. Izvršilna veja oblasti, katere pristojnosti temeljijo na zmožnosti, da uživa zaupanje izvoljenega spodnjega doma parlamenta Združenega kraljestva, je odgovorna obema domovoma parlamenta (spodnjemu in zgornjemu domu parlamenta Združenega kraljestva), ki sta odgovorna za pregled dela vlade ter razpravo o zakonih in njihovo sprejemanje. Parlament Združenega kraljestva je odgovornost za sprejemanje zakonodaje o nekaterih domačih vprašanjih na Škotskem, v Walesu in na Severnem Irskem prenesel na škotski parlament, valižanski parlament (Senedd Cymru) in skupščino Severne Irske. O vprašanju varstva podatkov lahko razpravlja samo parlament Združenega kraljestva, tj. ista zakonodaja se uporablja po vsej državi, druga področja politike, ki se nanašajo na ta sklep, pa so delegirana. Pristojnosti na področju sistemov kazenskega pravosodja na Škotskem in Severnem Irskem, vključno s policijskim delom (dejavnosti, ki jih izvaja policija), so bile na primer prenesene na škotski parlament oziroma na skupščino Severne Irske ([9]).

(8) Čeprav Združeno kraljestvo nima kodificirane ustave v običajnem pomenu uveljavljene ustanovne listine, so se sčasoma razvijala ustavna načela, zlasti na podlagi sodne prakse in družbenih norm. Priznana je bila ustavnopravna vrednost določenih listin in predpisov, kot so Magna Carta, Bill of Rights iz leta 1689 in zakon o človekovih pravicah iz leta 1998 (Human Rights Act 1998). Kot del ustave so se z običim pravom (common law), navedenimi listinami in predpisi in mednarodnimi pogodbami, zlasti Evropsko konvencijo o človekovih pravicah (EKČP), ki jo je Združeno kraljestvo ratificiralo leta 1951, razvile temeljne pravice posameznikov. Združeno kraljestvo je leta 1987 ratificiralo tudi Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov ([10]).

(9) Z zakonom o človekovih pravicah iz leta 1998 so bile pravice iz EKČP vključene v pravo Združenega kraljestva. S tem zakonom so vsem posameznikom podeljene temeljne pravice in svoboščine iz členov 2 do 12 in 14 EKČP ter členov 1 do 3 Protokola št. 1 k EKČP in člena 1 Protokola št. 13 k EKČP v povezavi s členi 16 do 18 EKČP. To zajema pravico do spoštovanja zasebnega in družinskega življenja, ki vključuje tudi pravico do varstva podatkov, in pravico do poštenega sojenja ([11]). Natančneje, v skladu s členom 8 EKČP se lahko javna oblast vmešava v izvrševanje pravice do zasebnosti le, če je to določeno z zakonom, kadar je nujno v demokratični družbi zaradi nacionalne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.

([8]) Zakon o varstvu podatkov iz leta 2018 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (UK Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement), ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Načela navedene konvencije so bila prvotno prenesena v pravo Združenega kraljestva z zakonom o varstvu podatkov iz leta 1984, ki je bil nadomeščen z zakonom o varstvu podatkov iz leta 1998 in nato z zakonom o varstvu podatkov iz leta 2018 (v povezavi z UK GDPR). Združeno kraljestvo je leta 2018 podpisalo tudi Protokol o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov in trenutno dela na ratifikaciji Konvencije.

([11]) Člena 6 in 8 EKČP (glej tudi dodatek 1 k zakonu o človekovih pravicah iz leta 1998).

(10) V skladu z zakonom o človekovih pravicah iz leta 1998 mora biti vsak ukrep javnih organov združljiv s pravico, ki jo zagotavlja EKČP ([12]). Poleg tega je treba primarno in sekundarno zakonodajo razumeti in izvajati tako, da sta združljivi z navedenimi pravicami ([13]). Če posameznik meni, da so javni organi kršili njegove pravice, vključno s pravico do zasebnosti in varstva podatkov, lahko pri sodiščih Združenega kraljestva uveljavlja pravna sredstva na podlagi zakona o človekovih pravicah iz leta 1998, ko izčrpa vsa nacionalna pravna sredstva, pa lahko zaradi kršitve pravic, zagotovljenih na podlagi EKČP, uveljavlja pravna sredstva pri Evropskem sodišču za človekove pravice.

2.2 **Okvir Združenega kraljestva za varstvo podatkov**

(11) Združeno kraljestvo je 31. januarja 2020 izstopilo iz Unije. Na podlagi Sporazuma o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo ([14]) se je v Združenem kraljestvu v prehodnem obdobju do 31. decembra 2020 še naprej uporabljalo pravo Unije. Pred izstopom in v prehodnem obdobju je bil zakonodajni okvir o varstvu osebnih podatkov v Združenem kraljestvu, ki ureja obdelavo osebnih podatkov s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, sestavljen iz pomembnih delov zakona o varstvu podatkov iz leta 2018 (Data Protection Act 2018), s katerim je bila v nacionalno zakonodajo prenesena Direktiva (EU) 2016/680.

(12) Vlada Združenega kraljestva je za pripravo na izstop iz EU sprejela zakon iz leta 2018 o izstopu iz Evropske unije (European Union (Withdrawal) Act 2018) (v nadaljnjem besedilu: zakon o izstopu iz EU) ([15]), ki je zakonodajo Unije, ki se neposredno uporablja, vključil v zakonodajo Združenega kraljestva in določil, da se t. i. domača zakonodaja, ki izhaja iz EU, še naprej uporablja do konca prehodnega obdobja. Del 3 zakona o varstvu podatkov iz leta 2018 ([16]), s katerim se Direktiva (EU) 2016/680 prenaša v nacionalno zakonodajo, pomeni domačo zakonodajo, ki izhaja iz EU, v skladu z zakonom o izstopu iz EU. Sodišča Združenega kraljestva morajo v skladu z zakonom o izstopu iz EU nespremenjeno domačo zakonodajo, ki izhaja iz EU, razlagati v skladu z ustrezno sodno prakso Sodišča Evropske unije (v nadaljnjem besedilu: Sodišče) in splošnimi načeli prava Unije, kot so učinkovala tik pred koncem prehodnega obdobja (tako imenovana ohranjena sodna praksa EU oziroma ohranjena splošna načela prava EU) ([17]).

(13) Ministri Združenega kraljestva lahko na podlagi zakona o izstopu iz EU sprejemajo sekundarno zakonodajo v obliki aktov z zakonsko močjo, da se v ohranjeno pravo EU uvedejo potrebne spremembe, ki so posledica izstopa Združenega kraljestva iz Unije. To pooblastilo je bilo izvršeno s predpisi o varstvu podatkov, zasebnosti in elektronski komunikaciji (spremembe itd.) (izstop iz EU) iz leta 2019 (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ali DPPEC Regulations) (v nadaljnjem besedilu: predpisi DPPEC) ([18]). S temi predpisi se zakonodaja Združenega kraljestva o varstvu podatkov, vključno z zakonom o varstvu podatkov iz leta 2018, spreminja tako, da ustreza domačemu kontekstu ([19]).

([12]) Člen 6 zakona o človekovih pravicah iz leta 1998.

([13]) Člen 3 zakona o človekovih pravicah iz leta 1998.

([14]) Sporazum o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo (2019/C 384 I/01, XT/21054/2019/INIT, UL C 384I, 12.11.2019, str. 1) (Sporazumu o izstopu), ki je na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=SL.

([15]) Zakon iz leta 2018 o izstopu iz Evropske unije je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([16]) Zakon o varstvu podatkov iz leta 2018 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([17]) Člen 6 zakona iz leta 2018 o izstopu iz EU.

([18]) Predpisi DPPEC iz leta 2019 (The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) so na voljo na povezavi: https://www.legislation.gov.uk/uksi/2019/419/contents/made, kot so bili spremenjeni s predpisi DPPEC iz leta 2020, ki so na voljo na povezavi: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) S predpisi o izstopu se uvajajo številne spremembe v del 3 zakona o varstvu podatkov iz leta 2018. Mnogo teh sprememb je tehničnih, kot je črtanje sklicevanj na „državo članico“ ali „direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj“ (glej na primer člen 48(8) ali člen 73(5)(a) zakona o varstvu podatkov iz leta 2018) in nadomestitev s pojmom „domače pravo“, tako da bo del 3 po koncu prehodnega obdobja deloval učinkovito kot domače pravo. V nekaterih delih so bile potrebne druge vrste sprememb, na primer glede tega, „kdo“ sprejema „sklepe o ustreznosti“ za zakonodajni okvir Združenega kraljestva o varstvu podatkov (glej člen 74A zakona o varstvu podatkov iz leta 2018), in sicer pristojni minister, ne Evropska komisija.

(14) Zato bodo pravni standardi za obdelavo osebnih podatkov s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, v Združenem kraljestvu po prehodnem obdobju v skladu s sporazumom o izstopu še naprej določeni v pomembnih delih zakona o varstvu podatkov iz leta 2018, vendar kakor je bil spremenjen s predpisi DPPEC, zlasti v delu 3 navedenega zakona. Splošna uredba o varstvu podatkov, kakor se uporablja v Združenem kraljestvu (UK GDPR), se za tovrstno obdelavo ne uporablja.

(15) Del 3 zakona o varstvu podatkov iz leta 2018 določa pravila za obdelavo osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, vključno z načeli o varstvu podatkov, pravnimi podlagami za obdelavo (zakonitost), pravicami posameznikov, na katere se nanašajo osebni podatki, obveznostmi pristojnih organov kot upravljavcev in omejitvami nadaljnjih prenosov podatkov. Obenem so veljavna pravila za nadzor, izvrševanje in sodno varstvo, ki se uporabljajo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, določena v delih 5 in 6 zakona o varstvu podatkov iz leta 2018.

(16) Poleg tega je treba glede na pomembno vlogo policije na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj upoštevati pravila, ki urejajo policijsko delo. Policijsko delo se izvaja decentralizirano, zato se za policijsko delo (a) v Angliji in Walesu, (b) na Škotskem in (c) na Severnem Irskem uporabljajo različni zakonodajni akti, ki pa so po svoji vsebini pogosto podobni ([20]). Poleg tega različne vrste smernic vsebujejo dodatna pojasnila o načinu uporabe pristojnosti policije. Obstajajo tri glavne oblike smernic za policijsko delo: 1) zakonsko predpisane smernice, izdane v skladu z zakonodajo, kot so etični kodeks (Code of Ethics) ([21]) in kodeks ravnanja pri upravljanju policijskih informacij (Code of Practice on the Management of Police Information) ([22]), izdan v skladu z zakonom o policiji iz leta 1996 ([23]), ali kodeksi PACE ([24]), izdani v skladu z zakonom o policijskih dokazih in dokazih v kazenskih postopkih ([25]), 2) smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij (Authorised Professional Practice on the Management of Police Information) ([26]), ki jih je objavil strokovni organ uslužbencev policije (College of Policing), ter 3) operativne smernice (ki jih je objavila policija). Svet nacionalnih načelnikov policije (National Police Chiefs Council) (usklajevalni organ za vse policijske službe Združenega kraljestva) objavlja operativne smernice, ki so jih podprle vse policijske službe in se zato uporabljajo na nacionalni ravni ([27]). Namen teh smernic je zagotoviti skladnost med službami glede načina upravljanja informacij ([28]).

(17) Kodeks ravnanja pri upravljanja policijskih informacij je pristojni minister objavil leta 2005, pri čemer je uporabil pooblastila iz člena 39A zakona o policiji iz leta 1996 ([29]). Vsak kodeks ravnanja, izdan na podlagi zakona o policiji, mora odobriti pristojni minister, preden je predložen parlamentu, pa se je treba o njem posvetovati z nacionalno agencijo za boj proti kriminalu (National Crime Agency). Člen 39A(7) zakona o policiji določa, da mora policija ustrezno upoštevati kodekse, izdane na podlagi zakona, zaradi česar se pričakuje, da policija ravna skladno

([20]) Za podrobnejše pojasnilo o policiji in njenih pooblastilih v Združenem kraljestvu glej: obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (glej opombo 9).

([21]) Kodeks ravnanja o načelih in standardih strokovnega ravnanja v policijskem poklicu v Angliji in Walesu (The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales) je na voljo na povezavi: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; etični kodeks policijskih organov Severne Irske (the Police Service Northern Ireland Code of Ethic) je na voljo na povezavi: https://www.nipolicingboard.org.uk/psni-code-ethics; etični kodeks o policijskem delu na Škotskem (the Code of Ethic for policing in Scotland) je na voljo na povezavi: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Kodeks ravnanja pri upravljanju policijskih informacij (Code of Practice on the Management of Police Information) je na voljo na povezavi: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Zakon o policiji iz leta 1996 (Police Act 1996) je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Kodeksi ravnanja v zvezi z zakonom o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984 (Police and Criminal Evidence Act 1984 (PACE) codes of practice) so na voljo na povezavi: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Zakon o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984 (Police and Criminal Evidence Act 1984) je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij so na voljo na povezavi: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Priročnik o varstvu podatkov za strokovnjake na področju varstva policijskih podatkov (Data Protection Manual for Police Data Protection Professionals) je na voljo na povezavi: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Kodeks ravnanja pri upravljanju policijskih informacij (glej opombo 22) se na primer uporablja za hrambo informacij pri operativnem policijskem delu (glej uvodno izjavo (47) tega sklepa).

([29]) Iz informacij organov Združenega kraljestva izhaja, da je strokovni organ uslužbencev policije med razpravami o ustreznosti pripravljal kodeks ravnanja pri upravljanju informacij in evidenc (Information and Records Management Code of Practice), ki bi nadomestil kodeks ravnanja pri upravljanju policijskih informacij. Osnutek kodeksa, ki je bil 25. januarja 2021 objavljen za javno posvetovanje, je na voljo na naslednji povezavi: https://www.college.police.uk/article/information-records-management-consultation.

z njimi ([30]). Poleg tega morajo biti nezavezujoče smernice (kot so smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij) vedno skladne s kodeksom ravnanja pri upravljanju policijskih informacij, ki je nadrejeni akt ([31]). Čeprav se lahko v določenih operativnih razmerah zgodi, da morajo policisti odstopati od teh smernic, morajo vsekakor še vedno izpolnjevati zahteve iz dela 3 zakona o varstvu podatkov iz leta 2018 ([32]).

(18) Dodatne smernice v zvezi z zakonodajo Združenega kraljestva o varstvu podatkov za obdelavo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zagotavlja informacijski pooblaščenec ([33]) (za dodatne podrobnosti o uradu informacijskega pooblaščenca glej uvodne izjave od (93) do (109)). Čeprav navedene smernice niso pravno zavezujoče, bi bila sodišča v sodnem postopku zavezana upoštevati vsako kršitev teh smernic, saj imajo razlagalno vrednost in prikazujejo, kako informacijski pooblaščenec v praksi razlaga in izvaja zakonodajo o varstvu podatkov ([34]).

(19) Nazadnje, organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj Združenega kraljestva morajo, kot je navedeno v uvodnih izjavah od (8) do (10), zagotoviti skladnost z EKČP in Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

(20) Pravni okvir, ki ureja obdelavo osebnih podatkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj Združenega kraljestva, je torej po strukturi in glavnih elementih zelo podoben okviru, ki se uporablja v EU. V to je zajeto dejstvo, da okvir ne temelji le na obveznostih iz domačega prava, ki jih je oblikovalo pravo EU, temveč tudi na obveznostih, kot so določene v mednarodnem pravu, zlasti s pristopom Združenega kraljestva k EKČP in Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov ter njegovim priznavanjem pristojnosti Evropskega sodišča za človekove pravice. Te obveznosti, ki izhajajo iz pravno zavezujočih mednarodnih instrumentov, ki se nanašajo zlasti na varstvo osebnih podatkov, so torej še posebno pomemben element pravnega okvira, ki se ocenjuje v tem sklepu.

2.3 **Stvarno področje uporabe in ozemeljska veljavnost**

(21) Stvarno področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 sovpada s področjem uporabe Direktive (EU) 2016/680, kot je določeno v členu 2(2) Direktive. Del 3 se uporablja za obdelavo osebnih podatkov, ki jo pristojni organ v celoti ali delno izvaja z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so že ali bodo del zbirke in ki je pristojni organ ne izvaja z avtomatiziranimi sredstvi.

(22) Da bi upravljavec spadal na področje uporabe dela 3, mora biti pristojni organ, obdelava pa mora biti izvedena za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Ureditev varstva podatkov, ki se ocenjuje v tem sklepu, se torej uporablja za vse dejavnosti teh pristojnih organov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

(23) Pojem „pristojni organ“ je opredeljen v členu 30 zakona o varstvu podatkov kot oseba iz dodatka 7 k zakonu o varstvu podatkov iz leta 2018 ter vsaka druga oseba, kolikor ima ta oseba zakonske pristojnosti za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Pristojni organi iz dodatka 7 ne zajemajo le policije, temveč tudi vse ministrske in vladne oddelke Združenega kraljestva ter druge organe s preiskovalnimi nalogami (npr. vodja oddelkov davčne in carinske uprave Združenega kraljestva (Commissioner for Her Majesty's Revenue and Customs), valižanska davčna uprava (Welsh Revenue Authority), organ, pristojen za konkurenco in

([30]) V zadevi R proti the Commission of Police of the Metropolis [2014] EWCA Civ 585 je bil potrjen pravni status kodeksa ravnanja pri upravljanju policijskih informacij, prizivni sodnik Laws pa je izjavil, da mora komisar londonske policijske uprave (Metropolitan Police) upoštevati navedeni kodeks in smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij v skladu s členom 39A zakona o policiji iz leta 1996.

([31]) Inšpekcijske nadzore policije v zvezi s skladnostjo s kodeksom ravnanja pri upravljanju policijskih informacij izvaja inšpektorat policije in gasilsko-reševalne službe Združenega kraljestva (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services – HMICFRS).

([32]) Glej v zvezi s tem stališče strokovnega organa uslužbencev policije o skladnosti s smernicami o dovoljeni strokovni praksi pri upravljanju policijskih informacij glede vseh vidikov policijskega dela, ki pojasnjuje, da je „smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij odobril strokovni organ za policijsko delo (strokovni organ uslužbencev policije) kot uradni vir poklicne prakse za policijsko delo. Pričakuje se, da policijski uradniki in uslužbenci pri izvajanju pooblastil upoštevajo navedene smernice. Vendar se lahko pojavijo okoliščine, v katerih mora policija zaradi upravičenega operativnega razloga odstopati od navedenih smernic, če je tako ravnanje jasno utemeljeno. Policija bi morala biti odgovorna za lokalna in nacionalna tveganja, povezana z delovanjem zunaj nacionalno dogovorjenih smernic; če je posledica tega incident ali preiskava (kot na primer prek neodvisnega urada za ravnanje policije (Independent Office of Police Conduct)), pa je policija odgovorna za vsako tveganje“, stališče je na voljo na povezavi https://www.app.college.police.uk/faq-page/.

([33]) Smernice o obdelavi podatkov v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Guide to Law Enforcement Processing) so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Glej sodbo v zadevi Bridges proti Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), v kateri je sodišče High Court kljub navedbi, da smernice informacijskega pooblaščenca niso zakonsko določene, navedlo: „[p]ri presoji, ali je upravljavec podatkov upošteval obveznosti po členu člen 64 [glede izvedbe ocene učinka v zvezi z varstvom podatkov, ki se nanaša na obdelavo, pri kateri obstaja visoko tveganje], bo sodišče upoštevalo smernice, ki jih je objavil informacijski pooblaščenec glede ocene učinka v zvezi z varstvom podatkov.“

trge (Competition and Markets Authority), zemljiška knjiga Združenega kraljestva (Her Majesty's Land Register) ali nacionalna agencija za boj proti kriminalu), organe, pristojne za pregon, druge organe kazenskega pravosodja in druge nosilce pooblastil ali organizacije, ki izvajajo dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([35]). Del 3 zakona o varstvu podatkov iz leta 2018 se uporablja tudi za sodišča, kadar izvajajo sodne funkcije, razen za del, povezan s pravicami posameznika, na katerega se nanašajo osebni podatki, in nadzorom, ki ga izvaja urad informacijskega pooblaščenca ([36]). Seznam pristojnih organov, naveden v dodatku 7, ni dokončen in ga lahko posodobi pristojni minister s predpisi, s katerimi se upoštevajo spremembe v organizaciji javnih funkcij ([37]).

(24) Zadevna obdelava mora biti tudi za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, pri čemer je ta namen opredeljen kot preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem ([38]). Kadar se obdelava, ki jo izvajajo pristojni organi, ne izvaja za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ni urejena z delom 3 zakona o varstvu podatkov iz leta 2018. Tako je na primer, ko organ, pristojen za konkurenco in trge, preiskuje primere, ki niso inkriminirani (npr. združitve med podjetji). V tem primeru se uporablja UK GDPR skupaj z delom 2 zakona o varstvu podatkov iz leta 2018, saj pristojni organi obdelavo osebnih podatkov izvajajo za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Da bi se določilo, katera ureditev varstva podatkov (del 3 ali del 2 zakona o varstvu podatkov iz leta 2018) se uporablja pri posamezni obdelavi osebnih podatkov, mora pristojni organ, tj. upravljavec, proučiti, ali je glavni namen take obdelave eden od namenov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v skladu z navedenim zakonom.

(25) V členu 207(2) zakona je glede ozemeljske veljavnosti dela 3 zakona o varstvu podatkov iz leta 2018 določeno, da se navedeni zakon uporablja za obdelavo osebnih podatkov v kontekstu dejavnosti osebe, ki ima ustanovitev na ozemlju Združenega kraljestva. To vključuje javne organe ozemelj Anglije, Walesa, Škotske in Severne Irske, ki spadajo na ozemeljsko področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 ([39]).

2.3.1 *Opredelitev pojmov osebni podatki in obdelava*

(26) Ključna pojma osebni podatki in obdelava sta opredeljena v delu 3 zakona o varstvu podatkov iz leta 2018 in se uporabljata v celotnem zakonu. Opredelitve natančno sledijo ustreznim opredelitvam iz člena 3 Direktive (EU) 2016/680. V skladu z zakonom o varstvu podatkov iz leta 2018 pojem osebni podatki zajema vse informacije, ki se nanašajo na določenega ali določljivega živega posameznika ([40]). V skladu s členom 3(3) zakona o varstvu podatkov iz leta 2018 je določljiv posameznik tisti, ki ga je mogoče neposredno ali posredno določiti na podlagi informacij, vključno z navedbo imena ali identifikatorja ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika. Pojem „obdelava" je opredeljen kot dejanje ali niz dejanj, ki se izvaja v zvezi z informacijami ali nizi informacij, kot so (a) zbiranje, beleženje, urejanje, strukturiranje ali shranjevanje, (b) prilagajanje ali spreminjanje, (c) priklic, vpogled ali uporaba, (d) razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, (e) prilagajanje ali kombiniranje ali (f) omejevanje, izbris ali uničenje. Poleg tega je v zakonu pojem „obdelava občutljivih podatkov" opredeljen kot (a) obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, vero ali filozofsko prepričanje ali članstvo v sindikatu; (b) obdelava genskih podatkov ali biometričnih podatkov za namene edinstvene identifikacije posameznika; (c) obdelava podatkov o zdravstvenem stanju ter (d) obdelava podatkov v zvezi s spolnim življenjem ali spolno usmerjenostjo posameznika" ([41]). V členu 205 zakona o varstvu podatkov iz leta 2018 so v zvezi s tem opredeljeni pojmi „biometrični podatki" ([42]), „podatki o zdravstvenem stanju" ([43]) in „genski podatki" ([44]).

([35]) V dodatku 7 k zakonu o varstvu podatkov iz leta 2018 so med drugim navedeni direktor javnega tožilstva, direktor javnega tožilstva za Severno Irsko ali informacijski pooblaščenec.

([36]) Člen 43(3) zakona o varstvu podatkov iz leta 2018.

([37]) Člen 30(3) zakona o varstvu podatkov iz leta 2018. Obveščevalne službe (tajna obveščevalna služba, varnostna služba in britanska obveščevalna služba GCHQ (Government Communications Headquarters)) niso pristojni organi (glej člen 30(2) zakona o varstvu podatkov iz leta 2018) in del 3 zakona o varstvu podatkov iz leta 2018 se ne uporablja za nobeno od njihovih dejavnosti. Njihove dejavnosti spadajo na področje uporabe dela 4 zakona o varstvu podatkov iz leta 2018.

([38]) Člen 31 zakona o varstvu podatkov iz leta 2018.

([39]) To pomeni, da se zakon o varstvu podatkov iz leta 2018 in torej ta sklep ne uporabljata za kronska odvisna ozemlja Združenega kraljestva in druga čezmorska ozemlja Združenega kraljestva, kot so na primer Falklandski otoki in ozemlje Gibraltarja.

([40]) Osebni podatki o pokojniku ne spadajo na področje uporabe zakona o varstvu podatkov iz leta 2018.

([41]) Člen 35(8) zakona o varstvu podatkov iz leta 2018.

([42]) „Biometrični podatki" pomenijo osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki.

([43]) „Podatki o zdravstvenem stanju" pomenijo osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju.

([44]) „Genski podatki" pomenijo osebne podatke v zvezi s podedovanimi ali pridobljenimi genetskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika.

(27) V členu 32 zakona o varstvu podatkov iz leta 2018 sta pojasnjeni opredelitvi pojmov „upravljavec“ in „obdelovalec“ v kontekstu obdelave osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ki natančno sledita ustreznim opredelitvam iz Direktive (EU) 2016/680. Upravljavec pomeni pristojni organ, ki določa namene in sredstva obdelave osebnih podatkov. Kadar obdelavo določa pravo, je upravljavec tisti pristojni organ, ki mu to pravo nalaga tako obveznost. Obdelovalec je opredeljen kot oseba, ki obdeluje osebne podatke v imenu upravljavca (ki ni oseba, zaposlena pri upravljavcu).

2.4 **Zaščitni ukrepi, pravice in obveznosti**

2.4.1 *Zakonitost in poštenost obdelave*

(28) V skladu s členom 35 zakona o varstvu podatkov iz leta 2018 mora biti obdelava osebnih podatkov zakonita in poštena, in to na podoben način, kot je določen v členu 4(l)(a) Direktive (EU) 2016/680. V skladu s členom 35(2) zakona o varstvu podatkov iz leta 2018 je obdelava osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zakonita le, če temelji na pravu in je posameznik, na katerega se nanašajo osebni podatki, privolil v njihovo obdelavo za navedeni namen, ali pa je obdelava potrebna za opravljanje naloge, ki jo v ta namen izvaja pristojni organ.

2.4.1.1 Obdelava, ki temelji na pravu

(29) Za zakonitost obdelave, ki spada v del 3 zakona o varstvu podatkov iz leta 2018, mora taka obdelava podobno kot v členu 8 Direktive (EU) 2016/680 „temeljiti na pravu“. „Zakonita“ obdelava pomeni, da jo dovoljujejo predpisi, obče pravo ali posebne kraljeve pravice ([45]).

(30) Pooblastila pristojnih organov so na splošno urejena s predpisi, kar pomeni, da so njihove naloge in pristojnosti jasno določene v zakonodaji, ki jo sprejme Parlament ([46]). Policija in drugi pristojni organi iz dodatka 7 k zakonu o varstvu podatkov iz leta 2018 se lahko v nekaterih primerih pri obdelavi podatkov sklicujejo na obče pravo ([47]). Obče pravo se je oblikovalo s precedensi, določenimi v odločbah sodišč. Obče pravo je pomembno v smislu pooblastil, ki jih ima na voljo policija, ki iz tega pravnega vira pridobiva svoje temeljne dolžnosti, tj. varovanje javnosti z odkrivanjem in preprečevanjem kaznivih dejanj ([48]). Vendar policija pri izvajanju takih dolžnosti uporablja obče pravo in zakonodajna

([45]) Pojasnjevalne opombe k zakonu o varstvu podatkov iz leta 2018, odstavek 181, ki so na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Pooblastila nacionalne agencije za boj proti kriminalu (National Crime Agency) na primer izhajajo iz zakona o kaznivih dejanjih in sodiščih iz leta 2013 (Crime and Courts Act 2013), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2013/22/contents. Podobno so pooblastila agencije za prehranske standarde (Food Standards Agency) določena z zakonom o prehranskih standardih iz leta 1999 (Food Standards Act 1999), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1999/28/contents. Drugi primeri zajemajo zakon o pregonu storilcev kaznivih dejanj iz leta 1985 (Prosecution of Offenders Act 1985), s katerim je bilo ustanovljeno državno tožilstvo (Crown Prosecution Service) (glej: https://www.legislation.gov.uk/ukpga/1985/23/contents); zakon o vodjih oddelkov davčne in carinske uprave iz leta 2005 (Commissioners for Revenue and Customs Act 2005), s katerim je bila ustanovljena davčna in carinska uprava Združenega kraljestva (glej https://www.legislation.gov.uk/ukpga/2005/11/contents); zakon o kazenskem postopku (Škotska) iz leta 1995 (Criminal Procedure (Scotland) Act 1995), s katerim je bila ustanovljena škotska komisija za ponovno proučitev kazenskih zadev (Scottish Criminal Cases Review Commission) (glej https://www.legislation.gov.uk/ukpga/1995/46/contents); zakon o pravosodju (Severna Irska) iz leta 2002 (Justice (Northern Ireland) Act 2002), s katerim je bilo ustanovljeno državno tožilstvo na Severnem Irskem (Public Prosecution Service in Northern Ireland) (glej https://www.legislation.gov.uk/ukpga/2002/26/contents), ter zakon o kazenskem pravosodju iz leta 1987 (Criminal Justice Act 1987), s katerim je bil ustanovljen in je dobil pooblastila urad za resne prevare (Serious Fraud Office) (glej https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Glede na podatke organov Združenega kraljestva na primer pristojnosti za preiskovanje smrti in pregon kaznivih dejanj škotskega glavnega državnega tožilca (Lord Advocate), ki je vodja sistema kazenskega pregona na Škotskem in deluje v okviru škotskega državnega tožilstva (Crown Office and Procurator Fiscal Service), pristojnega za zadeve pregona na Škotskem, izhajajo iz občega prava, medtem ko so nekatere od njegovih nalog določene v predpisih. Nadalje, pristojnosti monarha ter posledično različnih vladnih oddelkov in ministrov prav tako izhajajo iz kombinacije zakonodaje, občega prava in posebnih kraljevih pravic (to so pristojnosti na podlagi občega prava, podeljene monarhu, ki pa jih izvajajo ministri).

([48]) Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, stran 8 (glej opombo 9).

pooblastila ([49]). Kadar ima policija zakonska pooblastila, ta nadomeščajo vsa pooblastila, ki izhajajo iz občega prava ([50]).

(31) Sodišča so priznala, da so v obseg pooblastil in obveznosti policijskega uradnika na podlagi občega prava vključeni „vsi koraki, ki se mu zdijo potrebni za zagotavljanje miru, preprečevanje kaznivih dejanj ali varovanje lastnine pred škodo, povzročeno s kaznivim dejanjem“ ([51]). Pooblastila na podlagi občega prava niso neomejena. Imajo številne omejitve, vključno s tistimi, ki sta jih uvedla sodišče ([52]) in zakonodaja, zlasti zakon o človekovih pravicah iz leta 1998 in zakon o enakosti iz leta 2010 (Equality Act 2010) ([53]). Za pristojne organe, ki obdelujejo podatke v skladu z delom 3 zakona o varstvu podatkov iz leta 2018, je v to zajeto tudi, da se pooblastila na podlagi občega prava izvajajo skladno z zahtevami iz navedenega zakona ([54]). Pri odločitvi o izvedbi kakršne koli obdelave podatkov je treba proučiti zahteve iz veljavnih smernic, kot je kodeks ravnanja glede upravljanja policijskih informacij, in smernic specifično za eno od držav Združenega kraljestva ([55]). Številne smernice, ki jih izdajo vlada in policijski organi, zagotavljajo, da policijski uradniki izvajajo pooblastila v omejitvah, ki jih določa obče pravo ali ustrezni predpis ([56]).

(32) Posebne kraljeve pravice, ki so še en sestavni del prava, se nanašajo na določene pristojnosti, podeljene kroni, ki jih lahko izvaja izvršilna veja oblasti in ne temeljijo na predpisu, temveč izhajajo iz suverenosti monarha ([57]). V okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je pomembnih zelo malo primerov posebnih pristojnosti. Vključujejo na primer okvir medsebojne pravne pomoči, ki pristojnemu ministru omogoča, da si za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj izmenjuje podatke s tretjimi državami, pristojnost za

([49]) Ključni zakonodajni akti, ki urejajo glavna policijska pooblastila (aretacije, preiskave, dovoljenja za neprekinjeno pridržanje, odvzem prstnih odtisov, odvzem brisov sluznice in drugega biološkega materiala, prestrezanje tiralic, dostop do komunikacijskih podatkov), so: (i), za Anglijo in Wales – zakon o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984 (Police and Criminal Evidence Act 1984 (PACE)), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1984/60/contents (kot je bil spremenjen z zakonom o varstvu svoboščin iz leta 2012 (Protection of Freedoms Act 2012), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2012/9/contents), in zakonom o preiskovalnih pooblastilih iz leta 2016 (Investigatory Powers Act 2016), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2016/25/contents), (ii) za Škotsko – zakon o kazenskem pravosodju (Škotska) iz leta 2016 (Criminal Justice (Scotland) Act 2016), ki je na voljo na povezavi: https://www.legislation.gov.uk/asp/2016/1/contents in zakon o kazenskem postopku (Škotska) iz leta 1995 (Criminal Procedure (Scotland) Act 1995, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1995/46/contents), ter (iii) za Severno Irsko – zakon o policijskih dokazih in dokazih v kazenskih postopkih (Severna Irska) iz leta 1989 (Police and Criminal Evidence (Northern Ireland) Order 1989), ki je na voljo na povezavi: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Organi Združenega kraljestva so pojasnili, da je v Združenem kraljestvu že dolgo vzpostavljena prevlada zakonskega prava, ki sega do sodbe Entick proti Carrington [1765] EWHC KB J98, s katero se je priznalo, da je izvajanje pooblastil izvršilne veje oblasti omejeno, ter uvedlo načelo, da so pooblastila na podlagi občega prava in posebna pooblastila monarha in vlade podrejena pravu države.

([51]) Glej sodbo Rice proti Connolly [1966] 2 QB 414.

([52]) Glej sodbo R(Catt) proti Association of Chief police Officers [2015] AC 1065, v kateri je sodnik Lord Sumption v zvezi s policijskimi pooblastili za pridobitev informacij od posameznika (ki je storil kaznivo dejanje) in njihovo hrambo odločil, da ima policija na podlagi občega prava pooblastilo za pridobivanje in hrambo informacij za namene policijskega dela, tj. na splošno za vzdrževanje javnega reda in preprečevanje in odkrivanje kaznivih dejanj. Ta pooblastila ne dovoljujejo, da bi se informacije pridobivale z vsiljivimi metodami, kot je vstop na zasebno posest, ali dejanji (ki niso aretacija v skladu s pooblastili na podlagi občega prava), ki bi pomenila napad. Sodnik je menil, da so bila v tej zadevi pooblastila na podlagi občega prava dovolj široka, da je bilo dovoljeno pridobivanje in shranjevanje take vrste javnih informacij, ki so se obravnavale v teh pritožbah.

([53]) Zakon o enakosti iz leta 2010 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Za primer zadeve, v kateri so policijska pooblastila na podlagi občega prava ocenjena v skladu z zakonom o varstvu podatkov iz leta 1998, glej odločbo sodišča High Court v zadevi Bridges proti the Chief Constable of South Wales Police (glej opombo 33). Glej tudi sodbi v zadevi Vidal-Hall proti Google Inc [2015] EWCA Civ 311 in v zadevi Richard proti BBC [2018] EWHC 1837 (Ch).

([55]) Glej na primer smernice severnoirske policije o navodilih za storitev upravljanja evidenc, ki so na voljo na povezavi: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Spodnji dom parlamenta Združenega kraljestva je objavil informativni dokument, v katerem so določena glavna pooblastila na podlagi občega prava in zakonska pooblastila policije v Angliji in Walesu (glej https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). V skladu s tem dokumentom so na primer pooblastila za zagotavljanje „državnega miru“ ter „uporaba telesne sile“ pooblastila, izvedena na podlagi občega prava, „pooblastila za pridržanje in pregled“ pa so vedno izvedena iz predpisa. Poleg tega škotska vlada na svojem spletnem mestu zagotavlja informacije o policijskih pooblastilih za aretacijo ter pridržanje in pregled (glej https://www.gov.scot/policies/police/police-powers/).

([57]) V skladu z informacijami, ki so jih zagotovili organi Združenega kraljestva, med posebne pristojnosti, ki jih izvaja vlada, spadajo sestavljanje in ratifikacija mednarodnih pogodb, opravljanje diplomatske dejavnosti, uporaba oboroženih sil v Združenem kraljestvu za vzdrževanje miru v podporo policiji.

izmenjavo informacij na ta način pa ni vedno določena v predpisih ([58]). Posebne kraljeve pravice zavezujejo načela občega prava ([59]) in so podrejene zakonskim aktom, zato zanje veljajo omejitve iz zakona o človekovih pravicah iz leta 1998 in zakona o varstvu podatkov iz leta 2018 ([60]).

(33) V ureditvi Združenega kraljestva se podobno kot v členu 8 Direktive (EU) 2016/680 zahteva, da morajo pristojni organi za upoštevanje načela zakonitosti zagotoviti, da mora biti obdelava, kadar temelji na pravu, tudi potrebna za opravljanje naloge, ki se izvaja za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Urad informacijskega pooblaščenca v smernicah v zvezi s tem pojasnjuje, da „mora biti usmerjen in sorazmeren način za dosego namena. Pravna podlaga se ne bo uporabljala, če se lahko namen razumno doseže z drugimi manj vsiljivimi sredstvi. Ne zadostuje trditev, da je obdelava potrebna, ker ste se odločili za določen način opravljanja poslovne dejavnosti. Vprašanje je, ali je obdelava za navedeni namen potrebna“ ([61]).

2.4.1.2 Obdelava na podlagi privolitve posameznika, na katerega se nanašajo osebni podatki

(34) V členu 35(2) zakona o varstvu podatkov iz leta 2018 je določena možnost obdelave osebnih podatkov na podlagi privolitve posameznika, kot je navedeno v uvodni izjavi (28).

(35) Vendar se zdi, da privolitev ni pravna podlaga, ki bi bila ustrezna za dejanja obdelave, ki spadajo na področje uporabe tega sklepa. Dejanja obdelave, ki jih zajema ta sklep, se bodo vedno nanašala na podatke, ki so jih pristojni organ države članice v skladu z Direktivo (EU) 2016/680 prenesli pristojnemu organu Združenega kraljestva. Zato običajno ne bodo zajemala neposrednega stika (zbiranje) med javnim organom in posamezniki, na katere se nanašajo osebni podatki, ki lahko temelji na privolitvi v skladu s členom 35(2)(a) zakona o varstvu podatkov iz leta 2018.

(36) Čeprav se sklicevanje na privolitev pri oceni, izvedeni v skladu s tem sklepom, ne šteje za pomembno, je treba zaradi popolnosti opozoriti, da obdelava v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj nikoli ne temelji izključno na privolitvi, saj mora pristojni organ vedno imeti osnovno pristojnost, s katero je njegova obdelava podatkov upravičena ([62]). Podobno kot je to dovoljeno v skladu z Direktivo (EU) 2016/680 ([63]), to bolj konkretno pomeni, da se privolitev uporablja kot dodatni pogoj, da se omogočijo določena omejena in specifična dejanja obdelave, ki jih sicer ne bi bilo mogoče izvesti, na primer zbiranje in obdelava vzorcev DNK posameznika, ki ni osumljenec. Obdelava se v tem primeru ne bi izvajala, če privolitev ni bila dana ali je preklicana ([64]).

([58]) V zvezi s tem glej oceno ureditve Združenega kraljestva za nadaljnje prenose v uvodnih izjavah (74) do (87).

([59]) Glej sodbo v zadevi Bancoult proti Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, v kateri je sodišče ugotovilo, da lahko za posebno pristojnost za izdajanje odločb v svetu veljajo tudi običajni razlogi za sodno presojo.

([60]) Glej sodbo v zadevi Attorney-General proti De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, v kateri je sodišče ugotovilo, da posebnih pristojnosti ni mogoče uporabiti, če jih nadomeščajo zakonska pooblastila; sodbo v zadevi Laker Airways Ltd v Department of Trade [1977] QB 643, v kateri je sodišče ugotovilo, da posebnih pristojnosti ni mogoče uporabiti za onemogočanje zakonskega prava; sodbo v zadevi R. proti Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, v kateri je sodišče ugotovilo, da posebnih pristojnosti ni mogoče uporabiti, kadar so v nasprotju s sprejeto zakonodajo, tudi če ta še ni veljavna; sodbo v zadevi R (Miller) proti Secretary of State for Exiting the European Union [2017] UKSC 5, v kateri je sodišče potrdilo zmožnost zakonskega prava, da prilagodi in ukine posebne pristojnosti. Za splošni pregled razmerja med posebnimi kraljevimi pravicami in predpisi ali pooblastili na podlagi občega prava glej informativni dokument spodnjega doma parlamenta Združenega kraljestva, ki je na voljo na povezavi: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Kaj je bistvo prvega načela?“ (Guide to Law Enforcement Processing, "What is the first principle about?"), ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) To izhaja iz besedila ustrezne določbe zakona o varstvu podatkov iz leta 2018, v skladu s katero je obdelava osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zakonita le in v obsegu, če „temelji na pravu in je (a) posameznik, na katerega se nanašajo osebni podatki, privolil v njihovo obdelavo v ta namen, (b) ali pa je obdelava potrebna za opravljanje naloge, ki jo v ta namen izvaja pristojni organ“.

([63]) Glej uvodni izjavi 35 in 37 Direktive (EU) 2016/680.

([64]) Organi Združenega kraljestva so pojasnili, da bi bil en primer, v katerem bi bila privolitev ustrezna podlaga za obdelavo, kadar policija v povezavi s pogrešano osebo pridobi vzorec DNK, da ga primerja s truplom, ki je najdeno. V takih primerih ne bi bilo ustrezno, da bi policija posameznika, na katerega se nanašajo osebni podatki, prisilila k predložitvi vzorca; pač pa bi ga prosila za privolitev, ki je dana prostovoljno in se lahko kadar koli prekliče. Če se privolitev prekliče, podatkov ni več mogoče obdelati, razen če se za nadaljnjo obdelavo vzorca določi nova pravna podlaga (npr. posameznik, na katerega se nanašajo osebni podatki, je postal osumljenec). Drug primer bi bil lahko, kadar policija preiskuje kaznivo dejanje, v katerem bi lahko imela žrtev (lahko gre za žrtev ropa, kaznivega dejanja zoper spolno nedotakljivost ali nasilja v družini, sorodnike žrtve, ki ji je bilo vzeto življenje, ali žrtve drugih kaznivih dejanj) korist od napotitve na organizacijo za pomoč žrtvam (Victim Support) (tj. neodvisne dobrodelne organizacije, ki podpira ljudi, ki so jih prizadela kazniva dejanja in travmatični dogodki). V takih primerim bo policija, če ima žrtvino privolitev, organizaciji za pomoč žrtvam le posredovala osebne informacije, kot so ime in kontaktni podatki.

(37) V primerih, v katerih je potrebno privoljenje posameznika, mora biti tako privoljenje nedvoumno in mora zajemati jasno pritrdilno dejanje ([65]). Policija mora imeti obvestilo o varovanju zasebnosti, ki med drugim vključuje potrebne informacije, povezane z veljavno uporabo privolitve. Poleg tega nekateri oddelki policije objavljajo dodatno gradivo o tem, kako zagotavljajo skladnost z zakonodajo o varstvu podatkov, vključno z navedbo, kako in kdaj bodo privolitev uporabili kot pravno podlago ([66]).

2.4.1.3 Obdelava občutljivih podatkov

(38) Glede obdelave posebnih vrst podatkov bi morali veljati posebni zaščitni ukrepi. V zvezi s tem so v delu 3 zakona o varstvu podatkov iz leta 2018, podobno kot je določeno v členu 10 Direktive (EU) 2016/680, določeni strožji zaščitni ukrepi za t. i. obdelavo občutljivih podatkov ([67]).

(39) V skladu s členom 35(3) zakona o varstvu podatkov iz leta 1998 lahko pristojni organi obdelujejo občutljive podatke za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj le v dveh primerih: (1) posameznik, na katerega se nanašajo osebni podatki, je privolil v njihovo obdelavo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in ko se obdelava izvaja, ima upravljavec sestavljen dokument o ustrezni politiki (Appropriate Policy Document) ([68]) ali (2) obdelava je nujno potrebna za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in izpolnjuje vsaj enega od pogojev iz dodatka 8 k zakonu o varstvu podatkov iz leta 2018 ter ko se obdelava izvaja, ima upravljavec sestavljen dokument o ustrezni politiki ([69]).

(40) Kar zadeva prvi primer in kot je pojasnjeno v uvodni izjavi 38, se pri tovrstnem prenosu sklicevanje na privolitev ne šteje za ustrezno v skladu s tem sklepom ([70]).

(41) Kadar se pri obdelavi občutljivih podatkov ni mogoče sklicevati na privolitev, se lahko obdelava izvede z uporabo enega od pogojev iz dodatka 8 k zakonu o varstvu podatkov iz leta 2018. Ti pogoji se nanašajo na obdelavo, ki je potrebna za namene, opredeljene z zakonom, izvajanje sodne oblasti, zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugega posameznika, varstvo otrok in ogroženih posameznikov, pravne zahtevke, sodne akte, preprečevanje goljufij, arhiviranje, kadar posameznik, na katerega se nanašajo osebni podatki, sam objavi osebne podatke. Za vse pogoje iz dodatka 8 razen primera, ko posameznik sam objavi osebne podatke, velja preskus nujne potrebnosti. Urad informacijskega pooblaščenca je pojasnil, da „nujna potrebnost v tem

([65]) Ni ločene opredelitve privolitve za namene obdelave osebnih podatkov v skladu z delom 3 zakona o varstvu podatkov iz leta 2018. Urad informacijskega pooblaščenca je zagotovil smernice o pojmu privolitev v skladu z delom 3 zakona o varstvu podatkov iz leta 2018, v katerih je pojasnil, da ima enak pomen in da bi ga bilo treba uskladiti z opredelitvijo iz GDPR, zlasti da „mora biti privolitev prostovoljna, konkretna in informirana ter da mora biti posamezniku zagotovljena dejanska izbira, s katero izrazi strinjanje s podatki, ki se obdelujejo“ (Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „O čem govori prvo načelo?“ (glej opombo 64), za privolitev pa smernice glede varstva podatkov (Guide to Data Protection), ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Glej na primer informacije na spletni strani policije grofije Lincolnshire (https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) ali na spletni strani policije grofije Zahodni Yorkshire (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Člen 35(8) zakona o varstvu podatkov iz leta 2018.

([68]) Člen 35(4) zakona o varstvu podatkov iz leta 2018.

([69]) Člen 35(5) zakona o varstvu podatkov iz leta 2018.

([70]) Zaradi popolnosti je treba navesti, da kadar obdelava temelji na privolitvi, mora biti ta prostovoljna, konkretna in informirana ter mora vsebovati izrecno izbiro glede izražanja strinjanja s podatki, ki se obdelujejo. Kadar obdelava temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki, mora imeti upravljavec poleg tega sestavljen dokument o ustrezni politiki. V členu 42 zakona o varstvu podatkov iz leta 2018 so navedene zahteve, ki jih mora izpolnjevati tak dokument. Jasno je navedeno, da morajo biti v dokumentu vsaj pojasnjeni postopki upravljavca za zagotavljanje skladnosti z načeli o varstvu podatkov ter njegova politika glede hrambe in izbrisa osebnih podatkov. To v skladu s členom 42 zakona o varstvu podatkov iz leta 2018 pomeni, da mora upravljavec sestaviti dokument, v katerem (a) so pojasnjeni postopki upravljavca za zagotavljanje skladnosti z načeli o varstvu podatkov ter (b) je pojasnjena politika upravljavca glede hrambe in izbrisa osebnih podatkov, obdelanih s sklicevanjem na privolitev posameznika, na katerega se nanašajo osebni podatki, ali je določeno, kako dolgo se bodo taki osebni podatki najverjetneje hranili. Dokument o politiki vsebuje zlasti zahtevo, da mora upravljavec vedno vključevati elemente iz točk (a) in (b) ter pri tem spoštovati dolžnost vodenja evidence dejavnosti obdelave. Urad informacijskega pooblaščenca je objavil dokument s predlogo (Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj. Pogoji za obdelavo občutljivih podatkov (Guide to Law Enforcement Processing. „Conditions for sensitive processing“)), ki je na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing), če upravljavec ne izpolni teh zahtev, pa lahko tudi sprejme izvršilni ukrep. Ustrezni dokument o politiki proučijo tudi sodišča pri obravnavi morebitnih kršitev zakona o varstvu podatkov iz leta 2018. Na primer v nedavni sodbi v zadevi R (Bridges) proti Chief Constable of South Wales Police so sodišča pregledala ustrezni dokument o politiki upravljavca in ugotovila, da je bil primeren, a bi se vanj lahko vključile dodatne podrobnosti. Zato je policija južnega Walesa ustrezni dokument o politiki pregledala in ga posodobila z novimi smernicami urada informacijskega pooblaščenca (glej opombo 33). Ustrezni dokument o politiki mora upravljavec v skladu s členom 42(3) zakona o varstvu podatkov iz leta 2018 redno pregledovati. Nazadnje, kot dodatni zaščitni ukrep mora upravljavec v skladu s členom 42(4) zakona o varstvu podatkov iz leta 2018 voditi razširjeno evidenco dejavnosti obdelave, ki zajema dodatne elemente v primerjavi s splošno obveznostjo upravljavca, ki je voditi evidenco dejavnosti obdelave, ki je določena v členu 61 zakona o varstvu podatkov iz leta 2018.

kontekstu pomeni, da se mora obdelava nanašati na nujno družbeno potrebo, ki se je ne da razumno doseči z manj vsiljivimi sredstvi“ ([71]). Poleg tega za nekatere od pogojev veljajo dodatne omejitve. Na primer za sklicevanje na pogoj „namenov, opredeljenih z zakonom“ in „pogoj varstva“ (odstavka 1 in 4 dodatka 8) je treba opraviti dodaten preskus bistvenega javnega interesa. V zvezi s pogoji, ki se nanašajo na varstvo otroka (odstavek 4 dodatka 8), mora biti posameznik, na katerega se nanašajo osebni podatki, določene starosti in se šteti za ogroženega. Poleg tega lahko upravljavec uporabi pogoj iz odstavka 4 dodatka 8 le v primeru posebnih okoliščin ([72]). Podobne omejitve veljajo za pogoja „sodnih aktov“ in „preprečevanja goljufij“ (odstavka 7 oziroma 8 dodatka 8). Oba veljata le za posebne upravljavce. Le sodišče ali drug pravosodni organ lahko uporabi pogoj sodnih aktov in le upravljavci, ki so organizacije za boj proti goljufijam, se lahko sklicujejo na pogoj preprečevanja goljufij.

(42) Nazadnje, kadar se obdelava opira na enega od pogojev iz dodatka 8 oziroma je skladna s členom 42 k zakonu o varstvu podatkov iz leta 2018, mora biti sestavljen dokument o ustrezni politiki, v katerem so pojasnjeni postopki upravljavca za zagotavljanje skladnosti z načeli o varstvu podatkov in njegova politika glede hrambe in izbrisa osebnih podatkov, in uporabljajo se obveznosti razširjene evidence.

2.4.2 *Omejitev namena*

(43) Osebni podatki bi se morali obdelovati za določen namen in se nato uporabljati samo, če to ni nezdružljivo z namenom obdelave. To načelo o varstvu podatkov je zagotovljeno s členom 36 zakona o varstvu podatkov iz leta 2018. Ta določba podobno kot člen 4(1)(b) Direktive (EU) 2016/680 zahteva, da (a) mora biti namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za katerega so osebni podatki zbrani, vsakič določen, izrecen in zakonit ter (b) da se tako zbrani osebni podatki ne smejo obdelovati na način, ki je nezdružljiv z namenom, za katerega so bili zbrani.

(44) Kadar pristojni organi obdelujejo podatke za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, lahko to zajema namene arhiviranja, znanstveno- ali zgodovinskoraziskovalne namene in statistične namene ([73]). V takih primerih je v zakonu o varstvu podatkov iz leta 2018 tudi pojasnjeno, da arhiviranje (ali obdelava za znanstveno- ali zgodovinskoraziskovalne namene in statistične namene) ni dovoljeno, kadar se izvaja v zvezi z odločitvami, sprejetimi glede določenega posameznika, na katerega se nanašajo osebni podatki, ali če je verjetno, da bi mu to povzročilo znatno škodo ali stisko ([74]).

2.4.3 *Točnost in najmanjši obseg podatkov*

(45) Podatki morajo biti točni in, kjer je to potrebno, ažurirani. Podatki morajo biti tudi ustrezni, relevantni in ne smejo presegati namenov, za katere se obdelujejo. Ta načela so podobno, kot je določeno v členu 4(1)(c), (d) in (e) Direktive (EU) 2016/680, zagotovljena s členoma 37 in 38 zakona o varstvu podatkov iz leta 2018. Sprejeti je treba vse razumne korake, da bi se netočni osebni podatki ([75]) čim prej izbrisali ali

([71]) Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, „Pogoji za obdelavo občutljivih podatkov“ (glej opombo 70).

([72]) Obdelava se izvede brez privolitve posameznika, na katerega se nanašajo osebni podatki, kadar: (a) posameznik, na katerega se nanašajo osebni podatki, ne more privoliti v obdelavo, (b) se od upravljavca ne more razumno pričakovati, da bo pridobil privolitev posameznika, na katerega se nanašajo osebni podatki, v obdelavo, in (c) se mora obdelava izvesti brez privolitve posameznika, na katerega se nanašajo osebni podatki, saj bi njegova privolitev posegala v zagotavljanje zaščite iz pododstavka (1)(a).

([73]) Glej člen 41(1) zakona o varstvu podatkov iz leta 2018.

([74]) Glej člen 41(2) zakona o varstvu podatkov iz leta 2018.

([75]) V členu 205 zakona o varstvu podatkov iz leta 2018 je pojem „netočni“ opredeljen kot „nepravilni ali zavajajoči“ osebni podatki. Organi Združenega kraljestva so pojasnili, da je običajno, da so podatki, povezani s kazenskimi preiskavami, pogosto nepopolni, a so lahko ne glede na to točni.

popravili ([76]), pri čemer se upošteva namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za katerega se obdelujejo ([77]), ter da bi se zagotovilo, da se osebni podatki, ki so netočni, nepopolni ali neposodobljeni, ne posredujejo ali dajo na voljo za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([78]).

(46) V ureditvi varstva podatkov Združenega kraljestva je nadalje podobno kot v členu 7 Direktive (EU) 2016/680 določeno, da se osebni podatki, ki temeljijo na dejstvih, v največji možni meri razločijo od osebnih podatkov, ki temeljijo na osebnih ocenah ([79]). Kjer je to ustrezno in če je mogoče, je treba uvesti jasno razlikovanje med osebnimi podatki, ki se nanašajo na različne kategorije posameznikov, na katere se nanašajo osebni podatki, kot so osumljenci, osebe, obsojene za kaznivo dejanje, žrtve kaznivega dejanja in priče ([80]).

2.4.4 *Omejitev hrambe*

(47) V skladu s členom 5 Direktive (EU) 2016/680 se osebni podatki načeloma ne bi smeli hraniti dlje, kot je potrebno za namene, za katere se obdelujejo. V skladu s členom 39 zakona o varstvu podatkov iz leta 2018 in podobno kot v členu 5 navedene direktive je obdelane osebne podatke za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj prepovedano hraniti dlje, kot je potrebno za namen, za katerega se obdelujejo. V pravni ureditvi v Združenem kraljestvu je zahteva, da morajo biti določeni ustrezni časovni roki za reden pregled potrebe po nadaljnji hrambi osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Dodatna pravila o praksah, povezanih s hrambo osebnih podatkov, in uporabljenih časovnih rokih so bila določena v ustrezni zakonodaji in smernicah, ki urejajo pristojnosti in delovanje policije. V Angliji in Walesu je na primer s kodeksom ravnanja pri upravljanju policijskih informacij, ki ga je izdal strokovni organ uslužbencev policije, in smernicami o dovoljeni strokovni praksi pri upravljanju policijskih informacij zagotovljen okvir za dosledni postopek hrambe, pregleda in odstranjevanja na osnovi tveganja za upravljanje informacij pri operativnem policijskem delu ([81]). Ta okvir določa jasna pričakovanja v vseh službah policije, glede načina oblikovanja, izmenjave, uporabe in upravljanja informacij v posameznih policijskih enotah in drugih agencijah in med njimi ([82]). Pričakuje se, da policija ravna v skladu s kodeksom ravnanja, skladnost pa preverja inšpektorat policije in gasilsko-reševalne službe Združenega kraljestva ([83]).

(48) Severnoirska policija (Police Service of Northern Ireland) ni zakonsko obvezana upoštevati kodeksa ravnanja glede upravljanja policijskih informacij. Vendar je okvir kodeksa, sprejetega leta 2011, dopolnjen s priročnikom za severnoirsko policijo ([84]), ki določa politike in postopke o načinu uporabe navedenega kodeksa na Severnem Irskem.

([76]) Člen 38(1)(b) zakona o varstvu podatkov iz leta 2018.

([77]) V obrazložitvenem okviru Združenega kraljestva za razpravo o ustreznosti je navedeno: „to zagotavlja, da so priznane pravice posameznikov, na katere se nanašajo osebni podatki, in operativne potrebe organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Zgornja točka je bila med pripravo osnutka zakona o varstvu podatkov pozorno proučena, saj lahko obstajajo specifični in omejeni operativni razlogi, zakaj podatkov ni mogoče popraviti. To se najverjetneje zgodi v primeru, če se morajo zadevni netočni osebni podatki ohraniti v prvotni obliki za dokazne namene," (glej obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, stran 21 (glej opombo 9)).

([78]) Člen 38(4) zakona o varstvu podatkov iz leta 2018. Poleg tega je treba v skladu s členom 38(5) zakona o varstvu podatkov iz leta 2018 preveriti kakovost osebnih podatkov, še preden se jih posreduje ali da na voljo, vsako posredovanje osebnih podatkov pa se opremi s potrebnimi informacijami, ki prejemniku omogočijo, da oceni stopnjo točnosti, popolnosti in zanesljivosti podatkov, in mora vključevati stopnjo posodobljenosti, vendar če se po pošiljanju osebnih podatkov izkaže, da so bili poslani nepravilni podatki ali da posredovanje ni bilo zakonito, je treba prejemnika o tem takoj uradno obvestiti.

([79]) Člen 38(2) zakona o varstvu podatkov iz leta 2018.

([80]) Člen 38(3) zakona o varstvu podatkov iz leta 2018.

([81]) S tem okvirom se zagotavlja skladna hramba pridobljenih osebnih podatkov. Obdobje pregleda je odvisno od kaznivih dejanj, ki so razdeljena v štiri skupine: (1) določene zadeve, povezane z zaščito javnosti; (2) druga nasilna in huda kazniva dejanja zoper spolno nedotakljivost, (3) vsa druga kazniva dejanja in (4) razno. Več podrobnosti je na voljo v smernicah o dovoljeni strokovni praksi glede upravljanja policijskih informacij (glej opombo 26).

([82]) Druge organizacije se lahko glede na informacije organov Združenega kraljestva svobodno odločajo, ali bodo upoštevale načela kodeksa ravnanja glede upravljanja policijskih informacij, na primer davčna in carinska uprava Združenega kraljestva in nacionalna agencija za boj proti kriminalu prostovoljno sprejemata številna načela navedenega kodeksa zaradi doslednosti na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Na splošno večina organizacij zaposlenim zagotavlja posebne politike in smernice za vse zaposlene o načinu obravnavanja osebnih podatkov v okviru njihove vloge, ki so prilagojene posebni organizaciji. To običajno vključuje tudi obvezno usposabljanje.

([83]) Kodeks ravnanja pri upravljanju policijskih informacij je bil izdan z uporabo pooblastil iz zakona o policiji iz leta 1996, ki strokovnemu organu uslužbencev policije omogoča, da izdaja kodekse ravnanja v zvezi z učinkovitim delovanjem policijskega dela. Vsak kodeks ravnanja, izdan na podlagi tega zakona, mora odobriti pristojni minister, preden je predložen parlamentu, pa se je o njem treba posvetovati z nacionalno agencijo za boj proti kriminalu. Člen 39A(7) zakona o policiji iz leta 1996 določa, da mora policija ustrezno upoštevati kodekse, izdane na podlagi navedenega zakona.

([84]) Poglavja 1–6 priročnika za severnoirsko policijo h kodeksu ravnanja glede upravljanja policijskih informacij.

(49) Policija na Škotskem se sklicuje na standardni postopek delovanja za shranjevanje evidenc (Record Retention Standard Operating Procedure) ([85]), ki podpira politiko upravljanja evidenc škotske policije ([86]). V tem postopku delovanja so določena posebna pravila za hrambo evidenc s strani škotske policije.

(50) Poleg splošne zahteve po pregledu evidenc, ki se uporablja za celotno Združeno kraljestvo, so nadaljnje podrobnosti določene v lokalnih predpisih. Za nekaj primerov v zvezi z Anglijo in Walesom je v zakonu o policijskih dokazih in dokazih v kazenskih postopkih, kakor je bil spremenjen z zakonom o varstvu svoboščin iz leta 2012, navedena določba o hrambi prstnih odtisov in profilov DNA ter posebna ureditev za posameznike, ki niso obsojeni ([87]). Z navedenim zakonom o varstvu svoboščin je bil tudi vzpostavljen položaj pooblaščenca za hrambo in uporabo biometričnih podatkov (Commissioner for the Retention and Use of Biometric Material) (v nadaljnjem besedilu: pooblaščenec za biometrične podatke) ([88]). Posebna pravila o fotografijah, posnetih ob odvzemu prostosti, so določena v pregledu fotografij, posnetih ob odvzemu prostosti, iz leta 2017 ([89]). Glede Škotske so v zakonu o kazenskem postopku (Škotska) iz leta 1995 določena pravila za odvzem in hrambo prstnih odtisov in bioloških vzorcev ([90]). Tudi tu je z zakonodajo kot v Angliji in Walesu urejena hramba biometričnih podatkov v različnih primerih ([91]).

2.4.5 *Varnost podatkov*

(51) Osebni podatki se morajo obdelovati tako, da se zagotavlja njihovo varovanje, kar zajema tudi zaščito pred nepooblaščeno ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem. Zato morajo javni organi sprejeti ustrezne tehnične ali organizacijske ukrepe za varovanje osebnih podatkov pred morebitnimi grožnjami. Navedeni ukrepi se morajo presojati glede na najsodobnejšo tehnologijo in zadevne stroške.

(52) Ta načela se izražajo v členu 40 zakona o varstvu podatkov iz leta 2018, v skladu s katerim se morajo podobno kot v členu 4(1)(f) Direktive (EU) 2016/680 osebni podatki, ki se obdelujejo za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obdelati na način, ki zagotavlja ustrezno varnost osebnih podatkov, pri čemer se uporabijo ustrezni tehnični ali organizacijski ukrepi. To zajema ustrezno varstvo podatkov, tudi pred

([85]) Standardni postopek delovanja za shranjevanje evidenc je na voljo na povezavi: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Več podrobnosti o upravljanju evidenc je na voljo v informacijah, povezanih z nacionalnim registrom Škotske (National Records of Scotland) na povezavi: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Obdobja hrambe se razlikujejo glede na to, ali je posameznik obsojen ali ne (členi 63I–63KI zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Medtem ko se lahko na primer prstni odtisi in profil DNK odrasle osebe, obsojene za kaznivo dejanje, ki se vpiše v kazensko evidenco, hranijo za nedoločen čas (člen 63I(2) zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984), je hramba časovno omejena, če je obsojena oseba mlajša od 18 let, je kaznivo dejanje „manjše“ kaznivo dejanje, ki se vpiše v kazensko evidenco, in oseba še ni bila obsojena (člen 63K zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Hramba v primeru osebe, ki ji je bila odvzeta prostost ali je bila obtožena, ni pa bila obsojena, je omejena na tri leta (člen 63F zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Podaljšanje tega obdobja hrambe mora odobriti pravosodni organ (člen 63F(7) zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). V primeru osebe, ki ji je bila odvzeta prostost ali je bila obtožena, ni pa bila obsojena za prekršek, podatkov ni mogoče hraniti (člena 63D in 63H zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984).

([88]) S členom 20 zakona o varstvu svoboščin iz leta 2012 se vzpostavlja položaj pooblaščenca za biometrične podatke. Med nalogami tega pooblaščenca je odločanje, ali lahko policija evidenco profilov DNK in prstne odtise, odvzete posameznikom, ki jim je bila odvzeta prostost, niso pa bili obsojeni za kaznivo dejanje, ki ga je mogoče kvalificirati, hrani ali ne (člen 63G zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Splošna odgovornost pooblaščenca za biometrične podatke je tudi, da redno preverja hrambo in uporabo DNK in prstnih odtisov ter hrambo na podlagi nacionalne varnosti (člen 20(2) zakona o varstvu svoboščin iz leta 2012). Pooblaščenec za biometrične podatke je imenovan na podlagi kodeksa za imenovanje na javne funkcije (kodeks je na voljo na naslednji povezavi: Kodeks upravljanja za imenovanja na javne funkcije – GOV.UK (www.gov.uk)) in pogoji njegovega imenovanja jasno določajo, da ga lahko razreši minister za notranje zadeve le na podlagi ozko opredeljenega sklopa okoliščin; te okoliščine vključujejo neizpolnjevanje njegovih dolžnosti za obdobje treh mesecev, obsodbo zaradi storitve kaznivega dejanja ali nespoštovanje njegovega mandata.

([89]) Pregled uporabe in hrambe fotografij, posnetih ob policijskem pridržanju (Review of the Use and Retention of Custody Images) je na voljo na povezavi: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Člen 18 in naslednji zakona o kazenskem postopku (Škotska) iz leta 1995.

([91]) Obdobja hrambe se razlikujejo glede na to, ali je bila oseba obsojena (člen 18(3) zakona o kazenskem postopku (Škotska) iz leta 1995) in ali je mladoletna ali ne. V tem zadnjem primeru je obdobje hrambe tri leta od obsodbe v sodni obravnavi, v kateri je udeležen otrok (člen 18E(8) zakona o kazenskem postopku (Škotska) iz leta 1995). Podatki oseb, ki jim je bila odvzeta prostost, niso pa bile obsojene, se ne smejo hraniti (člen 18(3) zakona o kazenskem postopku (Škotska) iz leta 1995), razen v posebnih primerih in odvisno od teže kaznivega dejanja (člen 18A zakona o kazenskem postopku (Škotska) iz leta 1995). Zakon o škotskem pooblaščencu za biometrične podatke iz leta 2020 (Scottish Biometrics Commissioner Act 2020) (glej https://www.legislation.gov.uk/asp/2020/8/contents) vzpostavlja položaj škotskega komisarja za biometrične podatke, ki mora pripravljati in revidirati kodekse ravnanja o odvzemu, hrambi, uporabi in uničenju biometričnih podatkov (ki jih odobri škotski parlament) za namene kazenskega pravosodja in policijske namene (člen 7 zakona o škotskem komisarju za biometrične podatke iz leta 2020).

nepooblaščeno ali nezakonito obdelavo ter nenamerno izgubo, uničenjem ali poškodovanjem ([92]). V členu 66 zakona o varstvu podatkov iz leta 2018 je določeno še, da morata vsak upravljavec in vsak obdelovalec izvesti ustrezne tehnične in organizacijske ukrepe, da se zagotovi ustrezna raven varnosti glede na tveganja, ki izhajajo iz obdelave osebnih podatkov. Upravljavec mora v skladu s pojasnjevalnimi opombami oceniti tveganja in na podlagi te ocene uvesti ustrezne varnostne ukrepe, kot je na primer šifriranje ali varnostno dovoljenje ustrezne stopnje za osebje, ki obdeluje podatke ([93]). Pri oceni je treba na primer tudi upoštevati naravo obdelanih podatkov in druge pomembne dejavnike ali okoliščine, ki bi lahko vplivali na varnost obdelave.

(53) Ureditev, ki ureja skladnost z načeli varstva podatkov, je zelo podobna ureditvi, vzpostavljeni s členi 29 do 31 Direktive (EU) 2016/680. V členu 67(1) zakona o varstvu podatkov iz leta 2018 je zlasti v primeru kršitve varnosti osebnih podatkov, povezane z osebnimi podatki, za katere je odgovoren upravljavec, določeno, da mora upravljavec brez nepotrebnega odlašanja in, kadar je to izvedljivo, v 72 urah po seznanitvi s kršitvijo tako kršitev priglasiti informacijskemu pooblaščencu ([94]). Obveznost priglasitve se ne uporablja, kadar ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznikov ([95]). Upravljavec mora dejstva, ki se nanašajo na vsako kršitev varnosti osebnih podatkov, njene učinke in sprejete popravne ukrepe, dokumentirati tako, da lahko informacijski pooblaščenec preveri skladnost z zakonom o varstvu podatkov ([96]). Če se obdelovalec seznani s kršitvijo varnosti, mora to nemudoma priglasiti upravljavcu ([97]).

(54) Če bi kršitev varnosti osebnih podatkov verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec v skladu s členom 68(1) zakona o varstvu podatkov iz leta 2018 posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja obvestiti o kršitvi ([98]). Obvestilo mora vsebovati enake informacije kot priglasitev informacijskemu pooblaščencu iz uvodne izjave (53). Ta obveznost ne velja, če je upravljavec izvedel ustrezne tehnične in organizacijske zaščitne ukrepe, ki so se uporabili za osebne podatke, na katere je vplivala kršitev. Prav tako ne velja, če je upravljavec sprejel poznejše ukrepe za zagotovitev, da ni več verjetnosti, da bi se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, uresničilo. Upravljavcu ni treba obvestiti posameznika, na katerega se nanašajo osebni podatki, v primeru, ki bi vključeval nesorazmeren napor ([99]). V tem primeru je treba posamezniku, na katerega se nanašajo osebni podatki, informacije dati na voljo na drug, enakomerno učinkovit način, na primer prek javnih komunikacijskih sredstev ([100]). Če upravljavec posameznika, na katerega se nanašajo osebni podatki, ni obvestil o kršitvi, lahko informacijski pooblaščenec, ki mu je bila kršitev priglašena v skladu s členom 67 zakona o varstvu podatkov, po proučitvi verjetnosti, da bi kršitev povzročila veliko tveganje, od upravljavca zahteva, da takega posameznika uradno obvesti o kršitvi ([101]).

([92]) Upravljavec mora v skladu s pojasnjevalnimi opombami k zakonu o varstvu podatkov iz leta 2018 (glej opombo 45) zlasti: oblikovati in organizirati njihovo varnost, da bo ustrezala naravi shranjenih osebnih podatkov in škode, ki lahko nastane zaradi kršitve varnosti; jasno navesti, kdo v njihovi organizaciji je pristojen za zagotavljanje varnosti informacij; poskrbeti za pravilno fizično in tehnično varovanje, podprto z zanesljivimi politikami in postopki, ter zanesljive in dobro usposobljene zaposlene, ter biti pripravljen, da se hitro in učinkovito odzove na vsako kršitev varovanja tajnosti.

([93]) Odstavek 221 pojasnjevalnih opomb k zakonu o varstvu podatkov iz leta 2018 (glej opombo 45).

([94]) V členu 67(4) zakona o varstvu podatkov iz leta 2018 je določeno, da je treba v priglasitev vključiti opis vrste kršitve varnosti osebnih podatkov (po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov), ime in kontaktne podatke kontaktne osebe, opis verjetnih posledic kršitve varnosti osebnih podatkov in opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varnosti osebnih podatkov (vključno z, če je to primerno, ukrepi za ublažitev morebitnih škodljivih učinkov kršitve).

([95]) Člen 67(2) zakona o varstvu podatkov iz leta 2018.

([96]) Člen 67(6) zakona o varstvu podatkov iz leta 2018.

([97]) Člen 67(9) zakona o varstvu podatkov iz leta 2018.

([98]) Upravljavec lahko v skladu s členom 68(7) zakona o varstvu podatkov iz leta 2018 v celoti ali delno omeji zagotavljanje informacij posamezniku, na katerega se nanašajo osebni podatki, če in dokler je taka omejitev, ki mora spoštovati temeljne pravice in zakonite interese posameznika, na katerega se nanašajo osebni podatki, nujen in sorazmeren ukrep za (a) preprečitev oviranja uradne ali zakonite preiskave, poizvedbe ali postopka, (b) preprečitev vplivanja na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, (c) zaščito javne varnosti, (d) zaščito nacionalne varnosti, (e) zaščito pravic in svoboščin drugih.

([99]) Člen 68(3) zakona o varstvu podatkov iz leta 2018.

([100]) Člen 68(5) zakona o varstvu podatkov iz leta 2018.

([101]) Člen 68(6) zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 68(8) zakona o varstvu podatkov iz leta 2018).

2.4.6 *Preglednost*

(55) Posamezniki, na katere se nanašajo osebni podatki, morajo biti obveščeni o glavnih značilnostih obdelave njihovih osebnih podatkov. To načelo o varstvu podatkov se kaže v členu 44 zakona o varstvu podatkov iz leta 2018, v katerem je podobno kot v členu 13 Direktive (EU) 2016/680) določeno, da je splošna dolžnost upravljavca, da posameznikom, na katere se nanašajo osebni podatki, zagotavlja informacije o obdelavi njihovih osebnih podatkov (z zagotovitvijo splošnega dostopa javnosti do informacij ali kako drugače) ([102]). Informacije, ki se dajo na voljo, zajemajo (a) identiteto in kontaktne podatke upravljavca, (b) kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja, (c) namene obdelave osebnih podatkov, (d) o pravici posameznikov, na katere se nanašajo osebni podatki, da od upravljavca zahtevajo dostop do osebnih podatkov, popravek in izbris osebnih podatkov ali omejitev njihove obdelave, ter (e) o pravici do vložitve pritožbe pri informacijskem pooblaščencu in njegove kontaktne podatke ([103]).

(56) Upravljavec mora v posebnih primerih, da omogoči uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, v skladu za zakonom o varstvu podatkov iz leta 2018 (na primer ko so bili osebni podatki, ki se obdelujejo, zbrani brez vednosti posameznika, na katerega se nanašajo osebni podatki), takemu posamezniku tudi zagotoviti informacije o (a) pravni podlagi za obdelavo, (b) obdobju hrambe osebnih podatkov ali, če to ni mogoče, merilih, ki se uporabijo za določitev tega obdobja, in (c) če je ustrezno, o kategorijah uporabnikov osebnih podatkov (vključno z uporabniki v tretjih državah ali mednarodnih organizacijah), ter (d) nadaljnje informacije, ki so potrebne, da se omogoči uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, v skladu z delom 3 zakona o varstvu podatkov iz leta 2018 ([104]).

2.4.7 *Pravice posameznikov*

(57) Posameznikom, na katere se nanašajo osebni podatki, mora biti podeljenih več izvršljivih pravic. Posameznikom so v poglavju 3 dela 3 zakona o varstvu podatkov iz leta 2018 podeljene pravice do dostopa, popravka in izbrisa in omejitve ([105]), ki so primerljive s pravicami iz poglavja 3 Direktive (EU) 2016/680.

(58) Pravica do dostopa je določena v členu 45 zakona o varstvu podatkov iz leta 2018. Prvič, posameznik je upravičen, da od upravljavca pridobi potrditev, ali se njegovi osebni podatki obdelujejo ali ne ([106]). Drugič, če se osebni podatki obdelujejo, ima posameznik, na katerega se nanašajo osebni podatki, pravico do dostopa do teh podatkov in prejema teh informacij o obdelavi: (a) o namenih in pravnih podlagah za obdelavo, (b) o kategorijah zadevnih podatkov, (c) o prejemniku, ki so mu bili podatki razkriti, (d) o obdobju hrambe osebnih podatkov, (e) o obstoju pravice posameznika, na katerega se nanašajo osebni podatki, do popravka in izbrisa osebnih podatkov, (f) o pravici do vložitve pritožbe in (g) o informacijah o izvoru zadevnih osebnih podatkov ([107]).

(59) Posameznik, na katerega se nanašajo osebni podatki, ima v skladu s členom 46 zakona o varstvu podatkov iz leta 2018 pravico zahtevati, da upravljavec popravi netočne osebne podatke v zvezi z njim. Upravljavec mora podatke brez nepotrebnega odlašanja popraviti (ali kadar so podatki netočni, ker niso popolni, dopolniti). Če je treba osebne podatke ohraniti za namene dokazovanja, mora upravljavec (namesto njihovega popravka) omejiti njihovo obdelavo ([108]).

([102]) V smernicah za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj je naveden ta primer: „Na spletnem mestu imate splošno obvestilo o zasebnosti, ki zajema osnovne informacije o organizaciji, namenu obdelave osebnih podatkov, pravicah posameznika, na katerega se nanašajo osebni podatki, in njegovi pravici do pritožbe pri informacijskem pooblaščencu. Prejeli ste obveščevalne podatke, da je bil posameznik prisoten, ko je bilo storjeno kaznivo dejanje. Temu posamezniku morate med prvim zaslišanjem zagotoviti splošne informacije in dodatne podporne informacije, da bi lahko uveljavljal svoje pravice. Pošteno obdelavo informacij, ki jo zagotavljate, lahko omejite le, če bo negativno vplivala na začeto preiskavo“ (smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Katere informacije moramo zagotoviti posamezniku?“, na voljo na povezavi: 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 smernicah za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj je navedeno, da morajo biti zagotovljene informacije o obdelavi osebnih podatkov v jedrnati, razumljivi in lahko dostopni obliki, morajo biti napisane v jasnem in preprostem jeziku, prilagojenem potrebam ciljnih uporabnikov, kot so otroci, in morajo biti na voljo brezplačno (smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Kako moramo zagotavljati te informacije?“, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Člen 44(2) zakona o varstvu podatkov iz leta 2018.

([105]) Za podrobno analizo pravic posameznika glej smernice glede pravic posameznika v zvezi z obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Člen 45(1) zakona o varstvu podatkov iz leta 2018.

([107]) Člen 45(2) zakona o varstvu podatkov iz leta 2018.

([108]) Člen 46(4) zakona o varstvu podatkov iz leta 2018.

(60) Člen 47 zakona o varstvu podatkov iz leta 2018 posameznikom zagotavlja pravico do izbrisa in omejitve obdelave. Upravljavec mora ([109]) brez nepotrebnega odlašanja izbrisati osebne podatke, če bi njihova obdelava kršila katero koli načelo o varstvu podatkov, pravno podlago za obdelavo ali zaščitne ukrepe, povezane z arhiviranjem in občutljivo obdelavo podatkov. Upravljavec mora podatke izbrisati tudi, če je to obvezno po zakonu. Če je treba osebne podatke ohraniti za namene dokazovanja, mora upravljavec (namesto njihovega izbrisa) omejiti njihovo obdelavo ([110]). Upravljavec mora omejiti obdelavo osebnih podatkov, če posameznik, na katerega se nanašajo osebni podatki, izpodbija njihovo točnost in ni mogoče preveriti, ali so podatki točni ali ne ([111]).

(61) Kadar posameznik, na katerega se nanašajo osebni podatki, zahteva popravek ali izbris osebnih podatkov ali omejitev njihove uporabe, ga mora upravljavec pisno obvestiti, ali je odobril zahtevo, v primeru zavrnitve pa o razlogih za zavrnitev in razpoložljivih pravnih sredstvih (pravici posameznika, na katerega se nanašajo osebni podatki, do vložitve zahtevka pri informacijskem pooblaščencu za preiskavo glede zakonitosti uporabe omejitve, pravico do vložitve pritožbe pri informacijskem pooblaščencu in pravico do vložitve vloge pri sodišču za izdajo odločbe o izpolnitvi obveznosti) ([112]).

(62) Če upravljavec popravi osebne podatke, ki jih je prejel od drugega pristojnega organa, mora to priglasiti drugemu organu ([113]). Če upravljavec popravi ali izbriše osebne podatke, ki jih je razkril, ali omeji njihovo uporabo, mora o tem uradno obvestiti prejemnike, ti pa morajo podobno popraviti ali izbrisati osebne podatke ali omejiti njihovo uporabo (če ohranijo odgovornost za to) ([114]).

(63) Poleg tega ima posameznik, na katerega se nanašajo osebni podatki, pravico, da ga upravljavec brez nepotrebnega odlašanja obvesti o kršitvi varnosti osebnih podatkov, če bi ta kršitev verjetno povzročila veliko tveganje za pravice in svoboščine posameznika ([115]).

(64) Upravljavec mora v zvezi v vsemi navedenimi pravicami posameznika, na katerega se nanašajo osebni podatki, in podobno kot v določbah člena 12 Direktive (EU) 2016/680 zagotoviti, da se posamezniku, na katerega se nanašajo osebni podatki, vse informacije posredujejo v jedrnati, razumljivi in lahko dostopni obliki ([116]) ter po možnosti v jasnem in preprostem jeziku ([117]). Upravljavec mora zahtevi posameznika, na katerega se nanašajo osebni podatki, ugoditi brez nepotrebnega odlašanja in načeloma vsekakor v enem mesecu od njenega prejetja ([118]). Če upravljavec upravičeno dvomi o identiteti posameznika, lahko zahteva zagotovitev dodatnih informacij in odloži obravnavo zahteve, dokler ni ugotovljena identiteta. Upravljavec lahko zahteva razumno pristojbino ali zavrne ukrepanje, kadar meni, da je zahteva očitno neutemeljena ([119]). Urad informacijskega pooblaščenca je zagotovil smernice za primere, ko se zahteva šteje za očitno neutemeljeno ali pretirano ali ko se lahko zahteva pristojbina ([120]).

(65) Poleg tega lahko pristojni minister v skladu s členom 53(4) zakona o varstvu podatkov iz leta 2018 najvišji znesek pristojbine določi s predpisi.

([109]) Posameznik, na katerega se nanašajo osebni podatki, lahko od upravljavca zahteva, da izbriše osebne podatke ali omeji njihovo obdelavo (vendar mora upravljavec obveznosti, da izbriše podatke ali omeji njihovo obdelavo, izvajati ne glede na to, ali je podan tak zahtevek ali ne).

([110]) Člena 46(4) in 47(2) zakona o varstvu podatkov iz leta 2018.

([111]) Člen 47(3) zakona o varstvu podatkov iz leta 2018.

([112]) Člen 48(1) zakona o varstvu podatkov iz leta 2018.

([113]) Člen 48(7) zakona o varstvu podatkov iz leta 2018.

([114]) Člen 48(9) zakona o varstvu podatkov iz leta 2018.

([115]) Člen 68 zakona o varstvu podatkov iz leta 2018.

([116]) Člen 52(1) zakona o varstvu podatkov iz leta 2018.

([117]) Člen 52(3) zakona o varstvu podatkov iz leta 2018.

([118]) V členu 54 zakona o varstvu podatkov iz leta 2018 je opredeljen pomen pojma „veljavni rok“, ki pomeni obdobje enega meseca ali daljše obdobje, kot je lahko določeno v predpisih, ki se začne ob ustreznem času (ko upravljavec prejme zadevno zahtevo, ko upravljavec prejme (morebitne) informacije, zahtevane v zvezi z zahtevo iz člena 52(4) zakona o varstvu podatkov, ali ko je plačana (morebitna) pristojbina, zaračunana v zvezi z zahtevo iz člena 53 zakona o varstvu podatkov).

([119]) Člen 53(1) zakona o varstvu podatkov iz leta 2018.

([120]) Upravljavec se lahko na podlagi smernic urada informacijskega pooblaščenca odloči, da posamezniku, na katerega se nanašajo osebni podatki, zaračuna pristojbino, če je njegova zahteva očitno neutemeljena ali pretirana, vendar nanjo vseeno odgovori. Pristojbina mora biti razuma in mora upravičiti strošek. Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Očitno neutemeljene in pretirane zahteve“, ki na voljo na povezavi: 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 Omejitve pravic posameznika, na katerega se nanašajo osebni podatki, in obveznosti glede preglednosti

(66) Pristojni organ lahko v določenih okoliščinah omeji določene pravice posameznika, na katerega se nanašajo osebni podatki, tj. pravico do dostopa ([121]), do obveščenosti ([122]), do seznanitve s kršitvijo varnosti osebnih podatkov ([123]) in do obveščenosti o razlogih za zavrnitev popravka ali izbrisa ([124]). Pristojni organ lahko podobno, kot je določeno v ureditvi iz poglavja III Direktive (EU) 2016/680, omejitev uporablja le, kadar je ob spoštovanju temeljnih pravic in zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, potrebna in sorazmerna za: (a) preprečitev oviranja uradne ali zakonite preiskave, poizvedbe ali postopka, (b) preprečitev vplivanja na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, (c) zaščito javne varnosti, (d) zaščito nacionalne varnosti, (e) zaščito pravic in svoboščin drugih.

(67) Urad informacijskega pooblaščenca je zagotovil smernice o uporabi navedenih omejitev. V skladu s temi smernicami morajo upravljavci izvajati analizo vsakega primera posebej, da uravnotežijo pravice posameznika s škodo, ki bi jo tako razkritje povzročilo. Vsako uporabljeno omejitev morajo zlasti utemeljiti kot potrebno in sorazmerno, omejijo pa lahko le tisto, kar je določeno, če bi škodovalo navedenim namenom ([125]).

(68) Pristojni organi so izdali tudi več drugih smernic s podrobnimi informacijami o vseh vidikih zakonodaje o varstvu podatkov, tudi o uporabi omejitve pravic posameznikov, na katere se nanašajo osebni podatki ([126]). Na primer v zvezi s členom 45(4) je v priročniku o varstvu podatkov sveta nacionalnih načelnikov policije navedeno: „Opozoriti je treba, da se lahko omejitve uporabljajo le, če je to potrebno, in le tako dolgo, kot je potrebno. Zato ni dovoljena vsesplošna uporaba omejitev za vse osebne podatke vložnika ali stalna uporaba omejitev. Pri tej drugi točki pogosto velja, da je treba osebne podatke, zbrane brez vednosti posameznika, na katerega se nanašajo osebni podatki, ki je osumljenec v preiskavi, sprva zavarovati pred razkritjem temu posamezniku, da se prepreči vplivanje na preiskovanje med potekom preiskave, da pa pozneje ne bi škodovalo, če bi bili posamezniku med informativnim razgovorom razkriti osebni podatki. Policija mora sprejeti postopke, ki zagotavljajo, da se te omejitve uporabljajo le, kolikor je potrebno, in le za potreben čas trajanja“ ([127]). V teh smernicah so tudi navedeni verjetni primeri uporabe posameznih omejitev ([128]).

(69) Nadalje, v zvezi z možnostjo omejitve uporabe navedenih posebnih pravic zaradi zaščite „nacionalne varnosti“, lahko upravljavec zaprosi za izdajo potrdila, ki ga podpiše vladni minister ali generalni državni tožilec (ali generalni pravobranilec za Škotsko) in ki potrjuje, da je omejitev takih pravic potreben in sorazmeren ukrep za zaščito nacionalne varnosti ([129]). Vlada Združenega kraljestva je izdala smernice za potrdila o omejitvah iz razlogov nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018, v katerih je zlasti poudarjeno, da mora biti vsaka omejitev pravic posameznika, na katerega se nanašajo osebni podatki, zaradi varovanja nacionalne varnosti sorazmerna in potrebna ([130]) (za več podrobnosti o potrdilih glede nacionalne varnosti glej uvodne izjave (131) do (134)).

([121]) Člen 45(4) zakona o varstvu podatkov iz leta 2018.
([122]) Člen 44(4) zakona o varstvu podatkov iz leta 2018.
([123]) Člen 68(7) zakona o varstvu podatkov iz leta 2018.
([124]) Člen 48(3) zakona o varstvu podatkov iz leta 2018.
([125]) Glej na primer smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj o pravici do dostopa, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Glej na primer priročnik o varstvu podatkov za strokovnjake na področju varstva policijskih podatkov, ki ga je izdal svet nacionalnih načelnikov policije (glej opombo 27), ali smernice urada za resne prevare (Serious Fraud Office), ki so na voljo na povezavi: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Priročnik o varstvu podatkov sveta nacionalnih načelnikov policije, stran 140 (glej opombo 27).
([128]) V priročniku o varstvu podatkov sveta nacionalnih načelnikov policije je določeno, da je verjetno, da bo „preprečitev oviranja uradnih ali zakonitih poizvedb, preiskav ali postopkov“ relevantna za osebne podatke, ki se obdelujejo za sodne preiskave, v postopkih pred družinskim sodiščem, za nekazenske preiskave notranje discipline in preiskave, kot je neodvisna preiskava spolne zlorabe otrok; med tem ko je „zaščita pravic in svoboščin drugih“ pomembna za osebne podatke, ki bi se nanašali tudi na druge posameznike in vložnika (priročnik o varstvu podatkov sveta nacionalnih načelnikov policije, stran 140, glej opombo 27).
([129]) Člen 79 zakona o varstvu podatkov iz leta 2018.
([130]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti (UK Government Guidance on National Security Certificates) so na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Kadar se uporablja omejitev pravic posameznika, na katerega se nanašajo osebni podatki, mora pristojni organ tega posameznika brez nepotrebnega odlašanja obvestiti o omejitvi njegovih pravic, razlogih za omejitev in razpoložljivih možnostih pravnih sredstev, razen če bi zagotovitev te informacije ogrozila razlog za uporabo omejitve ([131]). Upravljavec mora kot dodatni zaščitni ukrep pred zlorabo omejitev evidentirati razloge za omejitev informacij in na zahtevo dati te evidence na voljo informacijskemu pooblaščencu ([132]).

(71) Če upravljavec ne zagotovi dodatnih informacij o preglednosti ali dostopu ali zavrne prošnjo za popravek ali izbris osebnih podatkov ali omejitev njihove obdelave, lahko posameznik od informacijskega pooblaščenca zahteva, da prouči, ali je upravljavec omejitev uporabil zakonito ([133]). Zadevni posameznik se lahko tudi pritoži pri informacijskem pooblaščencu ali vloži zahtevek na sodišču, da upravljavcu odredi, naj izpolni zahtevo ([134]).

2.4.7.2 Avtomatizirano sprejemanje odločitev

(72) Člena 49 in 50 zakona o varstvu podatkov iz leta 2018 zajemata pravice, povezane z avtomatiziranim sprejemanjem odločitev, oziroma zaščitne ukrepe, ki se uporabljajo ([135]). Podobno kot je določeno v členu 11 Direktive (EU) 2016/680, lahko upravljavec sprejme pomembno odločitev izključno na podlagi avtomatizirane obdelave osebnih podatkov le, če to predpisuje ali dovoljuje zakon ([136]). Odločitev je pomembna, če bi imela negativen pravni učinek za posameznika, na katerega se nanašajo osebni podatki, ali bi ga zelo prizadela ([137]).

(73) Kadar zakon predpisuje ali dovoljuje, da mora upravljavec sprejeti pomembno odločitev, so v členu 50 zakona o varstvu podatkov iz leta 2018 določeni zaščitni ukrepi, ki se bodo uporabljali pri taki odločitvi (ki je opredeljena kot omejitvena pomembna odločitev). Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, uradno obvestiti o sprejetju take odločitve takoj, ko je to razumno izvedljivo. Posameznik, na katerega se nanašajo osebni podatki, lahko nato od upravljavca zahteva, da v enem mesecu ponovno prouči odločitev ali sprejme novo odločitev, ki ne temelji izključno na podlagi avtomatizirane obdelave. Upravljavec mora zahtevo proučiti in posameznika, na katerega se nanašajo osebni podatki, obvestiti o rezultatu proučitve. Zakon o varstvu podatkov iz leta 2018 daje pristojnemu ministru pristojnost, da sprejema predpise o dodatnih zaščitnih ukrepih ([138]). Tak predpis do zdaj še ni bil izdan.

2.4.8 *Nadaljnji prenosi*

(74) Raven varstva, ki se zagotavlja osebnim podatkom, prenesenim od organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj države članice organu za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v Združenem kraljestvu, se ne sme poslabšati z nadaljnjim prenosom takih podatkov prejemnikom v tretji državi. Taki „nadaljnji prenosi“ podatkov, ki z vidika organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v Združenem kraljestvu pomenijo mednarodni prenos iz Združenega kraljestva, bi morali biti dovoljeni le, kadar tudi za nadaljnjega prejemnika zunaj Združenega kraljestva veljajo pravila, ki zagotavljajo podobno raven varstva, kot je zagotovljena v okviru pravnega reda Združenega kraljestva.

([131]) Člen 44(5) in (6), člen 45(5) in (6) ter člen 48(4) zakona o varstvu podatkov iz leta 2018.
([132]) Člen 44(7), člen 45(7) in člen 48(6) zakona o varstvu podatkov iz leta 2018.
([133]) Člen 51 zakona o varstvu podatkov iz leta 2018.
([134]) Člen 167 zakona o varstvu podatkov iz leta 2018.
([135]) V pojasnjevalnih opombah k zakonu o varstvu podatkov iz leta 2018 je glede področja uporabe avtomatizirane obdelave navedeno, da: „se te določbe nanašajo na povsem avtomatizirano sprejemanje odločitev, ne pa na avtomatizirano obdelavo. Avtomatizirana obdelava (vključno z oblikovanjem profilov) poteka, ko je operacija izvedena, ne da bi bilo potrebno človeško posredovanje. To se na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pogosto uporablja, da se veliki nabori podatkov filtrirajo v obvladljive količine, ki jih lahko nato uporabi človeški operater. Pri avtomatiziranem sprejemanju odločitev, ki je oblika avtomatizirane obdelave, mora biti končna odločitev sprejeta brez človeškega posredovanja.“ (Pojasnjevalne opombe k zakonu o varstvu podatkov, odstavek 204, glej opombo 45.)
([136]) Poleg zaščite, ki jo zagotavlja zakon o varstvu podatkov, obstajajo v pravnem okviru Združenega kraljestva druge zakonodajne omejitve, ki se uporabljajo za organe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in bi preprečevale avtomatizirano obdelavo (vključno z oblikovanjem profilov), ki povzroča nezakonito diskriminacijo. Z zakonom o človekovih pravicah iz leta 1998 so v pravo Združenega kraljestva vključene pravice iz EKČP, vključno s pravico iz člena 14 Konvencije, ki se nanaša na prepoved diskriminacije. Podobno zakon o enakosti iz leta 2010 preprečuje diskriminacijo osebe z zaščitenimi lastnostmi (kar vključuje spol, raso, invalidnost ipd.)
([137]) Člen 49(2) zakona o varstvu podatkov iz leta 2018.
([138]) Člen 50(4) zakona o varstvu podatkov iz leta 2018.

(75) Ureditev Združenega kraljestva o mednarodnih prenosih ureja poglavje 5 dela 3 zakona o varstvu podatkov iz leta 2018 ([139]) in izraža pristop iz Poglavja V Direktive (EU) 2016/680. Za prenos osebnih podatkov v tretjo državo mora pristojni organ izpolnjevati zlasti tri pogoje, in sicer: (a) prenos mora biti potreben za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, (b) prenos mora temeljiti na: (i) predpisu o ustreznosti v zvezi s tretjo državo, (ii) če ne temelji na predpisu o ustreznosti, obstoju ustreznih zaščitnih ukrepov ali (iii), če ne temelji na sklepu o ustreznosti ali obstoju ustreznih zaščitnih ukrepov, na posebnih okoliščinah, ter (c) prejemnik prenosa mora biti: (i) ustrezen organ (ki je enakovreden pristojnemu organu) v tretji državi, (ii) ustrezna mednarodna organizacija, npr. mednarodni organ, ki izvaja naloge, ki ustrezajo kateremu koli namenu preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ali (iii) oseba, ki ni ustrezen organ, vendar le, kadar je prenos nujno potreben za izvajanje enega od namenov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj; kadar nobena temeljna pravica in svoboščina zadevnega posameznika, na katerega se nanašajo osebni podatki, ne prevlada nad javnim interesom, zaradi katerega je prenos potreben; kadar bi bil prenos osebnih podatkov ustreznemu organu v tretji državi neučinkovit ali neustrezen, in kadar je prejemnik obveščen o namenih, za katere se lahko podatki obdelujejo ([140]).

(76) Predpise o ustreznosti v zvezi s tretjo državo, ozemljem ali področjem znotraj tretje države, mednarodno organizacijo ali opisom ([141]) take države, ozemlja, področja ali organizacije izda pristojni minister. Ta mora, kar zadeva standard, ki ga je treba izpolniti, presoditi, ali tako ozemlje/področje/organizacija zagotavlja ustrezno raven varstva osebnih podatkov. V členu 74A(4) zakona o varstvu podatkov iz leta 2018 je določeno, da mora pristojni minister v ta namen proučiti številne elemente, ki izražajo elemente iz člena 36 Direktive (EU) 2016/680 ([142]). Od konca prehodnega obdobja je del 3 zakona o varstvu podatkov iz leta 2018 „domača zakonodaja, ki izhaja iz EU“, ki jo bodo, kot je bilo pojasnjeno, sodišča Združenega kraljestva razlagala v skladu z ustrezno sodno prakso Sodišča, sprejeto pred izstopom Združenega kraljestva iz Unije, in splošnimi načeli prava Unije, kot so učinkovala tik pred koncem prehodnega obdobja. To zajema standard, da je „v osnovi enakovredna“, ki se bo tako uporabljal pri ocenah ustreznosti, ki jih bodo izvedli organi Združenega kraljestva.

(77) Glede postopka se za predpise uporabljajo „splošne“ procesne zahteve iz člena 182 zakona o varstvu podatkov iz leta 2018. V skladu s tem postopkom se mora pristojni minister pred sprejetjem prihodnjih predpisov Združenega

([139]) Ta novi okvir se je začel uporabljati ob koncu prehodnega obdobja, vključno s pristojnostjo pristojnega ministra za sprejemanje predpisov o ustreznosti. Predpisi DPPEC (zlasti odstavki 10 do 12 dodatka 21, ki je bil s predpisi DPPEC vključen v zakon o varstvu podatkov iz leta 2018) določajo, da se med prehodnim obdobjem in po koncu tega obdobja nekateri prenosi osebnih podatkov obravnavajo, kot da temeljijo na predpisih o ustreznosti. Mednje spadajo prenosi v tretje države, za katere ob koncu prehodnega obdobja velja sklep EU o ustreznosti, ter v države članice EU, države Efte in na ozemlje Gibraltarja zaradi njihove uporabe direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj za obdelavo podatkov s področja preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (države Efte uporabljajo Direktivo (EU) 2016/680 zaradi svojih obveznosti na podlagi schengenskega pravnega reda). To pomeni, da se lahko ob koncu prehodnega obdobja prenosi v te države nadaljujejo kot pred izstopom iz EU. Po koncu prehodnega obdobja mora pristojni minister v štirih letih opraviti pregled teh ugotovitev glede ustreznosti.

([140]) Člena 73 in 77 zakona o varstvu podatkov iz leta 2018.

([141]) Organi Združenega kraljestva so pojasnili, da se opis države ali mednarodne organizacije nanaša na okoliščine, ko bi bilo treba izvesti specifično in delno oceno ustreznosti z določenimi omejitvami (na primer predpisi o ustreznosti, ki se nanašajo le na določeno vrsto prenosov podatkov).

([142]) Glej člen 74A(4) zakona o varstvu podatkov iz leta 2018, v katerem je določeno, da mora pri presoji ustreznosti ravni varstva „pristojni minister zlasti upoštevati (a) načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, ustrezno splošno in področno zakonodajo, tudi na področju javne varnosti, obrambe, nacionalne varnosti in kazenskega prava ter dostopa javnih organov do osebnih podatkov, pa tudi izvajanje take zakonodaje, pravila o varstvu podatkov, strokovna pravila ter varnostne ukrepe, vključno s pravili za nadaljnji prenos osebnih podatkov v drugo tretjo državo ali mednarodno organizacijo, ki se spoštujejo v navedeni tretji državi ali mednarodni organizaciji, sodno prakso, pa tudi dejanske in izvršljive pravice ter učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo; (b) obstoj enega ali več učinkovito delujočih neodvisnih nadzornih organov v tretji državi članici ali pristojnih za mednarodno organizacijo, ki so odgovorni za zagotavljanje in izvrševanje predpisov o varstvu podatkov, kar vključuje tudi ustrezna pooblastila za izvrševanje, za pomoč in svetovanje posameznikom, na katere se nanašajo osebni podatki, pri uresničevanju njihovih pravic ter za sodelovanje z nadzornimi organi držav članic, ter (c) mednarodne zaveze, ki jih je sprejela zadevna tretja država ali mednarodna organizacija, ali druge obveznosti, ki izhajajo iz pravno zavezujočih konvencij ali instrumentov, pa tudi iz sodelovanja države ali mednarodne organizacije v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov“.

kraljestva o ustreznosti posvetovati z informacijskim pooblaščencem ([143]). Ko pristojni minister sprejme navedene predpise, se jih predloži parlamentu, ki jih obravnava v postopku tako imenovane negativne potrditve, v katerem lahko oba domova parlamenta proučita predpise in jih v 40 dneh razveljavita ([144]).

(78) V skladu s členom 74 B(1) zakona o varstvu podatkov iz leta 2018 je treba predpise o ustreznosti preverjati na največ štiri leta, pristojni minister pa mora redno spremljati dogajanje v tretjih državah in mednarodnih organizacijah, ki bi lahko vplivalo na odločitve o sprejemanju predpisov o ustreznosti, njihovem spreminjanju ali odpravi. Če pristojni minister izve, da zadevna država ali organizacija ne zagotavlja več ustrezne ravni varstva osebnih podatkov, mora po potrebi spremeniti ali odpraviti navedene predpise ter se z zadevno tretjo državo ali mednarodno organizacijo posvetovati o izboljšanju ravni varstva.

(79) Podobno kot je določeno v členu 37 Direktive (EU) 2016/680, bi bil prenos osebnih podatkov v okviru sektorja preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če takih predpisov o ustreznosti ni, mogoč le, če so vzpostavljeni ustrezni zaščitni ukrepi. Taki zaščitni ukrepi so zagotovljeni (a) z zavezujočim pravnim instrumentom, ki vsebuje ustrezne zaščitne ukrepe za varstvo osebnih podatkov, ali (b) s presojo, ki jo opravi upravljavec, ki po presoji vseh okoliščin prenosa ugotovi, da obstajajo ustrezni zaščitni ukrepi za varstvo podatkov ([145]). Kadar prenosi temeljijo na ustreznih zaščitnih ukrepih, je v zakonu o varstvu podatkov iz leta 2018 prav tako določeno, da mora urad informacijskega pooblaščenca poleg svoje običajne nadzorne vloge od pristojnih organov prejemati posebne informacije o prenosih temu uradu ([146]).

(80) Če prenos ne temelji na sklepu o ustreznosti ali ustreznih zaščitnih ukrepih, se lahko izvede le v določenih, posebnih okoliščinah, imenovanih „posebne okoliščine“ ([147]). Na primer, kadar je prenos potreben: (a) za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe; (b) za zaščito zakonitih interesov posameznika, na katerega se nanašajo osebni podatki; (c) za preprečitev neposredne in resne grožnje javni varnosti v tretji državi; (d) v posameznih primerih za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali (e) v posameznem primeru iz pravnih razlogov (kot na primer v zvezi s sodnimi postopki ali za zagotavljanje pravnih nasvetov) ([148]). Opozorimo lahko, da se točki (d) in (e) ne uporabljata, če pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, prevladajo nad javnim interesom v prenosu ([149]). Te okoliščine ustrezajo posebnim razmeram in pogojem, ki so v skladu s členom 38 Direktive (EU) 2016/680 opredeljeni kot „odstopanja“.

(81) V takih primerih je treba dokumentirati datum, čas in utemeljitev prenosa, ime prejemnika in druge ustrezne informacije o njem in opis prenesenih osebnih podatkov ter te informacije na zahtevo zagotoviti informacijskemu pooblaščencu ([150]).

(82) Člen 78 zakona o varstvu podatkov iz leta 2018 ureja scenarij „nadaljnjih prenosov“, in sicer ko se osebni podatki, ki so bili preneseni iz Združenega kraljestva v tretjo državo, nato prenesejo v drugo tretjo državo ali mednarodno organizacijo. V skladu s členom 78(1) navedenega zakona mora upravljavec Združenega kraljestva, ki izvede prenos, ta prenos pogojiti z zahtevo, da se podatki ne smejo nadalje prenesti v tretjo državo brez dovoljenja upravljavca, ki izvede prenos. Poleg tega v skladu s členom 78(3) in podobno s tem, kar določa člen 35(1)(e) Direktive (EU) 2016/680, za vsak primer, v katerem je potrebno tako dovoljenje, velja vrsta vsebinskih zahtev.

([143]) Glej memorandum o soglasju med ministrom za digitalne tehnologije, kulturo, medije in šport (Secretary of State for the Department for Digital, Culture, Media and Sport) ter uradom informacijskega pooblaščenca o vlogi tega urada v zvezi z novo oceno ustreznosti Združenega kraljestva, ki je na voljo na naslednji povezavi: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Med tem 40-dnevnim obdobjem imata lahko oba domova parlamenta Združenega kraljestva možnost, da glasujeta proti predpisom, če tako želita; če je taka odločitev izglasovana, predpisi nimajo več nobenega nadaljnjega pravnega učinka.

([145]) Člen 75 zakona o varstvu podatkov iz leta 2018.

([146]) V skladu s členom 75(3) zakona o varstvu podatkov iz leta 2018, kadar se prenos podatkov opira na ustrezne zaščitne ukrepe: (a) mora biti prenos dokumentiran, (b) mora biti informacijskemu pooblaščencu na zahtevo zagotovljena dokumentacija in (c) mora dokumentacija zajemati zlasti (i) datum in čas prenosa, (ii) ime prejemnika in vse druge ustrezne informacije o njem, (iii) utemeljitev prenosa ter (iv) opis prenesenih osebnih podatkov.

([147]) Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Ali obstajajo posebne zahteve?“, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

([148]) Člen 76 zakona o varstvu podatkov iz leta 2018.

([149]) Člen 76 zakona o varstvu podatkov iz leta 2018.

([150]) Člen 76(3) zakona o varstvu podatkov iz leta 2018.

Konkretneje se mora pristojni organ pri odločanju o tem, ali bo prenos dovolil ali ne, prepričati, da je nadaljnji prenos potreben za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter mora med drugimi dejavniki razmisliti o (a) resnosti okoliščin, zaradi katerih je bilo zahtevano dovoljenje, (b) namenu prvotnega prenosa osebnih podatkov in (c) standardih varstva osebnih podatkov, ki se uporabljajo v tretji državi ali mednarodni organizaciji, v katero bi se prenesli osebni podatki.

(83) Poleg tega se za podatke, ki so bili prvotno preneseni iz Evropske unije in so predmet nadaljnjega prenosa iz Združenega kraljestva, uporabljajo dodatni zaščitni ukrepi.

(84) Prvič, člen 73(1)(b) zakona o varstvu podatkov iz leta 2018 – podobno kot člen 35(1)(c) Direktive (EU) 2016/680 – določa, da kadar je država članica osebne podatke prvotno poslala ali drugače dala na voljo upravljavcu ali drugemu pristojnemu organu, je ta država članica ali katera koli oseba s sedežem v tej državi članici, ki je pristojni organ za namene Direktive (EU) 2016/680, morala dovoliti prenos v skladu s pravom te države članice.

(85) Tako dovoljenje pa po vzoru člena 35(2) Direktive (EU) 2016/680 ni potrebno, če (a) je prenos potreben, da se prepreči neposredna in resna grožnja javni varnosti v državi članici ali tretji državi ali vitalnim interesom države članice, in (b) dovoljenja ni mogoče pridobiti pravočasno. V tem primeru mora biti brez odlašanja obveščen organ v državi članici, ki bi bil pristojen za odločanje o odobritvi prenosa ([151]).

(86) Drugič, enak pristop velja za podatke, ki so bili prvotno preneseni iz Evropske unije v Združeno kraljestvo, nato pa jih je Združeno kraljestvo nadalje preneslo v tretjo državo, ki bi jih nato nadalje prenesla v drugo tretjo državo. V tem primeru pristojni organ Združenega kraljestva na podlagi člena 78(4) ne more dovoliti zadnje omenjenega prenosa v skladu s členom 78(1), razen če je „država članica[, ki je prvotno prenesla zadevne podatke,] ali katera koli druga oseba s sedežem v tej državi članici, ki je pristojni organ za namene direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, dovolila prenos v skladu s pravom te države članice“. Ti zaščitni ukrepi so pomembni, ker organom držav članic omogočajo, da v skladu s pravom EU o varstvu podatkov zagotavljajo neprekinjenost zaščite v celotni „verigi prenosov“.

(87) Ta novi okvir glede mednarodnih prenosov podatkov se je začel uporabljati ob koncu prehodnega obdobja ([152]). Vendar odstavki 10 do 12 dodatka 21 (uvedenega s predpisi DPPEC) določajo, da se od konca prehodnega obdobja naprej nekateri prenosi osebnih podatkov obravnavajo, kot da temeljijo na predpisih o ustreznosti. Ti prenosi zajemajo prenos v državo članico, državo Efte, tretjo državo, za katero ob koncu prehodnega obdobja velja sklep EU o ustreznosti, in ozemlje Gibraltarja. Posledično se lahko prenosi v navedene države nadaljujejo kot pred izstopom Združenega kraljestva iz Unije. Po koncu prehodnega obdobja mora pristojni minister v štirih letih opraviti pregled teh ugotovitev glede ustreznosti, tj. do konca decembra 2024. Iz pojasnila organov Združenega kraljestva izhaja, da čeprav mora pristojni minister tak pregled opraviti do konca decembra 2024, pa prehodne določbe ne vključujejo samoderogacijske določbe in zadevne prehodne določbe samodejno ne prenehajo veljati, če pregled ni opravljen do konca decembra 2024.

2.4.9 *Odgovornost*

(88) V skladu z načelom odgovornosti morajo javni organi, ki obdelujejo podatke, sprejeti ustrezne tehnične in organizacijske ukrepe, da lahko uspešno izpolnjujejo svoje obveznosti glede varstva podatkov in dokažejo tako skladnost, predvsem pristojnim nadzornim organom.

(89) To načelo se kaže v členu 56 zakona o varstvu podatkov iz leta 2018, v katerem so za upravljavca uvedene splošne obveznosti glede odgovornosti, tj. obveznost izvajanja ustreznih tehničnih in organizacijskih ukrepov, da se zagotovi in lahko dokaže, da je obdelava osebnih podatkov skladna z zahtevami iz dela 3 zakona o varstvu podatkov iz leta 2018. Po potrebi je treba pregledati in posodobiti izvedene ukrepe in, kjer je sorazmerno, v zvezi z obdelavo vključiti ustrezne politike varstva podatkov.

([151]) Člen 73(5) zakona o varstvu podatkov iz leta 2018.

([152]) Uporabo tega novega okvira je treba razumeti v smislu člena 782 Sporazuma o trgovini in sodelovanju med Evropsko unijo in Evropsko skupnostjo za atomsko energijo na eni strani ter Združenim Kraljestvom Velika Britanija in Severna Irska na drugi strani (L 444/14 z dne 31.12.2020), ki je na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:22020A1231(01)&from=SL.

(90) V skladu s poglavjem IV Direktive (EU) 2016/680 členi 55 do 71 zakona o varstvu podatkov iz leta 2018 določajo drugačne mehanizme za zagotovitev odgovornosti ter upravljavcem in obdelovalcem omogočajo, da dokažejo skladnost. Upravljavci morajo zlasti izvesti ukrepe za vgrajeno in privzeto varstvo podatkov, tj. zagotoviti, da se načela o varstvu podatkov učinkovito izvajajo, ter morajo voditi evidenco vseh kategorij dejavnosti obdelave, za katere je odgovoren upravljavec (vključno z informacijami o identiteti upravljavca, kontaktnimi podatki pooblaščene osebe za varstvo podatkov, nameni obdelave, kategorijami prejemnikov razkritih informacij in opisom kategorij posameznikov, na katere se nanašajo osebni podatki, in osebnih podatkov) in informacijskemu pooblaščencu na zahtevo omogočiti dostop do te evidence. Upravljavec in obdelovalec morata tudi voditi dnevnike določenih dejanj obdelave in informacijskemu pooblaščencu omogočiti dostop do njih ([153]). Od upravljavcev se tudi izrecno zahteva, da sodelujejo z informacijskim pooblaščencem pri izvajanju njegovih nalog.

(91) V zakonu o varstvu podatkov iz leta 2018 so prav tako določene dodatne zahteve za obdelavo, ki bi verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov. Med njimi sta obveznost izvedbe ocen učinka v zvezi z varstvom podatkov in posvetovanja z informacijskim pooblaščencem pred obdelavo, če iz take ocene izhaja, da bi obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov (kadar ni ukrepov za ublažitev tveganja).

(92) Upravljavci morajo nadalje imenovati pooblaščeno osebo za varstvo podatkov, razen če je upravljavec sodišče ali drug pravosodni organ, ki izvaja sodno pristojnost ([154]). Upravljavec mora poskrbeti, da je pooblaščena oseba za varstvo podatkov vključena v vsa vprašanja v zvezi z varstvom osebnih podatkov, da ima potrebna sredstva in dostop do osebnih podatkov in dejavnosti obdelave ter da lahko neodvisno izvaja svoje naloge. Naloge pooblaščene osebe za varstvo podatkov, ki zajemajo zagotavljanje informacij in nasvetov, spremljanje skladnosti ter sodelovanje s kontaktno točko in delovanje kot kontaktna točka za informacijskega pooblaščenca, so določene v členu 71 zakona o varstvu podatkov iz leta 2018. Ta pooblaščena oseba mora pri opravljanju nalog upoštevati tveganja, povezana z dejavnostmi obdelave, ter pri tem upoštevati naravo, obseg, okoliščine in namene obdelave.

2.5 **Nadzor in zagotavljanje skladnosti**

2.5.1 *Neodvisen nadzor*

(93) Vzpostaviti se mora neodvisen nadzorni organ s pristojnostjo spremljanja in zagotavljanja skladnosti s pravili o varstvu podatkov, da se tudi v praksi zagotovi ustrezna raven varstva podatkov. Pri izvajanju svojih obveznosti in pooblastil mora ta organ ravnati popolnoma neodvisno in nepristransko.

(94) V Združenem kraljestvu nadzor in zagotavljanje skladnosti z UK GDPR in zakonom o varstvu podatkov iz leta 2018 izvaja informacijski pooblaščenec ([155]). Informacijski pooblaščenec nadzoruje tudi, kako osebne podatke obdelujejo pristojni organi, kar spada na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 ([156]). Informacijski pooblaščenec je „Corporation Sole“, tj. ločen enoosebni pravni subjekt. Pri delu mu pomaga urad. Urad informacijskega pooblaščenca je imel 31. marca 2020 768 stalnih članov osebja ([157]). Podporno ministrstvo informacijskega pooblaščenca je ministrstvo za digitalne tehnologije, kulturo, medije in šport ([158]).

([153]) Člen 62 zakona o varstvu podatkov iz leta 2018.
([154]) Člen 69 zakona o varstvu podatkov iz leta 2018.
([155]) Člen 36(2)(b) Direktive (EU) 2016/680.
([156]) Člen 116 zakona o varstvu podatkov iz leta 2018.
([157]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2019–2020 sta na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.
([158]) Odnosi med njima so urejeni s sporazumom o upravljanju. Ključne odgovornosti ministrstva za digitalne tehnologije, kulturo, medije in šport kot podpornega ministrstva so zlasti: zagotavljanje ustreznega financiranja in ustreznih virov uradu informacijskega pooblaščenca; zastopanje interesov urada informacijskega pooblaščenca v parlamentu in drugih vladnih službah; zagotavljanje trdnega nacionalnega okvira varstva podatkov ter zagotavljanje smernic in podpore uradu informacijskega pooblaščenca v zvezi s poslovnimi vprašanji, kot so vprašanja nepremičnin, najemov in nabav (sporazum o upravljanju za obdobje 2018–2021 je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Neodvisnost informacijskega pooblaščenca je izrecno določena v členu 52 UK GDPR, ki v ničemer bistveno ne spreminja člena 52(1) do (3) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta ([159]). Informacijski pooblaščenec mora pri opravljanju svojih nalog in izvajanju svojih pooblastil v skladu z UK GDPR ravnati popolnoma neodvisno, ne sme biti izpostavljen niti neposrednemu niti posrednemu zunanjemu vplivu ter ne sme nikogar prositi za navodila niti jih od nikogar sprejemati. Poleg tega se mora vzdržati vsakega delovanja, ki je nezdružljivo z njegovimi dolžnostmi, in se v času svojega mandata ne sme ukvarjati z nobenim nezdružljivim delom, bodisi profitnim bodisi neprofitnim.

(96) Pogoji za imenovanje in razrešitev informacijskega pooblaščenca so določeni v dodatku 12 k zakonu o varstvu podatkov iz leta 2018. Informacijskega pooblaščenca imenuje kraljica na podlagi priporočila vlade ter na podlagi poštenega in odprtega postopka izbire. Kandidat mora imeti ustrezne kvalifikacije, izkušnje in znanje. V skladu s kodeksom upravljanja v zvezi z javnimi imenovanji ([160]) seznam ustreznih kandidatov pripravi svetovalni ocenjevalni odbor. Preden minister za digitalne tehnologije, kulturo, medije in šport sprejme končno odločitev, mora zadevni izbrani parlamentarni odbor opraviti preverjanje pred imenovanjem. Mnenje odbora se javno objavi ([161]).

(97) Mandat informacijskega pooblaščenca traja največ sedem let. Informacijskega pooblaščenca lahko s funkcije razreši kraljica, na podlagi nagovora obeh domov parlamenta ([162]). Predloga za razrešitev informacijskega pooblaščenca ni mogoče predložiti nobenemu od domov parlamenta brez poročila, ki ga pristojni minister predloži temu domu, iz katerega izhaja, da je po njegovem mnenju informacijski pooblaščenec kriv hujše kršitve dolžnega ravnanja uradnih oseb in/ali da ne izpolnjuje več pogojev za opravljanje svoje funkcije ([163]).

(98) Financiranje informacijskega pooblaščenca temelji na treh virih: (i) pristojbine za varstvo podatkov, ki jih plačujejo upravljavci in so določene s predpisi pristojnega ministra ([164]), ki znašajo od 85 % do 90 % letnega proračuna urada ([165]), (ii) nepovratna sredstva, ki jih informacijskemu pooblaščencu nameni vlada in s katerimi se financirajo predvsem operativni stroški informacijskega pooblaščenca v zvezi z nalogami, ki se ne nanašajo na varstvo podatkov ([166]), ter (iii) pristojbine, ki se zaračunavajo za opravljanje storitev ([167]). Trenutno se take pristojbine ne zaračunavajo.

(99) Splošne naloge informacijskega pooblaščenca v zvezi z obdelavo osebnih podatkov, ki spada na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018, so določene v dodatku 13 k zakonu o varstvu podatkov iz leta 2018. Mednje spadajo nadzor in izvajanje dela 3 zakona o varstvu podatkov iz leta 2018, večje ozaveščanje javnosti, svetovanje parlamentu, vladi in drugim institucijam o zakonodajnih in upravnih ukrepih, ozaveščanje upravljavcev in obdelovalcev o njihovih obveznostih, zagotavljanje informacij posameznikom, na katere se nanašajo

([159]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

([160]) Kodeks upravljanja v zvezi z javnimi imenovanji (Governance Code on Public Appointments) je na voljo na povezavi: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Drugo poročilo o srečanjih odbora spodnjega doma parlamenta Združenega kraljestva za kulturo, medije in šport za obdobje 2015–2016 je na voljo na povezavi: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) Nagovor (Address) je predlog, predložen parlamentu, katerega namen je monarha opozoriti na stališča parlamenta o posameznem vprašanju.

([163]) Odstavek 3 dodatka 12 k zakonu o varstvu podatkov iz leta 2018.

([164]) Člen 137 zakona o varstvu podatkov iz leta 2018.

([165]) Člena 137 in 138 zakona o varstvu podatkov iz leta 2018 vsebujeta več zaščitnih ukrepov, da se zagotovi ustrezna raven pristojbin. Natančneje, člen 137(4) zakona o varstvu podatkov iz leta 2018 vsebuje seznam vprašanj, ki jih mora pristojni minister upoštevati pri sprejemanju predpisov, ki določajo višino plačil raznih organizacij. Člen 138(1) in člen 182 zakona o varstvu podatkov iz leta 2018 vsebujeta tudi pravno zahtevo, da se mora pristojni minister pred sprejetjem predpisov posvetovati z informacijskim pooblaščencem in drugimi predstavniki oseb, na katere bodo predpisi verjetno vplivali, da bi se upoštevala njihova stališča. Poleg tega mora informacijski pooblaščenec na podlagi člena 138(2) zakona o varstvu podatkov iz leta 2018 redno preverjati učinkovanje predpisov o pristojbinah in lahko ministru predlaga njihove spremembe. Nazadnje, razen kadar so predpisi izdani zgolj zaradi upoštevanja zvišanja indeksa maloprodajnih cen (v takem primeru se izvede postopek negativne potrditve), se glede predpisov izvede postopek pozitivne potrditve, kar pomeni, da se ti ne smejo izdati, dokler jih s sklepom ne potrdita spodnji in zgornji dom parlamenta.

([166]) V sporazumu o upravljanju je pojasnjeno, da „lahko pristojni minister opravi izplačila informacijskemu pooblaščencu iz sredstev, ki jih zagotovi parlament na podlagi odstavka 9 dodatka 12 k zakonu o varstvu podatkov iz leta 2018. Ministrstvo za digitalne tehnologije, kulturo, medije in šport po posvetovanju z informacijskim pooblaščencem temu izplača odobrene zneske (nepovratna sredstva) za kritje upravnih stroškov urada informacijskega pooblaščenca ter opravljanje nalog informacijskega pooblaščenca v zvezi s številnimi posebnimi nalogami, vključno z zagotavljanjem svobode obveščanja“ (sporazum o upravljanju za obdobje 2018–2021, odstavek 1.12, glej opombo 158).

([167]) Člen 134 zakona o varstvu podatkov iz leta 2018.

osebni podatki, o uveljavljanju njihovih pravic in izvajanje preiskav. Informacijskemu pooblaščencu zaradi vzdrževanja neodvisnosti sodstva ni dovoljeno izvajati nalog v zvezi z obdelavo osebnih podatkov, ki jo izvaja posameznik, kolikor opravlja zadeve iz sodne pristojnosti, ali sodišče, kolikor opravlja zadeve iz sodne pristojnosti. Nadzor nad sodstvom pa je zagotovljen prek posebnih organov, opisanih v nadaljevanju.

2.5.1.1 Izvrševanje, vključno s sankcijami

(100) Informacijski pooblaščenec ima splošna preiskovalna in popravljalna pooblastila, pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi, ki se nanašajo na obdelavo osebnih podatkov, za katero se uporablja del 3 zakona o varstvu podatkov iz leta 2018. Ima pooblastila, da upravljavca ali obdelovalca uradno obvesti o domnevni kršitvi dela 3, da upravljavcu ali obdelovalcu izda opozorilo, da bi predvidena dejanja obdelave verjetno kršila določbe dela 3, in da upravljavcu ali obdelovalcu izreče opomin, kadar so bile z dejanji obdelave kršene določbe te dela 3. Poleg tega lahko na lastno pobudo ali na zahtevo izdaja mnenja za parlament, vlado ali druge institucije in organe Združenega kraljestva ter javnost o vseh zadevah, povezanih z varstvom osebnih podatkov ([168]).

(101) Informacijski pooblaščenec je prav tako pristojen, da:

— upravljavcu in obdelovalcu (ter v določenih okoliščinah vsaki drugi osebi) predloži potrebne informacije z izdajo obvestila o predložitvi informacij (v nadaljnjem besedilu: obvestilo o predložitvi informacij) ([169]),

— izvaja preiskave in preglede z izdajo obvestila o preverjanju, na podlagi katerega mora upravljavec ali obdelovalec informacijskemu pooblaščencu morda dovoliti vstop v določene prostore, pregled ali proučitev dokumentov ali opreme, razgovore z osebami, ki obdelujejo osebne podatke v imenu upravljavca (v nadaljnjem besedilu: obvestilo o preverjanju ([170])),

— na drug način pridobi dostop do dokumentov upravljavcev in obdelovalcev ter dostop v njihove prostore, v skladu s členom 154 zakona o varstvu podatkov iz leta 2018 (v nadaljnjem besedilu: pristojnost za vstop in pregled),

— izvaja popravljalna pooblastila, tudi na podlagi opozoril in opominov ali z izdajo odredb v obliki obvestil o izvršitvi, s katerimi od upravljavcev/obdelovalcev zahteva določeno ukrepanje ali prenehanje izvajanja določenih ukrepov (v nadaljnjem besedilu: obvestil o izvršitvi) ([171]), ter

— izreka upravne globe v obliki plačilnega naloga (v nadaljnjem besedilu: obvestilo o plačilnem nalogu) ([172]).

(102) V politiki urada informacijskega pooblaščenca o regulativnih ukrepih (Regulatory Action Policy) so določene okoliščine, v katerih se izda obvestilo o predložitvi informacij, obvestilo o ocenjevanju, obvestilo o izvršitvi oziroma obvestilo o plačilnem nalogu ([173]). Z obvestilom o izvršitvi se lahko naložijo zahteve, za katere informacijski pooblaščenec meni, da so ustrezne za odpravo pomanjkljivosti. Z obvestilom o plačilnem nalogu se zahteva, da mora oseba informacijskemu pooblaščencu plačati znesek, naveden v obvestilu. Tako obvestilo se lahko izda, če niso izpolnjene določene določbe zakona o varstvu podatkov iz leta 2018 ([174]), lahko pa se izda tudi upravljavcu ali obdelovalcu, ki ni spoštoval obvestila o predložitvi informacij, obvestila o ocenjevanju ali obvestila o izvršitvi.

(103) Natančneje, informacijski pooblaščenec mora pri odločanju o tem, ali naj upravljavcu ali obdelovalcu izda obvestilo o plačilnem nalogu in kako visoka naj bo kazen, upoštevati navedbe iz člena 155(3) zakona o varstvu podatkov iz leta 2018, vključno z naravo in težo kršitve, dejstvom, ali je kršitev naklepna ali posledica malomarnosti, ukrepi, ki jih je sprejel upravljavec ali obdelovalec, da bi omilil škodo, ki so jo utrpeli posamezniki, na katere se nanašajo

([168]) Odstavek 2 dodatka 13 k zakonu o varstvu podatkov iz leta 2018.
([169]) Člen 142 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 143 zakona o varstvu podatkov iz leta 2018).
([170]) Člen 146 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 147 zakona o varstvu podatkov iz leta 2018).
([171]) Členi 149 do 151 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 152 zakona o varstvu podatkov iz leta 2018).
([172]) Člen 155 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 156 zakona o varstvu podatkov iz leta 2018).
([173]) Politika o regulativnih ukrepih je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Urad informacijskega pooblaščenca lahko obvestilo o plačilnem nalogu izda zlasti zaradi kršitve iz člena 149(2), (3), (4) ali (5) zakona o varstvu podatkov iz leta 2018.

osebni podatki, stopnjo odgovornosti upravljavca ali obdelovalca (ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih je sprejel eden ali drugi), vsemi zadevnimi predhodnimi kršitvami upravljavca ali obdelovalca, kategorijami osebnih podatkov, na katere vpliva kršitev, ter dejstvom, ali bi bila kazen učinkovita, sorazmerna in odvračilna.

(104) Najvišji znesek kazni, ki se lahko naloži z obvestilom o plačilnem nalogu, znaša (a) 17 500 000 GBP zaradi neizpolnitve načel o varstvu podatkov (členi 35, 36 in 37, člena 38(1) in 39(1) ter člen 40 zakona o varstvu podatkov iz leta 2018), obveznosti glede preglednosti in pravic posameznikov (členi 44, 45, 46, 47, 48, 49, 52 in 53 zakona o varstvu podatkov iz leta 2018) ter načel o mednarodnih prenosih osebnih podatkov (členi 73, 75, 76, 77 ali 78 zakona o varstvu podatkov iz leta 2018) in (b) 8 700 000 GBP za kršitve po preostalih členih ([175]). V primeru neizpolnitve obvestila o predložitvi informacij, obvestila o ocenjevanju ali obvestila o izvršitvi je najvišji znesek kazni, ki se lahko izreče na podlagi obvestila o plačilnem nalogu 17 500 000 GBP.

(105) Informacijski pooblaščenec je glede na zadnji letni poročili (za obdobji 2018–2019 ([176]) in 2019–2020 ([177])) izvedel številne preiskave v zvezi z obdelavo osebnih podatkov s strani organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Oktobra 2019 je na primer izvedel preiskavo in objavil mnenje v zvezi z uporabo tehnologije za prepoznavanje obrazov na javnih mestih na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Preiskava je bila usmerjena zlasti na uporabo zmogljivosti prepoznavanja obrazov v živo v policiji južnega Walesa in londonski policiji (Metropolitan Police Service). Informacijski pooblaščenec je nadalje preiskoval „Gangs matrix“ (matrika tolp) ([178]) londonske policije in ugotovil vrsto resnih kršitev zakonodaje o varstvu podatkov, ki bi verjetno omajale zaupanje javnosti v matriko in uporabo podatkov.

(106) Novembra 2018 je informacijski pooblaščenec izdal obvestilo o izvršitvi, londonska policija pa je nato sprejela ukrepe, potrebne za povečanje varnosti in odgovornosti ter zagotovitev sorazmerne uporabe podatkov.

(107) Drug primer nedavnega izvršilnega ukrepa je globa v višini 325 000 GBP, ki jo je informacijski pooblaščenec maja 2018 naložil državnemu tožilstvu zaradi izgube nešifriranega DVD-ja s posnetki informativnih razgovorov pri policiji. Poleg tega je informacijski pooblaščenec izvedel preiskave širših tem, na primer v prvi polovici leta 2020 o uporabi pridobivanja podatkov iz mobilnega telefona za policijske namene ter obdelavi podatkov žrtev s strani policije.

(108) Poleg navedenih pooblastil informacijskega pooblaščenca za izvrševanje se določene kršitve zakonodaje o varstvu podatkov štejejo za kazniva dejanja, zato se lahko zanje izrečejo kazenske sankcije (člen 196 zakona o varstvu podatkov iz leta 2018). To se na primer nanaša na pridobitev ali razkritje osebnih podatkov brez privolitve upravljavca in zagotovitev razkritja osebnih podatkov drugi osebi brez privolitve upravljavca ([179]), ponovno identifikacijo informacij v primeru anonimizacije osebnih podatkov, brez privolitve upravljavca, ki je odgovoren za anonimizacijo osebnih podatkov ([180]), namerno oviranje informacijskega pooblaščenca pri izvrševanju njegovih pristojnosti v zvezi s preverjanjem osebnih podatkov v skladu z mednarodnimi obveznostmi ([181]), dajanje neresničnih izjav v odgovor na obvestilo o predložitvi informacij ali uničenje informacij v zvezi z obvestilom o predložitvi informacij ali obvestilom o ocenjevanju ([182]).

(109) Informacijski pooblaščenec ima v skladu s členom 139 zakona o varstvu podatkov iz leta 2018 tudi obveznost, da obema domovoma parlamenta predloži splošno poročilo o izvajanju svojih nalog na podlagi zakona ([183]).

([175]) Člen 157 zakona o varstvu podatkov iz leta 2018.

([176]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2018-2019 sta na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Letno poročilo informacijskega pooblaščenca za obdobje 2019–2020 (glej opombo 157).

([178]) Zbirka podatkov, v kateri so bili evidentirani obveščevalni podatki v zvezi z domnevnimi člani tolp in žrtvami kaznivih dejanj, povezanih s tolpami.

([179]) Člen 170 zakona o varstvu podatkov iz leta 2018.

([180]) Člen 171 zakona o varstvu podatkov iz leta 2018.

([181]) Člen 119 zakona o varstvu podatkov iz leta 2018.

([182]) Člena 144 in 148 zakona o varstvu podatkov iz leta 2018.

([183]) Leto poročilo mora, kot je določeno v sporazumu o upravljanju: (i) zajemati korporacije, odvisna ali skupna podjetja pod nadzorom urada informacijskega pooblaščenca, (ii) spoštovati priročnik o finančnem poročanju (Financial Reporting Manual) finančnega ministrstva, (iii) vsebovati izjavo vlade s predstavitvijo načinov, na katere je računovodja upravljal in nadzoroval sredstva, ki so bila med letom porabljena za organizacijo, s čimer se pokaže, kako dobro organizacija obvladuje tveganja za dosego svojih ciljev, ter (iv) orisati glavne dejavnosti in učinkovitost v prejšnjem finančnem letu in v obliki povzetka določiti nadaljnje načrte (sporazum o upravljanju za obdobje 2018–2021, odstavek 3.26, glej opombo 158).

2.5.2 *Nadzor nad sodstvom*

(110) Nadzor nad obdelavo osebnih podatkov, ki jo izvajajo sodišča in sodstvo, je dvostranski. Kadar nosilec sodne funkcije ali sodišče ne opravlja zadev iz sodne pristojnosti, izvaja nadzor informacijski pooblaščenec. Kadar pa upravljavec deluje v okviru sodne pristojnosti, urad informacijskega pooblaščenca ne more izvajati nadzorne funkcije ([184]), zato jo izvajajo posebni organi. To izraža pristop iz člena 32 Direktive (EU) 2016/680.

(111) Natančneje, v drugem primeru glede sodišč Anglije in Walesa ter glede prvostopenjskih in višjih sodišč Anglije in Walesa tak nadzor zagotavlja sodni svet za varstvo podatkov (Judicial Data Protection Panel) ([185]). Poleg tega sta vodja sodstva Anglije in Walesa (Lord Chief Justice) in višji predsednik sodišč (Senior President of Tribunals) izdala obvestilo o zasebnosti ([186]), ki določa, kako sodišča v Angliji in Walesu obdelujejo osebne podatke za namene opravljanja sodne funkcije. Podobni obvestili sta izdali tudi sodstvo Severne Irske ([187]) in sodstvo Škotske ([188]).

(112) Poleg tega je na Severnem Irskem vodja sodstva Severne Irske sodnika sodišča High Court imenoval za sodnika, pristojnega za nadzor podatkov (Data Supervisory Judge) ([189]). Izdane so bile tudi smernice za sodstvo Severne Irske o tem, kako ravnati v primeru izgube ali potencialne izgube podatkov ter kako obravnavati vsa vprašanja, ki iz tega izhajajo ([190]).

(113) Na Škotskem je vodja sodstva (Lord President) imenoval sodnika za nadzor podatkov (Data Supervisory Judge) za obravnavo vseh pritožb s področja varstva podatkov. Ta sistem je vzpostavljen na podlagi pravil o pritožbah v sodstvu, podobnih tistim v Angliji in Walesu ([191]).

(114) Nazadnje, pri sodišču Supreme Court je eden od sodnikov navedenega sodišča pooblaščen za nadzor nad varstvom podatkov.

([184]) Člen 117 zakona o varstvu podatkov iz leta 2018.

([185]) Naloga sveta je zagotavljati smernice in usposabljanje v sodstvu. Obravnava tudi pritožbe posameznikov, na katere se nanašajo osebni podatki, v zvezi z obdelavo osebnih podatkov, ki jo izvajajo sodišča in posamezniki, kolikor opravljajo zadeve iz sodne pristojnosti. Cilj sveta je zagotoviti način za reševanje vsake pritožbe. Če pritožnik ni zadovoljen z odločitvijo sveta in če predloži dodatne dokaze, lahko svet znova prouči svojo odločitev. Čeprav svet sam ne izreka finančnih sankcij, lahko zadevo preda uradu za preiskave ravnanja pravosodnih organov (Judicial Conduct Investigation Office), če meni, da je bila storjena dovolj resna kršitev zakona o varstvu podatkov iz leta 2018, navedeni urad nato pritožbo prouči. Če je pritožba potrjena, lord kancler in vodja sodstva Anglije in Walesa (ali višji sodnik, ki ga ta pooblasti) odloči, kateri ukrepi se sprejmejo zoper nosilca funkcije. To lahko vključuje (po vrstnem redu glede na težo): uradni nasvet, uradno opozorilo, opomin in nazadnje razrešitev s položaja. Če posameznik ni zadovoljen z načinom, kako je urad za preiskave ravnanja pravosodnih organov obravnaval pritožbo, se lahko nadalje pritoži varuhu pravic v zvezi z imenovanji v pravosodju in ravnanjem pravosodnih organov (Judicial Appointments and Conduct Ombudsman; glej https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Varuh pravic lahko od urada za preiskave ravnanja pravosodnih organov zahteva ponovno obravnavo pritožbe in predlaga izplačilo odškodnine pritožniku, če meni, da je ta zaradi nepravilnosti utrpel škodo.

([186]) Obvestilo vodje sodstva Anglije in Walesa ter višjega predsednika sodišč (Senior President of Tribunals) o zasebnosti je na voljo na povezavi: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Obvestilo vodje sodstva Severne Irske o zasebnosti je na voljo na povezavi: https://judiciaryni.uk/data-privacy.

([188]) Obvestilo o zasebnosti, ki se nanaša na škotska sodišča, je na voljo na povezavi: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Sodnik, pristojen za nadzor podatkov, zagotavlja smernice sodstvu ter obravnava kršitve in/ali pritožbe v zvezi z obdelavo osebnih podatkov, ki jo izvajajo sodišča ali posamezniki, kolikor opravljajo zadeve iz sodne pristojnosti.

([190]) Če se šteje, da gre za resno pritožbo ali težjo kršitev, se zadeva predloži uradniku za obravnavo pritožb v sodstvu (Judicial Complaints Officer) v nadaljnjo obravnavo, v skladu s kodeksom ravnanja v primeru pritožb, ki ga je izdal vodja sodstva Severne Irske. Rezultat take pritožbe je lahko: da se ne sprejme noben nadaljnji ukrep, izdaja nasveta, usposabljanje ali mentorstvo, neuradno opozorilo, uradno opozorilo, zadnje opozorilo, omejitev delovanja ali napotitev pred sodišče, ustanovljeno na podlagi zakona. Kodeks ravnanja v primeru pritožb, ki ga je izdal vodja sodstva Severne Irske, je na voljo na povezavi: 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]) Vsako utemeljeno pritožbo obravnava sodnik za nadzor podatkov, nato pa se predloži vodji sodstva, ki je pristojen izdati nasvet, uradno opozorilo ali opomin, če meni, da je to potrebno (za člane sodišč (tribunals) obstajajo enakovredna pravila, ki so na voljo na povezavi: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3 *Pravna sredstva*

(115) Posameznik, na katerega se nanašajo osebni podatki, mora imeti na voljo učinkovito upravno in sodno varstvo, vključno z odškodnino za škodo, da se zagotovita ustrezno varstvo in zlasti uveljavljanje pravic posameznika.

(116) Prvič, posameznik, na katerega se nanašajo osebni podatki, ima pravico vložiti pritožbo pri informacijskem pooblaščencu, če meni, da je v zvezi z osebnimi podatki, ki se nanašajo nanj, prišlo do kršitve dela 3 zakona o varstvu podatkov iz leta 2018 ([192]). Kot je opisano v uvodnih izjavah (100) in (109), lahko informacijski pooblaščenec preveri, kako upravljavec in obdelovalec zagotavljata skladnost z zakonom o varstvu podatkov iz leta 2018, od njiju zahteva, da v primeru neskladnosti sprejmeta potrebne ukrepe ali se vzdržita določenih ukrepov, ter naloži globe.

(117) Drugič, zakon o varstvu podatkov iz leta 2018 določa pravico do pravnega sredstva zoper odločitev informacijskega pooblaščenca. Če informacijski pooblaščenec pritožbe posameznika, na katerega se nanašajo osebni podatki, ne obravnava ([193]), ima pritožnik dostop do pravnega sredstva, saj lahko od sodišča prve stopnje zahteva ([194]), naj informacijskemu pooblaščencu naloži sprejetje ustreznih ukrepov v odziv na pritožbo ali obveščanje pritožnika o stanju zadeve ([195]). Poleg tega se lahko vsakdo, ki mu informacijski pooblaščenec izda enega od navedenih obvestil (o predložitvi informacij, o ocenjevanju, o izvršitvi ali o plačilnem nalogu), pritoži pri sodišču prve stopnje. Če sodišče ugotovi, da odločba informacijskega pooblaščenca ni v skladu s pravom ali da bi moral ta odločiti drugače, mora sodišče pritožbo dovoliti ali obvestilo oziroma odločbo informacijskega pooblaščenca nadomestiti z drugo ([196]).

(118) Tretjič, posamezniki lahko pravno sredstvo zoper upravljavce in obdelovalce uveljavljajo neposredno pred sodiščem v skladu s členom 167 zakona o varstvu podatkov iz leta 2018. Če sodišče na podlagi vloge posameznika, na katerega se nanašajo osebni podatki, ugotovi, da so bile kršene njegove pravice s področja zakonodaje o varstvu podatkov, lahko upravljavcu, ki je odgovoren za obdelavo takih podatkov, ali obdelovalcu, ki deluje v njegovem imenu, odredi sprejetje ali opustitev določenih ukrepov, navedenih v odločbi. Poleg tega je v skladu s členom 169 zakona o varstvu podatkov iz leta 2018 vsaka oseba, ki utrpi škodo zaradi kršitve zahteve iz zakonodaje o varstvu podatkov (vključno z delom 3 zakona o varstvu podatkov iz leta 2018), ki ni UK GDPR, upravičena do odškodnine za škodo, ki jo je povzročil upravljavec ali obdelovalec, razen če upravljavec ali obdelovalec dokaže, da nikakor ni odgovoren za dogodek, ki je povzročil škodo. Škoda vključuje finančno in nefinančno izgubo, kot je na primer stiska.

(119) Četrtič, vsakdo, ki meni, da so javni organi kršili njegove pravice, vključno s pravico do zasebnosti in do varstva podatkov, lahko uveljavlja pravna sredstva pred sodišči Združenega kraljestva na podlagi zakona o človekovih pravicah iz leta 1998. Upravljavci v skladu z delom 3 zakona o varstvu podatkov iz leta 2018, tj. pristojni organi, so vedno javni organi v smislu zakona o človekovih pravicah iz leta 1998. Posameznik, ki trdi, da je javni organ ravnal (ali predlaga ravnanje) neskladno s pravico iz Konvencije, kar je posledično nezakonito na podlagi člena 6(1) zakona o človekovih pravicah iz leta 1998, lahko pri pristojnem sodišču začne postopek zoper tak organ ali se na zadevne pravice sklicuje v vsakem pravnem postopku, če je (ali bi postal) žrtev nezakonitega dejanja ([197]).

([192]) Člen 165 zakona o varstvu podatkov iz leta 2018.

([193]) Člen 166 zakona o varstvu podatkov iz leta 2018 se nanaša predvsem na te okoliščine: (a) če informacijski pooblaščenec ne sprejme ustreznih ukrepov v odziv na pritožbo, (b) če informacijski pooblaščenec pritožnika ne obvesti o stanju zadeve ali odločitvi o pritožbi v treh mesecih od dne, ko informacijski pooblaščenec prejme pritožbo, ali (c) če informacijski pooblaščenec v navedenem roku ne odloči o pritožbi in pritožnika ustrezno ne obvesti v nadaljnjih treh mesecih.

([194]) Sodišče prve stopnje je pristojno za obravnavo pritožb zoper odločitve vladnih regulativnih organov. Pristojni senat za obravnavo odločitev informacijskega pooblaščenca je splošni regulativni senat (General Regulatory Chamber), ki je pristojen za celotno Združeno kraljestvo.

([195]) Člen 166 zakona o varstvu podatkov iz leta 2018.

([196]) Člena 161 in 162 zakona o varstvu podatkov iz leta 2018.

([197]) Glej sodbo Brown proti Commissioner of Police of the Metropolis iz leta 2016, v kateri je sodišče tožeči stranki v tožbi zoper policijo odredilo odškodnino v okviru varstva podatkov. Sodišče je razsodilo v korist tožeče stranke, tako da je ugodilo njenim zahtevkom v zvezi s kršitvijo obveznosti iz zakona o varstvu podatkov iz leta 1998, kršitvijo zakona o človekovih pravicah iz leta 1998 (in povezanih pravic iz člena 8 EKČP) ter škodnim dejanjem zlorabe zasebnih informacij (tožena stranka je nazadnje priznala, da je kršila zakon o varstvu podatkov in EKČP, zato se je sodba usmerila na določitev primernega pravnega sredstva). Zaradi teh kršitev je sodišče tožeči stranki dodelilo denarno odškodnino.

(120) Če sodišče ugotovi, da je katero koli dejanje javnega organa nezakonito, lahko odobri odškodnino ali pravno sredstvo ali izda odredbo, za katero je pristojen in kot meni, da je pravično in ustrezno ([198]). Sodišče lahko odloči tudi, da določba primarne zakonodaje ni skladna s pravico, zagotovljeno na podlagi EKČP.

(121) Nazadnje, ko posameznik izčrpa nacionalna pravna sredstva, se lahko obrne na Evropsko sodišče za človekove pravice zaradi kršitev pravic, zagotovljenih na podlagi EKČP.

2.6 **Nadaljnja izmenjava**

(122) Pravo Združenega kraljestva pod določenimi pogoji dovoljuje izmenjavo podatkov med organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in drugimi organi Združenega kraljestva za namene, ki se razlikujejo od tistih, za katere so bili podatki prvotno zbrani (tako imenovana nadaljnja izmenjava).

(123) Člen 36(3) zakona o varstvu podatkov iz leta 2018 po vzoru člena 4(2) Direktive (EU) 2016/680 omogoča nadaljnjo obdelavo osebnih podatkov (s strani prvotnega ali drugega upravljavca), ki jih pristojni organ zbere za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za kateri koli drug namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni drug namen ter če je obdelava potrebna in sorazmerna ([199]). V takem primeru se vsi zaščitni ukrepi, navedeni v delu 3 zakona o varstvu podatkov iz leta 2018 in analizirani zgoraj, uporabljajo za obdelavo, ki jo izvaja organ prejemnik.

(124) V okviru pravnega reda Združenega kraljestva različni zakoni izrecno omogočajo nadaljnjo izmenjavo. Zlasti (i) zakon o digitalnem gospodarstvu iz leta 2017 (Digital Economy Act 2017) omogoča izmenjavo med javnimi organi za več namenov, na primer v primeru goljufije zoper javni sektor, ki vključuje izgubo ali tveganje izgube za javni organ ([200]), ali v primeru dolga javnemu organu ali državi ([201]); (ii) zakon o kriminalu in sodiščih iz leta 2013 (Crime and Courts Act 2013), ki omogoča izmenjavo informacij z nacionalno agencijo za boj proti kriminalu (National Crime Agency) ([202]) za namene boja proti hudim kaznivim dejanjem in organiziranemu kriminalu ter preiskovanja in pregona hudih kaznivih dejanj in organiziranega kriminala; (iii) zakon o hudih kaznivih dejanjih iz leta 2007 (Serious Crime Act 2007), ki javnim organom omogoča, da razkrijejo informacije organizacijam za boj proti goljufijam zaradi preprečevanja goljufij ([203]).

(125) Ti zakoni izrecno določajo, da mora biti izmenjava informacij v skladu z načeli iz zakona o varstvu podatkov iz leta 2018. Poleg tega je poklicni organ uslužbencev policije izdal dokument o odobreni strokovni praksi glede izmenjave informacij ([204]), ki je policiji v pomoč pri izpolnjevanju njenih obveznosti glede varstva podatkov na podlagi UK GDPR, zakona o varstvu podatkov in zakona o človekovih pravicah iz leta 1998. Skladnost izmenjave informacij s pravnim okvirom varstva podatkov, ki se uporablja, je seveda stvar sodne presoje ([205]).

(126) Nadalje, zakon o varstvu podatkov iz leta 2018 podobno kot člen 9 Direktive (EU) 2016/680 določa, da se lahko osebni podatki, zbrani za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obdelujejo za namene, ki ne spadajo na področje preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če tako obdelavo omogoča zakon ([206]). Ta vrsta izmenjave vključuje dva primera: (1) ko organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj posreduje podatke organu z drugega področja, ki ni obveščevalna agencija (na primer

([198]) Člen 8(1) zakona o človekovih pravicah iz leta 1998.

([199]) Člen 36(3) zakona o varstvu podatkov iz leta 2018.

([200]) Člen 56 zakona o digitalnem gospodarstvu iz leta 2017, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) Člen 48 zakona o digitalnem gospodarstvu iz leta 2017.

([202]) Člen 7 zakona o kriminalu in sodiščih iz leta 2013, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2013/22/contents.

([203]) Člen 68 zakona o hudih kaznivih dejanjih iz leta 2007, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([204]) Smernice o dovoljeni strokovni praksi glede izmenjave informacij so na voljo na povezavi: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

([205]) Glej na primer zadevo M. proti the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), pri kateri je sodišče High Court presojalo o izmenjavi podatkov med policijo in organizacijo Business Crime Reduction Partnership (BCRP), ki upravlja program obveščanja o izključitvi, na podlagi katerih se osebam prepove vstop v poslovne prostore članov organizacije. Sodišče je proučilo izmenjavo podatkov, ki je potekala na podlagi dogovora, sklenjenega z namenom zaščite javnosti in preprečevanja kriminala, ter ugotovilo, da je bila večina vidikov izmenjave podatkov zakonita, razen glede nekaterih občutljivih podatkov, ki sta si jih izmenjala policija in navedena organizacija. Drug primer je zadeva Cooper proti NCA [2019] EWCA Civ 16 , pri kateri je pritožbeno sodišče (Court of Appeal) potrdilo pravilnost izmenjave podatkov med policijo in agencijo za hude primere organiziranega kriminala (Serious Organised Crime Agency (SOCA)), tj. organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki je trenutno del nacionalne agencije za boj proti kriminalu.

([206]) Člen 36(4) zakona o varstvu podatkov iz leta 2018.

finančnemu ali davčnemu organu, organu za varstvo konkurence, socialnemu uradu za mladoletnike itd.), ter (2) ko organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj podatke posreduje obveščevalni agenciji. V prvem primeru obdelava osebnih podatkov spada na področje uporabe UK GDPR ter dela 2 zakona o varstvu podatkov iz leta 2018. Kot je določeno v sklepu, sprejetem v skladu z Uredbo (EU) 2016/679, je z zaščitnimi ukrepi iz UK GDPR in dela 2 zakona o varstvu podatkov iz leta 2018 zagotovljena raven varstva, v osnovi enakovredna tisti, ki se zagotavlja v Uniji ([207]).

(127) V drugem primeru, tj. glede izmenjave podatkov, ki jih organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj zbere ter posreduje obveščevalni agenciji za namene nacionalne varnosti, pa je pravna podlaga za izmenjavo člen 19 zakona o boju proti terorizmu iz leta 2008 (Counter Terrorism Act 2008) ([208]). Na podlagi navedenega zakona iz leta 2008 lahko vsaka oseba daje informacije kateri koli obveščevalni službi za namene izvrševanja katere koli naloge take službe, vključno z „nacionalno varnostjo“.

(128) Glede pogojev, na podlagi katerih je mogoča izmenjava podatkov za namene nacionalne varnosti, zakon o obveščevalnih službah (Intelligence Services Act) in zakon o varnostnih službah (Security Services Act) omejujeta zmožnost obveščevalnih služb za pridobivanje podatkov na tisto, kar je potrebno za izvrševanje njihovih zakonskih nalog. Pristojni organi, ki spadajo na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018, ki želijo posredovati podatke obveščevalnim službam, morajo poleg zakonskih nalog agencij, navedenih v zakonu o obveščevalnih službah in zakonu o varnostnih službah, proučiti več dejavnikov oziroma upoštevati več omejitev ([209]). Člen 20 zakona o boju proti terorizmu iz leta 2008 jasno določa, da mora biti vsaka izmenjava podatkov na podlagi člena 19 tega zakona v skladu z zakonodajo o varstvu podatkov; to pomeni, da se uporabljajo vse omejitve in zahteve iz dela 3 zakona o varstvu podatkov iz leta 2018. Nadalje, organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter obveščevalne službe so javni organi za namen zakona o človekovih pravicah iz leta 1998, ki si morajo zato prizadevati, da bi ravnali skladno s pravicami, zagotovljenimi na podlagi EKČP, vključno iz njenega člena 8. Povedano drugače, te zahteve pomenijo, da je vsakršna izmenjava podatkov med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in obveščevalnimi službami skladna z zakonodajo o varstvu podatkov in z EKČP.

(129) Pri obdelavi osebnih podatkov, prejetih od organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki jo izvajajo obveščevalne službe za namene nacionalne varnosti, veljajo številni pogoji in zaščitni ukrepi ([210]). Del 4 zakona o varstvu podatkov iz leta 2018 se uporablja za vse primere obdelave, ki jih izvajajo obveščevalne službe ali

([207]) Izvedbeni sklep Komisije v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu (C(2021) 4800).

([208]) Člen 19 zakona iz leta 2008 o hudih kaznivih dejanjih, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) Člen 2(2) zakona o obveščevalnih službah iz leta 1994 (glej spletno mesto: https://www.legislation.gov.uk/ukpga/1994/13/contents) določa, da je „vodja obveščevalne službe odgovoren za učinkovitost navedene službe ter da je njegova dolžnost zagotoviti: (a) ureditev, ki omogoča, da lahko obveščevalna služba prejme le tiste informacije, ki so potrebne za ustrezno izvajanje njenih nalog, ter da lahko razkrije le tiste informacije, ki so potrebne (i) za navedeni namen, (ii) za namene nacionalne varnosti, (iii) za namene preprečevanja ali odkrivanja hudih kaznivih dejanj, ali (iv) za namene katerega koli kazenskega postopka; ter (b) da obveščevalna služba ne sme izvajati nobenih ukrepov v korist katere koli politične stranke v Združenem kraljestvu“; člen 2(2) zakona o varnostnih službah iz leta 1989 (glej spletno mesto: https://www.legislation.gov.uk/ukpga/1989/5/contents) pa določa, da je „generalni direktor odgovoren za učinkovitost službe ter da mora zagotoviti: (a) ureditev, ki zagotavlja, da lahko služba prejme le tiste informacije, ki so potrebne za ustrezno izvajanje njenih nalog, ter da lahko razkrije le tiste informacije, ki so potrebne za navedeni namen ali namen [preprečevanja ali odkrivanja] hudih kaznivih dejanj [ali katerega koli kazenskega postopka]; (b) da služba ne sme izvajati nobenih ukrepov v korist katere koli politične stranke ter (c) ureditev, v dogovoru z generalnim direktorjem nacionalne agencije za boj proti kriminalu, glede usklajevanja dejavnosti službe na podlagi člena 1(4) tega zakona z dejavnostmi policije, nacionalne agencije za boj proti kriminalu in drugimi organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“.

([210]) Zaščitni ukrepi in omejitve pooblastil obveščevalnih služb so urejeni tudi z zakonom o preiskovalnih pooblastilih iz leta 2016, ki skupaj z zakonom o urejanju preiskovalnih pooblastil iz leta 2000 (Regulation of Investigatory Powers Act 2000) za Anglijo, Wales in Severno Irsko ter zakonom o urejanju preiskovalnih pooblastil (Škotska) iz leta 2000 (Regulation of Investigatory Powers (Scotland) Act 2000) za Škotsko zagotavlja pravno podlago za uporabo takih pooblastil. Vendar ta pooblastila v primeru nadaljnje izmenjave niso pomembna, saj zajemajo neposredno zbiranje osebnih podatkov s strani obveščevalnih agencij. Za oceno pooblastil, ki so na podlagi zakona o preiskovalnih pooblastilih podeljena obveščevalnim agencijam, gej Izvedbeni sklep Komisije v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu (C(2021) 4800).

ki se izvajajo v njihovem imenu. Določa zlasti glavna načela o varstvu podatkov (zakonitost, poštenost in preglednost ([211]); omejitev namena ([212]), najmanjši obseg podatkov ([213]), točnost ([214]); omejitev hrambe ([215]) in varnost ([216])), določa tudi pogoje glede obdelave posebnih vrst podatkov ([217]) in pravice posameznikov, na katere se nanašajo osebni podatki ([218]), vsebuje zahtevo o vgrajenem varstvu podatkov ([219]) ter ureja mednarodni prenos osebnih podatkov ([220]).

(130) Hkrati člen 110 zakona o varstvu podatkov iz leta 2018 določa izjemo od posebnih določb v delu 4 zakona o varstvu podatkov iz leta 2018, kadar je taka izjema potrebna za zaščito nacionalne varnosti. Člen 110(2) zakona o varstvu podatkov iz leta 2018 navaja seznam določb, pri katerih je mogoče uporabiti izjemo. Med njimi so načela o varstvu podatkov (razen načela zakonitosti), pravice posameznika, na katerega se nanašajo osebni podatki, obveznost obveščanja informacijskega pooblaščenca o kršitvi varnosti podatkov, inšpekcijska pooblastila informacijskega pooblaščenca v skladu z mednarodnimi obveznostmi, določena pooblastila informacijskega pooblaščenca za izvrševanje, določbe, na podlagi katerih se nekatere kršitve varnosti podatkov štejejo za kaznivo dejanje, in določbe, ki se nanašajo na posebne namene obdelave, na primer za novinarske, akademske ali umetniške namene. To izjemo je mogoče uporabiti le na podlagi analize vsakega primera posebej ([221]). Kot so pojasnili organi Združenega kraljestva in je bilo potrjeno s sodno prakso sodišč Združenega kraljestva, „(a) mora upravljavec upoštevati dejanske posledice za nacionalno varnost ali obrambo, če bi moral zagotoviti skladnost s posamezno določbo za varstvo podatkov, ter to, ali bi lahko razumno zagotovil skladnost z običajnim pravilom brez ogrožanja nacionalne varnosti ali obrambe“ ([222]). Urad informacijskega pooblaščenca nadzoruje, ali je bila izjema ustrezno uporabljena ali ne ([223]).

([211]) V skladu s členom 86(6) zakona o varstvu podatkov iz leta 2018 je treba pri ugotavljanju poštenosti in preglednosti obdelave upoštevati tudi metodo pridobitve podatkov. V tem smislu je zahteva glede poštenosti in preglednosti izpolnjena, če so podatki pridobljeni od osebe, ki je zakonito pooblaščena, da jih lahko zagotovi, ali ki jih na podlagi zakona mora zagotoviti.

([212]) V skladu s členom 87 zakona o varstvu podatkov iz leta 2018 mora biti namen obdelave specifičen, izrecen in zakonit. Podatki se ne smejo obdelovati na način, ki ni skladen z nameni, za katere so bili zbrani. V skladu s členom 87(3) je nadaljnja obdelava osebnih podatkov dovoljena le, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni namen ter če je obdelava potrebna in sorazmerna z navedenim drugim namenom. Obdelava se šteje za skladno, če se izvaja za namene arhiviranja v javnem interesu, za namene znanstvenih ali zgodovinskih raziskav ali za statistične namene in če zanjo veljajo ustrezni zaščitni ukrepi (člen 87(4) zakona o varstvu podatkov iz leta 2018).

([213]) Osebni podatki morajo biti ustrezni, relevantni in ne čezmerni (člen 88 zakona o varstvu podatkov iz leta 2018).

([214]) Osebni podatki morajo biti točni in posodobljeni (člen 89 zakona o varstvu podatkov iz leta 2018).

([215]) Osebni podatki se ne smejo shranjevati dlje, kot je potrebno (člen 90 zakona o varstvu podatkov iz leta 2018).

([216]) Šesto načelo o varstvu podatkov je, da je treba osebne podatke obdelovati tako, da so upoštevani ustrezni zaščitni ukrepi glede tveganj, ki izhajajo iz obdelave osebnih podatkov. Tveganja med drugim vključujejo nenameren ali nepooblaščen dostop do osebnih podatkov, njihovo uničenje, izgubo, uporabo, spreminjanje ali razkritje (člen 91 zakona o varstvu podatkov iz leta 2018). Člen 107 zahteva tudi, da (1) mora vsak upravljavec vzpostaviti ustrezne zaščitne ukrepe, ki so primerni glede na tveganja, ki izhajajo iz obdelave osebnih podatkov, (2) v primeru avtomatizirane obdelave pa mora vsak upravljavec in vsak obdelovalec na podlagi ocene tveganja vzpostaviti preventivne ukrepe ali ukrepe za zmanjšanje tveganja.

([217]) Člen 86(2)(b) in dodatek 10 k zakonu o varstvu podatkov iz leta 2018.

([218]) V skladu s poglavjem 3 dela 4 zakona o varstvu podatkov iz leta 2018 gre predvsem za te pravice: za pravico do dostopa, pravico do popravka in izbrisa, pravico do ugovora obdelavi, pravico, da se za posameznika ne uporablja avtomatizirano sprejemanje odločitev, pravico poseči v avtomatizirano sprejemanje odločitev in pravico do obveščanja o sprejemanju odločitev. Poleg tega mora upravljavec posameznika, na katerega se nanašajo osebni podatki, obvestiti o obdelavi njegovih osebnih podatkov.

([219]) Člen 103 zakona o varstvu podatkov iz leta 2018.

([220]) Člen 109 zakona o varstvu podatkov iz leta 2018. Prenosi osebnih podatkov mednarodnim organizacijam ali državam zunaj Združenega kraljestva so mogoči, če je tak prenos potreben in sorazmeren ukrep, ki se izvaja za namene izvajanja zakonskih nalog upravljavca ali za druge namene, določene v zadevnih členih zakona o varnostnih službah iz leta 1989 (Security Service Act 1989) in zakona o obveščevalnih službah iz leta 1994 (Intelligence Services Act 1994).

([221]) Glej sodbo v zadevi Baker proti Secretary of State for the Home Department [2001] UKIT NSA2 (v nadaljnjem besedilu: Baker proti Secretary of State).

([222]) Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek H: Okvir varstva podatkov s področja državne varnosti in preiskovalnih pristojnosti, strani 15–16, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Glej tudi sodbo v zadevi Baker proti Secretary of State (glej opombo 220), v kateri je sodišče razveljavilo potrdilo o omejitvah iz razlogov nacionalne varnosti, ki ga je izdal minister za notranje zadeve in ki je potrjevalo uporabo izjeme na podlagi nacionalne varnosti, saj je menilo, da ni razloga, da bi se dovolila splošna izjema od obveznosti odziva na zahteve za dostop do podatkov, ter da bi omogočanje take izjeme v vseh okoliščinah brez analize vsakega primera posebej presegalo tisto, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

([223]) Glej memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, v skladu s katerim „se mora urad informacijskega pooblaščenca po prejetju pritožbe posameznika, na katerega se nanašajo osebni podatki, prepričati, da je bila zadeva pravilno obravnavana ter, če je ustrezno, da so bile morebitne izjeme ustrezno uporabljene“ (memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, odstavek 16, ki je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Nadalje, v zvezi z možnostjo omejitve uporabe navedenih posebnih pravic zaradi zaščite nacionalne varnosti je v členu 79 zakona o varstvu podatkov iz leta 2018 določeno, da lahko upravljavec zaprosi za izdajo potrdila, ki ga podpiše vladni minister ali generalni državni tožilec in ki potrjuje, da je, ali je kadar koli bila, omejitev takih pravic potreben in sorazmeren ukrep za zaščito nacionalne varnosti ([224]). Vlada Združenega kraljestva je izdala smernice za potrdila o omejitvah iz razlogov nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018, ki zlasti poudarjajo, da morajo biti vse omejitve pravic posameznikov, na katere se nanašajo osebni podatki, zaradi zaščite nacionalne varnosti sorazmerne in potrebne ([225]). Vsa potrdila o omejitvah iz razlogov nacionalne varnosti morajo biti objavljena na spletišču urada informacijskega pooblaščenca ([226]).

(132) Potrdilo se izda za določen čas največ pet let, da ga lahko izvršilna oblast redno preverja ([227]). Potrdilo opredeljuje osebne podatke ali kategorije osebnih podatkov, za katere se uporabi izjema, ter določbe zakona o varstvu podatkov iz leta 2018, ki jih zadeva izjema ([228]).

(133) Pomembno je omeniti, da potrdila o omejitvah iz razlogov nacionalne varnosti niso dodatni razlog za omejitev pravic do varstva podatkov iz razlogov nacionalne varnosti. Z drugimi besedami, upravljavec ali obdelovalec se lahko na potrdilo sklicuje le, če ugotovi, da se je treba sklicevati na izjemo zaradi nacionalne varnosti, kar pa mora uporabiti za vsak primer posebej. Tudi če se potrdilo o omejitvah iz razlogov nacionalne varnosti nanaša na posamezno zadevo, lahko urad informacijskega pooblaščenca prouči, ali je bilo v posameznem primeru sklicevanje na izjemo zaradi nacionalne varnosti upravičeno ([229]).

(134) Oseba, ki je neposredno prizadeta zaradi izdaje potrdila, se lahko zaradi tega ([230]) pritoži pri sodišču Upper Tribunal ([231]), če so v potrdilu podatki opredeljeni s splošnim opisom, pa lahko izpodbija uporabo potrdila glede posameznih podatkov ([232]).

(135) Sodišče prouči odločitev o izdaji potrdila in odloči, ali so za izdajo potrdila obstajali utemeljeni razlogi ([233]). Prouči lahko več vprašanj, vključno s potrebnostjo, sorazmernostjo in zakonitostjo, upošteva vpliv na pravice posameznikov, na katere se nanašajo podatki, in pretehta potrebo po zaščiti nacionalne varnosti. Posledično lahko sodišče ugotovi, da se potrdilo ne nanaša na določene osebne podatke, ki so predmet pritožbe ([234]).

([224]) Z zakonom o varstvu podatkov iz leta 2018 je bila ukinjena možnost izdaje potrdila na podlagi člena 28(2) zakona o varstvu podatkov iz leta 1998. Vendar pa možnost izdajanja „starih potrdil“ še vedno obstaja, in sicer v obsegu, kot to izhaja iz možnosti, ki zgodovinsko obstaja na podlagi zakona iz leta 1998 (glej odstavek 17 dela 5 dodatka 20 k zakonu o varstvu podatkov iz leta 2018). Vendar se zdi ta možnost zelo redka in velja samo v omejenem številu primerov, na primer kadar oseba, na katero se nanašajo podatki, izpodbija uporabo izjeme iz razlogov nacionalne varnosti v zvezi z obdelavo s stani javnega organa, ki je obdelavo izvedel v skladu z zakonom iz leta 1998. Treba je omeniti, da se bo v teh primerih v celoti uporabljal člen 28 zakona o varstvu podatkov iz leta 1998, vključno z možnostjo, da lahko posameznik, na katerega se nanašajo podatki, izpodbija potrdilo. Trenutno ne obstaja nobeno potrdilo o omejitvah iz razlogov nacionalne varnosti, izdano na podlagi zakona o varstvu podatkov iz leta 1998.

([225]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018 (UK Government Guidance on National Security Certificates under the Data Protection Act 2018) so na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) V skladu s členom 130 zakona o varstvu podatkov iz leta 2018 se lahko urad informacijskega pooblaščenca odloči, da ne objavi besedila ali dela besedila takega potrdila, če bi bilo to v nasprotju z interesi nacionalne varnosti ali v nasprotju z javnim interesom ali bi lahko ogrozilo varnost katerega koli posameznika. V teh primerih urad informacijskega pooblaščenca objavi dejstvo, da je bilo potrdilo izdano.

([227]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti, odstavek 15, glej opombo 225.

([228]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti, odstavek 5, glej opombo 225.

([229]) Člen 102 zakona o varstvu podatkov iz leta 2018 določa, da mora upravljavec dokazati, da je zagotovil skladnost z zakonom o varstvu podatkov iz leta 2018. To pomeni, da mora obveščevalna služba uradu informacijskega pooblaščenca dokazati, da je pri uporabi izjeme proučila posebne okoliščine posamezne zadeve. Urad informacijskega pooblaščenca objavlja tudi evidenco potrdil o omejitvah iz razlogov nacionalne varnosti, ki je na voljo na povezavi: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Člen 111(3) zakona o varstvu podatkov iz leta 2018.

([231]) Sodišče Upper Tribunal je pristojno za obravnavo pritožb zoper odločitve nižjih upravnih sodišč in ima posebne pristojnosti glede neposrednih pritožb zoper odločitve nekaterih vladnih organov.

([232]) Člen 111(5) zakona o varstvu podatkov iz leta 2018.

([233]) V zadevi Baker proti Secretary of State (glej opombo 221) je sodišče Information Tribunal razveljavilo potrdilo o omejitvah iz razlogov nacionalne varnosti, ki ga je izdal minister za notranje zadeve, saj je menilo, da ni razloga, da bi se dovolila splošna izjema od obveznosti odziva na zahteve za dostop do podatkov, ter da bi omogočanje take izjeme v vseh okoliščinah brez analize vsakega primera posebej, presegalo tisto, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

([234]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti, odstavek 25, glej opombo 224.

(136) Druga vrsta morebitnih omejitev se nanaša na tiste, ki se na podlagi dodatka 11 k zakonu o varstvu podatkov iz leta 2018, nanašajo na nekatere določbe dela 4 zakona o varstvu podatkov iz leta 2018 ([235]), da bi se zaščitili drugi pomembni cilji splošnega javnega interesa ali zaščiteni interesi, kot so na primer parlamentarni privilegij, varovanje zaupnosti sporazumevanja med odvetnikom in stranko, vodenje sodnega postopka ali bojna učinkovitost oboroženih sil. Uporaba teh določb je izvzeta za določene vrste informacij (izjema na podlagi vrste) ali če bi uporaba teh določb verjetno posegala v zaščitene interese (izjema na podlagi poseganja) ([236]). Na izjeme na podlagi poseganja se je mogoče sklicevati le, če je verjetno, da bi uporaba navedene določbe o varstvu podatkov posegala v zadevni posamezni interes. Uporaba izjeme mora torej biti vedno upravičena s sklicevanjem na zadevno poseganje, do katerega bi v posameznem primeru verjetno prišlo. Na izjeme na podlagi vrste se je mogoče sklicevati le glede specifičnih, ozko opredeljenih vrst informacij, glede katerih je uporaba izjeme mogoča. Te so glede na namen in učinek podobne več izjemam od UK GDPR (na podlagi dodatka 2 k zakonu o varstvu podatkov iz leta 2018), ki pa izražajo tiste iz člena 23 Splošne uredbe o varstvu podatkov.

(137) Iz navedenega izhaja, da so na podlagi pravnih določb Združenega kraljestva, ki se uporabljajo, vzpostavljene omejitve in pogoji, kakor jih razlagajo tudi sodišča in informacijski pooblaščenec, ki zagotavljajo, da navedene izjeme in omejitve ostajajo znotraj okvirov tega, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

(138) Informacijski pooblaščenec nadzoruje obdelavo osebnih podatkov, ki jo izvajajo obveščevalne službe v skladu z delom 4 zakona o varstvu podatkov iz leta DPA 2018 ([237]).

(139) Splošne naloge informacijskega pooblaščenca v zvezi z obdelavo osebnih podatkov, ki jo izvajajo obveščevalne službe na podlagi dela 4 zakona o varstvu podatkov iz leta 2018, so določene v dodatku 13 k zakonu o varstvu podatkov iz leta 2018. Te med drugim vključujejo zlasti nadzor in izvajanje dela 4 zakona o varstvu podatkov iz leta 2018, večje ozaveščanje javnosti, svetovanje parlamentu, vladi in drugim institucijam o zakonodajnih in upravnih ukrepih, ozaveščanje upravljavcev in obdelovalcev o njihovih obveznostih, zagotavljanje informacij posameznikom, na katere se nanašajo osebni podatki, o uveljavljanju njihovih pravic in izvajanje preiskav.

(140) Kot je določeno v delu 3 zakona o varstvu podatkov iz leta 2018, je informacijski pooblaščenec pristojen za obveščanje upravljavca o domnevnih kršitvah, izdajanje opozoril, da bo obdelava verjetno kršila pravila, in izrekanje opominov ob potrditvi kršitve. Izdaja lahko tudi obvestila o izvršitvi in o plačilnem nalogu za kršitve določenih določb akta ([238]). Informacijski pooblaščenec pa v nasprotju z drugimi deli zakona o varstvu podatkov iz leta 2018 ne more izdati obvestila o preverjanju organu za nacionalno varnost ([239]).

(141) Poleg tega je v členu 110 zakona o varstvu podatkov iz leta 2018 določena izjema od uporabe določenih pooblastil informacijskega pooblaščenca, ko je to potrebno zaradi zaščite nacionalne varnosti. To vključuje pristojnost informacijskega pooblaščenca, da lahko na podlagi zakona o varstvu podatkov izdaja obvestila (vseh vrst) (obvestilo o predložitvi informacij, obvestilo o preverjanju, obvestilo o izvršitvi in obvestilo o plačilnem nalogu), pristojnost za opravljanje inšpekcijskega nadzora v skladu z mednarodnimi obveznostmi, pristojnost za vstop in inšpekcijski

([235]) To vključuje: (i) načela o varstvu podatkov iz dela 4, razen zahteve glede zakonitosti obdelave na podlagi prvega načela ter dejstva, da mora obdelava izpolnjevati enega od zadevnih pogojev iz dodatkov 9 in 10, (ii) pravice posameznikov, na katere se nanašajo osebni podatki, in (iii) obveznosti, ki se nanašajo na kršitev poročanja uradu informacijskega pooblaščenca.

([236]) V skladu z obrazložitvenim okvirom Združenega kraljestva so izjeme na podlagi vrste: (i) informacije o podelitvi državnih častnih odlikovanj; (ii) varovanje zaupnosti sporazumevanja med odvetnikom in stranko; (iii) zaupni sklici na zaposlitev, usposabljanje ali izobraževanje ter (iv) izpitne pole in ocene. Izjeme na podlagi poseganja se nanašajo na te zadeve: (i) preprečevanje ali odkrivanje kaznivih dejanj; prijetje in pregon storilcev; (ii) parlamentarni privilegij; (iii) sodni postopki; (iv) bojna učinkovitost oboroženih sil države; (v) gospodarska blaginja Združenega kraljestva; (vi) pogajanja s posameznikom, na katerega se nanašajo osebni podatki; (vii) znanstvene ali zgodovinske raziskave ali statistični nameni; (viii) arhiviranje v javnem interesu. Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek H: Nacionalna varnost, stran 13, glej opombo 222.

([237]) Člen 116 zakona o varstvu podatkov iz leta 2018.

([238]) Upravljavcu ali obdelovalcu se lahko v skladu s povezanim branjem člena 149(2) in člena 155 zakona o varstvu podatkov iz leta 2018 izdajo opozorila o izvršitvi in o plačilnem nalogu za kršitve poglavja 2 dela 4 zakona o varstvu podatkov iz leta 2018 (načela obdelave), določbe dela 4 zakona o varstvu podatkov iz leta 2018 o prenosu pravic posameznika, na katerega se nanašajo osebni podatki, zahteve o obveščanju informacijskega pooblaščenca o kršitvi varnosti osebnih podatkov v skladu s členom 108 zakona o varstvu podatkov iz leta 2018 ter načel prenosa osebnih podatkov v tretje države, države, ki niso podpisnice konvencije, in mednarodne organizacije iz člena 109 zakona o varstvu podatkov iz leta 2018. (Za več podrobnosti o opozorilih o izvršitvi in o plačilnem nalogu glej uvodni izjavi (102) in (103)).

([239]) Informacijski pooblaščenec v skladu s členom 147(6) zakona o varstvu podatkov iz leta 2018 ne sme izdati obvestila o preverjanju organu iz člena 23(3) zakona o dostopu do informacij javnega značaja iz leta 2000 (Freedom of Information Act 2000). To zajema varnostno službo (MI5), tajno obveščevalno službo (MI6) in vladno obveščevalno službo (GCHQ).

pregled in pravila o kaznivih dejanjih ([240]). Te izjeme se bodo, kot je pojasnjeno v uvodni izjavi (136), uporabljale le, če so potrebne in sorazmerne in za vsak primer posebej. Uporaba teh izjem bi morala biti predmet sodne presoje ([241]).

(142) Urad informacijskega pooblaščenca in obveščevalne službe Združenega kraljestva so podpisale memorandum o soglasju ([242]), ki vzpostavlja okvir za sodelovanje o številnih vprašanjih, vključno z obvestili o kršitvi varnosti podatkov in obravnavanjem pritožb posameznikov, na katere se nanašajo osebni podatki. V njem je določeno zlasti to, da urad informacijskega pooblaščenca ob prejetju pritožbe oceni, ali je bil sklic na izjemo zaradi nacionalne varnosti ustrezen. Odgovor na poizvedbe, ki jih opravi urad informacijskega pooblaščenca pri proučitvi pritožb posameznikov, je treba na podlagi zadevnih smernic vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti v skladu z zakonom o varstvu podatkov poslati v 20 delovnih dneh, če gre za zaupne informacije, pa je treba pri tem uporabiti varne komunikacijske kanale. Urad informacijskega pooblaščenca je od aprila 2018 do danes prejel 21 pritožb posameznikov glede obveščevalnih služb. Vsako pritožbo je proučil in rezultat sporočil posamezniku, na katerega se nanašajo osebni podatki ([243]).

(143) Odbor za obveščevalno in varnostno dejavnost (Intelligence and Security Committee) izvaja parlamentarni nadzor nad obdelavo podatkov, ki jo izvajajo obveščevalne službe. Njegova zakonska podlaga je zakon iz leta 2013 o pravosodju in varnosti (Justice and Security Act 2013) ([244]). Z zakonom je bil ustanovljen odbor parlamenta Združenega kraljestva za obveščevalno in varnostno dejavnost. Odbor za obveščevalno in varnostno dejavnost sestavljajo poslanci zgornjega ali spodnjega doma parlamenta Združenega kraljestva, ki jih imenuje predsednik vlade po posvetovanju z vodjem opozicije ([245]). Pripraviti mora letno poročilo za parlament o izvajanju svojih nalog in druga poročila, ki se mu zdijo ustrezna ([246]).

(144) Odboru za obveščevalno in varnostno dejavnost so bila od leta 2013 podeljena večja pooblastila, vključno z nadzorom nad operativnimi dejavnostmi varnostnih služb. V skladu s členom 2 zakona o pravosodju in varnosti iz leta 2013 je naloga tega odbora nadzor nad odhodki, upravljanjem, politiko in operacijami nacionalnih varnostnih agencij. V zakonu o pravosodju in varnosti iz leta 2013 je določeno, da lahko ta odbor izvaja preiskave

([240]) Izvzete so lahko naslednje določbe: člen 108 (obveščanje informacijskega pooblaščenca o kršitvi varnosti osebnih podatkov), člen 119 (inšpekcijski nadzor v skladu z mednarodnimi obveznostmi), členi 142 do 154 in dodatek 15 (obvestila informacijskega pooblaščenca in pooblastila za vstop in inšpekcijski pregled) ter členi 170 do 173 (kazniva dejanja, povezana z osebnimi podatki). Poleg tega pa še tiste, ki se nanašajo na obdelavo s strani obveščevalnih služb iz odstavka 1(a) in (g) ter odstavka 2 dodatka 13 (druge splošne naloge informacijskega pooblaščenca).

([241]) Glej na primer sodbo v zadevi Baker proti Secretary of State for the Home Department (glej opombo 221).

([242]) Memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, glej opombo 231.

([243]) Urad informacijskega pooblaščenca je v sedmih od teh primerov pritožniku svetoval, naj se s pritožbo obrne na upravljavca podatkov (tako je v primeru, če je posameznik pritožbo najprej vložil pri uradu informacijskega pooblaščenca, moral pa bi jo pri upravljavcu podatkov), v enem od teh primerov je urad upravljavcu podatkov zagotovil splošni nasvet (to se uporablja, ko ukrepi upravljavca ne kršijo zakonodaje, vendar bi se lahko z boljšo prakso preprečilo vlaganje pritožb pri uradu), v drugih 13 primerih pa ni bilo potrebno ukrepanje upravljavca podatkov (to se uporablja, kadar posamezniki izrazijo pomisleke, ki spadajo na področje uporabe zakona o varstvu podatkov iz leta 2018, ker se nanašajo na obdelavo osebnih informacij, vendar iz predloženih informacij ne izhaja, da bi upravljavec kršil zakonodajo).

([244]) Kot so pojasnili organi Združenega kraljestva, so se z zakonom o pravosodju in varnosti razširile pristojnosti odbora za obveščevalno in varnostno dejavnost, tako da vključujejo tudi nadzor nad obveščevalno skupnostjo, ki presega tri službe, in omogoča naknadni nadzor nad operativnimi dejavnostmi služb v zvezi z vprašanji večjega nacionalnega interesa.

([245]) Člen 1 zakona o pravosodju in varnosti iz leta 2013. Ministri ne morejo biti člani. Člani opravljajo funkcije v odboru za obveščevalno in varnostno dejavnost do konca mandata parlamenta, v času katerega so bili imenovani. Odpoklicani so lahko, če to potrdi dom parlamenta, ki jih je imenoval, ali če prenehajo biti poslanci ali prevzamejo vlogo ministra. Član lahko tudi odstopi.

([246]) Poročila in izjave odbora so na voljo na povezavi: http://isc.independent.gov.uk/committee-reports. Odbor za obveščevalno in varnostno dejavnost je leta 2015 izdal poročilo z naslovom Privacy and Security: A modern and transparent legal framework (Zasebnost in varnost: sodoben in pregleden pravni okvir; glej: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), v katerem je proučil pravni okvir za tehnike nadzora, ki jih uporabljajo obveščevalne službe, ter izdal vrsto priporočil, ki so bila nato proučena in vključena v osnutek predloga zakona o preiskovalnih pooblastilih, preoblikovanega v zakon, tj. zakon o preiskovalnih pooblastilih iz leta 2016 (Investigatory Powers Act 2016). Odgovori vlade na navedeno poročilo so na voljo na povezavi: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

o operativnih zadevah, kadar se ne nanašajo na potekajoče operacije ([247]). V memorandumu o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost ([248]) so podrobno določeni elementi, ki se upoštevajo pri presoji, ali dejavnost ni del katere koli potekajoče operacije ([249]). Predsednik vlade lahko navedenemu odboru naroči tudi preiskavo tekočih operacij, poleg tega lahko odbor prouči informacije, ki jih agencije predložijo prostovoljno.

(145) Odbor za obveščevalno in varnostno dejavnost lahko v skladu z dodatkom 1 k zakonu o pravosodju in varnosti iz leta 2013 prosi vodjo katere koli od treh obveščevalnih služb, da razkrije informacije. Služba mora take informacije dati na voljo, razen če pristojni minister vloži veto ([250]). Organi Združenega kraljestva so pojasnili, da se v praksi redko zgodi, da temu odboru kakšne informacije ne bi bile razkrite ([251]).

(146) Glede pravnih sredstev lahko posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 165(2) zakona o varstvu podatkov iz leta 2018 vloži pritožbo pri odboru za obveščevalno in varnostno dejavnost, če meni, da v zvezi z osebnimi podatki, ki se nanašajo nanj, obstaja kršitev iz dela 4 zakona o varstvu podatkov iz leta 2018, vključno z zlorabo odstopanj in omejitev na področju nacionalne varnosti.

(147) Poleg tega so posamezniki v skladu z delom 4 zakona o varstvu podatkov iz leta 2018 upravičeni, da pri sodišču High Court (ali sodišču Court of Session na Škotskem) vložijo predlog za izdajo odločbe, ki od upravljavca zahteva, da upošteva pravice do dostopa do podatkov ([252]), do ugovora obdelavi ([253]) in do popravka ali izbrisa.

(148) Posamezniki so prav tako upravičeni zahtevati odškodnino za škodo, ki nastane zaradi kršitve zahteve iz dela 4 zakona o varstvu podatkov iz leta 2018 s strani upravljavca ali obdelovalca ([254]). Škoda vključuje finančno in nefinančno izgubo, kot je na primer stiska ([255]).

(149) Nazadnje, posameznik lahko zaradi ravnanja s strani ali v imenu obveščevalnih agencij Združenega kraljestva ([256]) vloži pritožbo pri sodišču, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal). To sodišče je ustanovljeno z zakonom o urejanju preiskovalnih pooblastil iz leta 2000 za Anglijo, Wales in Severno Irsko in zakonom o urejanju preiskovalnih pooblastil (Škotska) iz leta 2000 za Škotsko ter je neodvisno od izvršilne veje oblasti ([257]). Člane tega sodišča v skladu s členom 65 zakona o urejanju preiskovalnih pooblastil iz leta 2000 imenuje kraljica za obdobje petih let.

(150) Člana tega sodišča lahko s funkcije razreši kraljica, na podlagi nagovora ([258]) obeh domov parlamenta ([259]).

(151) Da lahko posameznik vloži tožbo pri sodišču, ki obravnava preiskovalna pooblastila („procesno upravičenje“), mora biti v skladu s členom 65 zakona o urejanju preiskovalnih pooblastil iz leta 2000 prepričan o (i) obstoju ravnanja, ki ga je obveščevalna služba storila v zvezi z njim, njegovim premoženjem, komunikacijami, ki jih je poslal ali so mu bile poslane ali namenjene, ali uporabo poštnih storitev, telekomunikacijskih storitev ali telekomunikacijskega sistema ([260]), ter

([247]) Člen 2 zakona o pravosodju in varnosti iz leta 2013.
([248]) Memorandum o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost je na voljo na povezavi: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Memorandum o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost, odstavek 14, glej opombo 248.
([250]) Pristojni minister lahko vloži veto na razkritje informacij le iz dveh razlogov: informacije so občutljive in odboru za obveščevalno in varnostno dejavnost ne smejo biti razkrite zaradi nacionalne varnosti ali je narava informacij taka, da bi se pristojnemu ministru, če bi jih moral predstaviti pred resornim odborom spodnjega doma parlamenta Združenega kraljestva (zaradi razlogov, ki niso omejeni na nacionalno varnost), zdelo ustrezno, da tega ne stori (odstavek 4(2) dodatka 1 k zakonu o pravosodju in varnosti iz leta 2013).
([251]) Obrazložitveni okvir Združenega kraljestva, oddelek H: Nacionalna varnost, str. 43.
([252]) Člen 94(11) zakona o varstvu podatkov iz leta 2018.
([253]) Člen 99(4) zakona o varstvu podatkov iz leta 2018.
([254]) Člen 169 zakona o varstvu podatkov iz leta 2018 dopušča zahtevke „osebe, ki utrpi škodo zaradi kršitve zahteve iz zakonodaje o varstvu podatkov“.
([255]) Člen 169(5) zakona o varstvu podatkov iz leta 2018.
([256]) Glej člen 65(2)(b) zakona o urejanju preiskovalnih pooblastil.
([257]) V skladu z dodatkom 3 k zakonu o urejanju preiskovalnih pooblastil iz leta 2000 morajo imeti člani določene izkušnje na pravosodnem področju in so lahko ponovno imenovani.
([258]) Za pojem „nagovor (Address)“ glej opombo 183.
([259]) Odstavek 1(5) dodatka 3 k zakonu o urejanju preiskovalnih pooblastil iz leta 2000.
([260]) Člen 65(4) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

(ii) o tem, da je bilo ravnanje storjeno v „spornih okoliščinah“ ([261]) ali „storjeno s strani ali v imenu obveščevalnih služb“ ([262]). Ker se je zlasti ta standard prepričanja razlagal precej široko ([263]), se za predložitev zadeve navedenemu sodišču zahteva razmeroma nizek prag procesnega upravičenja.

(152) Sodišče, ki obravnava preiskovalna pooblastila, mora pri obravnavanju vložene pritožbe proučiti, ali so osebe, zoper katere je vložena pritožba, ukrepale v razmerju do pritožnika ter kako je ravnal organ, ki je domnevno vpleten v kršitve, in ali je bilo domnevno ravnanje storjeno ([264]). Kadar sodišče, ki obravnava preiskovalna pooblastila, vodi postopek, mora pri sprejemanju odločitve v tem postopku uporabiti ista načela, kot bi jih uporabilo sodišče na podlagi zahteve za sodno presojo ([265]).

(153) Sodišče, ki obravnava preiskovalna pooblastila, mora pritožnika obvestiti, ali je bila odločitev v njegovo korist ali ne ([266]). Sodišče, ki obravnava preiskovalna pooblastila, lahko v skladu s členom 67(6) in (7) zakona o urejanju preiskovalnih pooblastil iz leta 2000 izdaja začasne odredbe in priznava odškodnine ali izdaja druge odredbe, ki se mu zdijo primerne ([267]). V skladu s členom 67A zakona o urejanju preiskovalnih pooblastil iz leta 2000 se je mogoče pritožiti zoper odločitev sodišča, ki obravnava preiskovalna pooblastila, in sicer na podlagi dovoljenja tega sodišča ali ustreznega pritožbenega sodišča.

(154) Posamezniki lahko pri sodišču, ki obravnava preiskovalna pooblastila, zlasti vložijo tožbo – in uveljavljajo pravna sredstva – kadar menijo, da je javni organ ravnal (ali predlaga ravnanje) na način, ki ni skladen s pravicami iz EKČP, vključno s pravico do zasebnosti in do varstva podatkov, kar je posledično nezakonito na podlagi člena 6(1) zakona o človekovih pravicah iz leta 1998. Sodišču, ki obravnava preiskovalna pooblastila, je bila podeljena izključna pristojnost za vse pritožbene zahtevke v zvezi z obveščevalnimi agencijami, ki se nanašajo na zakon o človekovih pravicah. Kot je navedlo sodišče High Court, to pomeni, da „lahko o tem, ali je bil na podlagi dejstev v posamezni zadevi kršen zakon o človekovih pravicah, načeloma odloča neodvisno sodišče, ki lahko ima dostop do vsega ustreznega gradiva, tudi tajnega. […] Pri tem upoštevamo tudi, da se je zoper odločitev sodišča, ki obravnava preiskovalna pooblastila, zdaj mogoče pritožiti pri ustreznem pritožbenem sodišču (v Angliji in Walesu je to sodišče Court of Appeal), sodišče Supreme Court pa je pred kratkim ugotovilo, da je načeloma mogoče zahtevati sodno presojo zoper odločitve sodišča, ki obravnava preiskovalna pooblastila: glej sodbo v zadevi R (Privacy International) proti Investigatory Powers Tribunal [2019] UKSC 22, [2019] 2 WLR 1219“ ([268]). Če sodišče, ki obravnava preiskovalna pooblastila, ugotovi, da je katero koli dejanje javnega organa nezakonito, lahko odobri odškodnino ali pravno sredstvo ali izda odredbo, kot meni, da je pravično in ustrezno ter za katero je pristojno ([269]).

([261]) Take okoliščine se nanašajo na obstoj ravnanja javnih organov po pooblastilu (npr. nalog za prijetje, dovoljenje/obvestilo za pridobitev podatkov o komunikacijah itd.) ali v primeru okoliščin (ne glede na to, ali tako pooblastilo obstaja ali ne), v katerih obstoj ravnanja ne bi bil ustrezen brez pooblastila ali vsaj brez ustrezne proučitve, ali bi bilo tako pooblastilo potrebno. Ravnanje, ki ga odobri pravosodni pooblaščenec, se obravnava kot ravnanje, storjeno v spornih okoliščinah (člen 65(7ZA) zakona o urejanju preiskovalnih pooblastil iz leta 2000), medtem ko se za druga ravnanja, storjena z dovoljenjem osebe, ki opravlja sodno funkcijo, šteje, da niso bila storjena v spornih okoliščinah (člen 65(7) in (8) zakona o urejanju preiskovalnih pooblastil iz leta 2000).

([262]) Iz informacij organov Združenega kraljestva izhaja, da glede na nizek prag za vložitev pritožbe ni nenavadno, da se med preiskavo sodišča, ki obravnava preiskovalna pooblastila, ugotovi, da javni organ dejansko ni nikoli preiskoval pritožnika. V zadnjem statističnem poročilu sodišča, ki obravnava preiskovalna pooblastila, je navedeno, da je to sodišče leta 2016 prejelo 209 pritožb, od katerih jih je bilo 52 % obravnavanih kot neresnih ali zlonamernih, pri 25 % pa ni bilo mogoče podati ugotovitve. Organi Združenega kraljestva so pojasnili, da to pomeni, da v zvezi s pritožnikom niso bile uporabljene prikrite dejavnosti/pooblastila ali pa so bile uporabljene prikrite metode, vendar je sodišče ugotovilo, da so bile zakonite. Poleg tega je za 11 % pritožb veljalo, da je bilo ugotovljeno, da sodišče zanje ni pristojno, da so bile umaknjene ali da so neveljavne, 5 % pritožb ni bilo vloženih pravočasno, v 7 % pa je bilo odločeno v korist pritožnika. Statistično poročilo sodišča, ki obravnava preiskovalna pooblastila, iz leta 2016, je na voljo na povezavi: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([263]) Glej sodbo v zadevi Human Rights Watch proti Secretary of State [2016] UKIPTrib15_165-CH. V tej zadevi je sodišče, ki obravnava preiskovalna pooblastila, s sklicevanjem na sodno prakso Evropskega sodišča za človekove pravice ugotovilo, da se prepričanje, da je bilo s strani ali v imenu katere koli obveščevalne službe storjeno katero koli ravnanje, ki spada v podčlen 68(5) zakona o urejanju preiskovalnih pooblastil iz leta 2000, ustrezno preskusi z obstojem podlage za tako prepričanje, kar pomeni tudi, da lahko posameznik trdi, da je žrtev kršitve, ki jo povzroči že sam obstoj tajnih ukrepov ali zakonodaje, ki dovoljuje tajne ukrepe, le, če lahko dokaže, da je zaradi svojega osebnega položaja v morebitni nevarnosti za izpostavljenost takim ukrepom (glej sodbo v zadevi Human Rights Watch proti Secretary of State, točka 41).

([264]) Člen 67(3) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([265]) Člen 67(2) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([266]) Člen 68(4) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

([267]) To lahko zajema odredbo, s katero se zahteva uničenje evidenc informacij, ki jih imajo javni organi glede katere koli osebe.

([268]) Sodba High Court of Justice v zadevi Liberty, [2019] EWHC 2057 (Admin), točka 170.

([269]) Člen 8(1) zakona o človekovih pravicah iz leta 1998.

(155) Ko posameznik izčrpa nacionalna pravna sredstva, se lahko obrne na Evropsko sodišče za človekove pravice zaradi kršitev pravic, zagotovljenih na podlagi EKČP, vključno s pravico do zasebnosti in do varstva podatkov.

(156) Iz navedenega izhaja, da izmenjava podatkov, prenesenih na podlagi tega sklepa, med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj Združenega kraljestva in drugimi javnimi organi, vključno z obveščevalnimi agencijami, poteka v okviru omejitev in pogojev, ki zagotavljajo, da bodo taki nadaljnji prenosi potrebni in sorazmerni ter da se pri njih upoštevajo posebni zaščitni ukrepi za varstvo podatkov na podlagi zakona o varstvu podatkov iz leta 2018. Poleg tega obdelavo podatkov s strani zadevnih javnih organov nadzorujejo neodvisni javni organi, zadevni posamezniki pa imajo dostop do učinkovitih pravnih sredstev.

3. SKLEPNA UGOTOVITEV

(157) Komisija meni, da del 3 zakona o varstvu podatkov iz leta 2018 zagotavlja, da je raven varstva osebnih podatkov, ki jih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pristojni organi v Uniji prenašajo pristojnim organom Združenega kraljestva, v osnovi enakovredna ravni, zagotovljeni z Direktivo (EU) 2016/680.

(158) Poleg tega Komisija meni, da gledano v celoti nadzorni mehanizmi in pravna sredstva v pravu Združenega kraljestva v praksi omogočajo, da se kršitve ugotovijo in kaznujejo, ter da so posameznikom, na katere se nanašajo osebni podatki, na voljo pravna sredstva, s katerimi lahko pridobijo dostop do osebnih podatkov, ki se nanašajo nanje, in po potrebi dosežejo popravek ali izbris takih podatkov.

(159) Komisija glede na razpoložljive informacije o pravnem redu Združenega kraljestva nazadnje meni, da so vsi posegi v temeljne pravice posameznikov, katerih osebne podatke iz Evropske unije v Združeno kraljestvo prenašajo javni organi Združenega kraljestva v imenu javnega interesa, tudi v okviru izmenjave osebnih podatkov med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in drugimi javnimi organi, kot so organi nacionalne varnosti, omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, ter da obstaja učinkovita pravna zaščita zoper take posege.

(160) Zato bi bilo treba odločiti, da Združeno kraljestvo zagotavlja ustrezno raven varstva v smislu člena 36(2) Direktive (EU) 2016/680, kot se razlaga ob upoštevanju Listine EU o temeljnih pravicah.

(161) Ta ugotovitev temelji na ustrezni nacionalni ureditvi Združenega kraljestva in na njegovih mednarodnih zavezah, zlasti zavezanosti Evropski konvenciji o varstvu človekovih pravic ter priznavanju pristojnosti Evropskega sodišča za človekove pravice. Nadaljnja zavezanost takim mednarodnim obveznostim je torej posebej pomemben element ocene, na kateri temelji ta sklep.

4. UČINKI TEGA SKLEPA IN UKREPI ORGANOV ZA VARSTVO PODATKOV

(162) Države članice in njihovi organi morajo sprejeti ukrepe, potrebne za zagotavljanje skladnosti z akti institucij Unije, saj se domneva, da so ti zakoniti in imajo pravne učinke, dokler se njihova veljavnost ne izteče, dokler niso preklicani, razglašeni za nične v okviru ničnostne tožbe ali razglašeni za neveljavne v okviru postopka predhodnega odločanja ali ugovora nezakonitosti.

(163) Zato je sklep Evropske komisije o ustreznosti, sprejet na podlagi člena 36(3) Direktive (EU) 2016/680, zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z njihovimi neodvisnimi nadzornimi organi. Natančneje, prenosi od upravljavca ali obdelovalca v Uniji upravljavcu ali obdelovalcu v Združenem kraljestvu lahko v obdobju uporabe tega sklepa potekajo, ne da bi bilo treba pridobiti nadaljnje dovoljenje.

(164) Hkrati je treba opozoriti, da v skladu s členom 47(5) Direktive (EU) 2016/680 in glede na pojasnila Sodišča v sodbi v zadevi Schrems velja, da če ima nacionalni organ za varstvo podatkov, med drugim kadar je prejel pritožbo, pomisleke o skladnosti sklepa Komisije o ustreznosti s temeljnimi pravicami posameznika do zasebnosti in varstva podatkov, mu mora nacionalno pravo zagotavljati pravno sredstvo za predložitev teh očitkov nacionalnemu sodišču, od katerega se lahko zahteva, da Sodišču predloži predlog za sprejetje predhodne odločbe ([270]).

([270]) Sodba v zadevi Schrems, točka 65.

5. **SPREMLJANJE, ZAČASNO ZADRŽANJE IZVAJANJA, RAZVELJAVITEV ALI SPREMEMBA TEGA SKLEPA**

(165) Komisija v skladu s členom 36(4) Direktive (EU) 2016/680 redno spremlja razvoj dogodkov v Združenem kraljestvu po sprejetju tega sklepa, da lahko presodi, ali Združeno kraljestvo še vedno zagotavlja v osnovi enakovredno raven varstva. Tako spremljanje je v tem primeru še posebej pomembno, saj bo Združeno kraljestvo upravljalo, uporabljalo in izvajalo novo ureditev varstva podatkov, za katero se ne uporablja več pravo Unije in se bo morda spremenila. Posebna pozornost v okviru tega spremljanja bo namenjena temu, kako Združeno kraljestvo v praksi uporablja svoja pravila za prenose osebnih podatkov v tretje države, vključno s sklenitvijo mednarodnih sporazumov, ter učinek, ki ga lahko to ima na raven varstva, ki se zagotavlja za podatke, ki se prenesejo na podlagi tega sklepa, pa tudi na učinkovitost uveljavljanja pravic posameznika na področjih, zajetih s tem sklepom. Komisija bo pri spremljanju med drugim upoštevala razvoj sodne prakse ter nadzor, ki ga izvajajo urad informacijskega pooblaščenca in drugi neodvisni organi.

(166) Za lajšanje tega spremljanja bi morali organi Združenega kraljestva Komisijo brez odlašanja in redno obveščati o vsaki bistveni spremembi pravnega reda Združenega kraljestva, ki vpliva na pravni okvir, ki je predmet tega sklepa, ter o vsakem razvoju praks v zvezi z obdelavo osebnih podatkov, ocenjenih v tem sklepu, zlasti glede elementov, omenjenih v uvodni izjavi (165).

(167) Poleg tega bi morale države članice Komisijo obveščati o vseh pomembnih ukrepih nacionalnih organov za varstvo podatkov, zlasti glede poizvedb ali pritožb posameznikov iz EU, na katere se nanašajo osebni podatki, v zvezi s prenosom osebnih podatkov iz Unije pristojnim organom v Združenem kraljestvu, da lahko Komisija učinkovito izvaja naloge spremljanja. Komisija bi morala biti obveščena tudi o vseh indicih, da ukrepi javnih organov Združenega kraljestva, odgovornih za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj, vključno z vsemi nadzornimi organi, ne zagotavljajo zahtevane ravni varstva.

(168) Če se na podlagi razpoložljivih informacij, zlasti tistih, ki izhajajo iz spremljanja tega sklepa ali ki jih zagotovijo organi Združenega kraljestva ali držav članic, ugotovi, da raven varstva, ki ga zagotavlja Združeno kraljestvo, morda ni več ustrezna, bi morala Komisija o tem nemudoma obvestiti pristojne organe Združenega kraljestva in zahtevati, da v določenem roku, ki ne sme presegati treh mesecev, sprejmejo ustrezne ukrepe. To obdobje se lahko po potrebi podaljša za določeno obdobje, pri čemer se upoštevata narava zadevnega vprašanja in/ali ukrepov, ki jih je treba sprejeti.

(169) Če pristojni organi Združenega kraljestva ob preteku tega določenega roka ne sprejmejo navedenih ukrepov ali drugače zadovoljivo dokažejo, da ta sklep še naprej temelji na ustrezni ravni varstva, bo Komisija začela postopek iz člena 58(2) Direktive (EU) 2016/680 za začasno zadržanje izvajanja ali za razveljavitev dela ali celotnega tega sklepa.

(170) Druga možnost je, da bo Komisija začela postopek za spremembo tega sklepa, zlasti z uvedbo dodatnih pogojev za prenos podatkov ali z omejitvijo področja uporabe ugotovitve o ustreznosti samo na prenose podatkov, za katere je še naprej zagotovljena ustrezna raven varstva.

(171) Komisija bo v nujnih in ustrezno utemeljenih primerih uporabila možnost, da v skladu s postopkom iz člena 58(3) Direktive (EU) 2016/680 sprejme izvedbene akte, ki se začnejo uporabljati takoj in s katerimi se začasno zadrži izvajanje tega sklepa oziroma se sklep razveljavi ali spremeni.

6. **TRAJANJE IN PODALJŠANJE VELJAVNOSTI TEGA SKLEPA**

(172) Upoštevati je treba, da bo Združeno kraljestvo ob koncu prehodnega obdobja, določenega v sporazumu o izstopu, in takoj po prenehanju uporabe začasne določbe iz člena 782 sporazuma o trgovini in sodelovanju med EU in Združenim kraljestvom upravljalo, uporabljalo in izvajalo novo ureditev varstva podatkov, ne pa več ureditve, ki je veljala, ko jo je zavezovalo pravo Evropske unije. To lahko vključuje zlasti dopolnitve ali spremembe okvira varstva podatkov, ki se ocenjuje v tem sklepu, ter drug ustrezen razvoj.

(173) Zato je primerno določiti, da ta sklep velja štiri leta od začetka njegove veljavnosti.

(174) Kadar zlasti iz informacij, ki izhajajo iz spremljanja tega sklepa, izhaja, da so ugotovitve, ki se nanašajo na ustreznost ravni varstva, ki se zagotavlja v Združenem kraljestvu, še vedno dejansko in pravno upravičene, bi morala Komisija najpozneje šest mesecev pred prenehanjem uporabe tega sklepa začeti postopek za spremembo tega sklepa, tako da se veljavnost načeloma podaljša za dodatna štiri leta. Vsak tak izvedbeni akt, ki spreminja ta sklep, mora biti sprejet v skladu s postopkom iz člena 58(2) Direktive (EU) 2016/680.

7. **SKLEPNE UGOTOVITVE**

(175) Evropski odbor za varstvo podatkov je objavil svoje mnenje ([271]), ki je bilo upoštevano pri pripravi tega sklepa.

(176) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 58 Direktive (EU) 2016/680.

(177) V skladu s členom 6a Protokola št. 21 o stališču Združenega kraljestva in Irske v zvezi z območjem svobode, varnosti in pravice, ki je priložen PEU in PDEU, pravila iz Direktive (EU) 2016/680 in zato tega izvedbenega sklepa, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar opravljajo dejavnosti s področja uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU, za Irsko niso zavezujoča, če je ne zavezujejo pravila, ki urejajo oblike pravosodnega sodelovanja v kazenskih zadevah ali policijskega sodelovanja, v okviru katerih je treba upoštevati določbe, sprejete na podlagi člena 16 PDEU. Poleg tega Irska na podlagi Izvedbenega sklepa Sveta (EU) 2020/1745 ([272]) od 1. januarja 2021 začasno izvaja in uporablja Direktivo (EU) 2016/680. Irsko zato zavezuje ta izvedbeni sklep pod enakimi pogoji, kot veljajo za uporabo Direktive (EU) 2016/680 na Irskem, kakor so bili določeni v Izvedbenem sklepu Sveta (EU) 2020/1745 glede schengenskega pravnega reda, v katerem sodeluje.

(178) V skladu s členoma 2 in 2a Protokola št. 22 o stališču Danske, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, pravila iz Direktive (EU) 2016/680 in zato tega izvedbenega sklepa, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar opravljajo dejavnosti s področja uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU, za Dansko niso zavezujoča in se v njej ne uporabljajo. Ker Direktiva (EU) 2016/680 nadgrajuje schengenski pravni red, je Danska v skladu s členom 4 navedenega protokola 26. oktobra 2016 priglasila svojo odločitev o izvajanju Direktive (EU) 2016/680. Danska je tako v skladu z mednarodnim pravom zavezana izvajati ta izvedbeni sklep.

(179) Kar zadeva Islandijo in Norveško, ta izvedbeni sklep pomeni razvoj določb schengenskega pravnega reda v smislu Sporazuma, sklenjenega med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško v zvezi s pridružitvijo teh dveh držav k izvajanju, uporabi in razvoju schengenskega pravnega reda ([273]).

(180) Kar zadeva Švico, ta izvedbeni sklep pomeni razvoj določb schengenskega pravnega reda v smislu Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda ([274]).

(181) Kar zadeva Lihtenštajn, ta izvedbeni sklep pomeni razvoj določb schengenskega pravnega reda v smislu Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda ([275]) –

([271]) Mnenje št. 15/2021 o osnutku izvedbenega sklepa Evropske komisije v skladu z Direktivo (EU) 2016/680 o ustreznem varstvu osebnih podatkov v Združenem kraljestvu, na voljo na naslednji povezavi: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Izvedbeni sklep Sveta (EU) 2020/1745 z dne 18. novembra 2020 o začetku izvajanja določb schengenskega pravnega reda o varstvu podatkov in začetku začasnega izvajanja nekaterih določb schengenskega pravnega reda na Irskem (UL L 393, 23.11.2020, str. 3).

([273]) UL L 176, 10.7.1999, str. 36.

([274]) UL L 53, 27.2.2008, str. 52.

([275]) UL L 160, 18.6.2011, str. 21.

SPREJELA NASLEDNJI SKLEP:

Člen 1

Združeno kraljestvo za namene člena 36 Direktive (EU) 2016/680 zagotavlja ustrezno raven varstva osebnih podatkov, ki se iz Evropske unije prenesejo javnim organom v Združenem kraljestvu, pristojnim za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij.

Člen 2

Kadar pristojni nadzorni organi države članice zaradi varstva posameznikov pri obdelavi njihovih osebnih podatkov izvajajo svoja pooblastila na podlagi člena 47 Direktive (EU) 2016/680 v zvezi s prenosi podatkov javnim organom v Združenem kraljestvu na področju uporabe iz člena 1, zadevna država članica o tem brez odlašanja obvesti Komisijo.

Člen 3

1. Komisija stalno spremlja uporabo pravnega okvira, na katerem temelji ta sklep, vključno s pogoji, pod katerimi se izvajajo nadaljnji prenosi in uveljavljajo pravice posameznika, da se oceni, ali Združeno kraljestvo še naprej zagotavlja ustrezno raven varstva v smislu člena 1.

2. Države članice in Komisija se medsebojno obveščajo o primerih, ko informacijski pooblaščenec ali kateri koli drug pristojni organ Združenega kraljestva ne zagotovi skladnosti s pravnim okvirom, na katerem temelji ta sklep.

3. Države članice in Komisija se medsebojno obveščajo o vseh indicih, da posegi javnih organov Združenega kraljestva v pravico posameznikov do varstva njihovih osebnih podatkov presegajo tisto, kar je nujno potrebno, ali da zoper take posege ni učinkovitega pravnega varstva.

4. Če Komisija utemeljeno sumi, da ustrezna raven varstva ni več zagotovljena, o tem obvesti pristojne organe Združenega kraljestva in lahko začasno zadrži izvajanje tega sklepa, ga razveljavi ali spremeni.

5. Komisija lahko začasno zadrži izvajanje tega sklepa, ga razveljavi ali spremeni tudi, če zaradi nesodelovanja vlade Združenega kraljestva ne more ugotoviti, ali je ugotovitev iz člena 1 prizadeta.

Člen 4

Ta sklep preneha veljati 27. junija 2025, razen če je podaljšan v skladu s postopkom iz člena 58(2) Direktive (EU) 2016/680.

Člen 5

Ta sklep je naslovljen na države članice.

V Bruslju, 28. junija 2021

Za Komisijo
Didier REYNDERS
član Komisije

IZVEDBENI SKLEP SVETA (EU) 2021/1774

z dne 5. oktobra 2021

o spremembi Izvedbenega sklepa (EU) 2018/1493 o dovoljenju Madžarski, da uvede posebni ukrep, ki odstopa od točke (a) člena 26(1) ter členov 168 in 168a Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost ([1]) in zlasti člena 395(1), prvi pododstavek, Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Z Izvedbenim sklepom Sveta (EU) 2018/1493 ([2]) je bilo Madžarski dovoljeno, da do 31. decembra 2021 uporablja posebni ukrep, ki na eni strani omejuje pravico do odbitka davka na dodano vrednost (DDV) na izdatke v zvezi z osebnimi avtomobili, ki se ne uporabljajo izključno za poslovne namene, na 50 %, z odstopanjem od členov 168 in 168a Direktive 2006/112/ES, ter na drugi strani določa, da se uporaba osebnega avtomobila, vključenega v sredstva davčnega zavezanca, za neposlovne namene ne obravnava kot storitev za plačilo, kadar za zadevni avtomobil velja omejitev, ki se dovoli na podlagi člena 1 navedenega izvedbenega sklepa, z odstopanjem od člena 26(1), točka (a), navedene direktive (v nadaljnjem besedilu: posebni ukrep).

(2) Madžarska je z dopisom, ki ga je Komisija evidentirala 25. februarja 2021, zaprosila za dovoljenje za nadaljnjo uporabo posebnega ukrepa (v nadaljnjem besedilu: zahteva za podaljšanje).

(3) Na podlagi člena 395(2), drugi pododstavek, Direktive 2006/112/ES je Komisija z dopisom z dne 7. aprila 2021 zahtevo Madžarske posredovala drugim državam članicam. Z dopisom z dne 8. aprila 2021 je Komisija uradno obvestila Madžarsko, da ima vse informacije, potrebne za presojo zahteve za podaljšanje.

(4) Na podlagi člena 5 Izvedbenega sklepa (EU) 2018/1493 je Madžarska skupaj z zahtevo za podaljšanje predložila poročilo, ki vključuje pregled odstotka, določenega za odbitek DDV. Madžarska na podlagi trenutno razpoložljivih informacij, in sicer rezultatov davčnega nadzora in statističnih podatkov v zvezi z zasebno uporabo osebnih avtomobilov, v svoji zahtevi za podaljšanje potrjuje, da je omejitev na 50 % še vedno upravičena in primerna. Poleg tega se je pri poenostavljenem pobiranju DDV s posebnim ukrepom dejansko zmanjšalo upravno breme za podjetja in davčne organe. Hkrati preprečuje davčno utajo zaradi nepravilnega vodenja evidenc. Zato bi bilo treba Madžarski dovoliti nadaljnjo uporabo posebnega ukrepa.

([1]) UL L 347, 11.12.2006, str. 1.

([2]) Izvedbeni sklep Sveta (EU) 2018/1493 z dne 2. oktobra 2018 o dovoljenju Madžarski, da uvede posebni ukrep, ki odstopa od točke (a) člena 26(1) ter členov 168 in 168a Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 252, 8.10.2018, str. 44).

(5) Podaljšanje posebnega ukrepa bi bilo treba časovno omejiti, da se lahko ocenita njegova učinkovitost in ustrezen odstotek. Madžarski bi bilo zato treba dovoliti, da posebni ukrep uporablja še naprej za omejeno obdobje do 31. decembra 2024.

(6) Če bi Madžarska menila, da je potrebno podaljšanje dovoljenja po letu 2024, bi morala Komisiji najpozneje do 31. marca 2024 predložiti poročilo, ki vključuje pregled odstotkovne omejitve, skupaj z zahtevo za podaljšanje.

(7) Posebni ukrep bo imel zgolj zanemarljiv učinek na skupni znesek davčnih prihodkov, zbranih na ravni končne potrošnje, in ne bo negativno vplival na lastna sredstva Unije iz pobranega DDV.

(8) Izvedbeni sklep (EU) 2018/1493 bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Člen 5 Izvedbenega sklepa (EU) 2018/1493 se nadomesti z naslednjim:

„*Člen 5*

Ta sklep se uporablja od 1. januarja 2019 do 31. decembra 2024.

Vsaka zahteva za podaljšanje dovoljenja iz tega sklepa se predloži Komisiji do 31. marca 2024, priloži pa se ji poročilo, ki vključuje pregled odstotka iz člena 1.“

Člen 2

Ta sklep začne učinkovati z dnem uradne obvestitve.

Člen 3

Ta sklep je naslovljen na Madžarsko.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

IZVEDBENI SKLEP SVETA (EU) 2021/1775

z dne 5. oktobra 2021

o spremembi Izvedbenega sklepa (EU) 2018/789 o dovoljenju Madžarski, da uvede posebni ukrep, ki odstopa od člena 193 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost ([1]) in zlasti člena 395(1), prvi pododstavek, Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Člen 193 Direktive 2006/112/ES določa, da je davčni zavezanec, ki dobavlja blago ali storitve, po splošnem pravilu dolžan plačati davek na dodano vrednost (DDV) davčnim organom.

(2) Madžarski je bilo z Izvedbenim sklepom Sveta (EU) 2018/789 ([2]) dovoljeno, da uvede ukrep, ki odstopa od člena 193 Direktive 2006/112/ES, kar zadeva osebo, ki je dolžna plačati DDV, v primerih kadar so nekatere vrste dobave opravljene s strani davčnih zavezancev, ki so v postopku likvidacije ali v katerem koli drugem postopku, s katerim se sodno ugotovi insolventnost (v nadaljnjem besedilu: posebni ukrep).

(3) Madžarska je z dopisom, ki ga je Komisija evidentirala 18. februarja 2021, Komisiji predložila zahtevo za podaljšanje dovoljenja za uporabo posebnega ukrepa do 31. decembra 2026 (v nadaljnjem besedilu: zahteva). Madžarska je zahtevi priložila poročilo, ki vključuje pregled posebnega ukrepa.

(4) Na podlagi člena 395(2), drugi pododstavek, Direktive 2006/112/ES je Komisija z dopisom z dne 7. aprila 2021 posredovala zahtevo drugim državam članicam. Z dopisom z dne 8. aprila 2021 je Komisija uradno obvestila Madžarsko, da ima vse informacije, potrebne za presojo zahteve.

(5) Madžarska trdi, da davčni zavezanci v postopku likvidacije ali insolventnosti davčnim organom pogosto ne plačajo dolgovanega DDV. Hkrati lahko kupec, ki je davčni zavezanec s pravico do odbitka, še vedno odbije nastali DDV, kar ima negativen učinek na proračun in s čimer se financira likvidacija. Madžarska je prav tako evidentirala primere goljufije, ko so podjetja v postopku likvidacije izdajala navidezne račune aktivnim podjetjem in znatno zmanjšala svoje davčne obveznosti brez kakršnega koli jamstva, da bo izdajatelj plačal dolgovani DDV.

(6) Člen 199(1), točka (g), Direktive 2006/112/ES omogoča državam članicam, da določijo, da je oseba, ki je dolžna plačati DDV, davčni zavezanec, za katerega se opravi dobava nepremičnin, ki jih prodaja dolžnik po sodbi v postopku obvezne prodaje drugi osebi (v nadaljnjem besedilu: mehanizem obrnjene davčne obveznosti). Posebni ukrep Madžarski omogoča, da uporabo mehanizma obrnjene davčne obveznosti razširja na druge vrste dobave s strani davčnih zavezancev, ki so v postopku insolventnosti, in sicer za dobavo investicijskega blaga in dobavo drugega blaga in storitev s tržno vrednostjo nad 100 000 HUF.

([1]) UL L 347, 11.12.2006, str. 1.

([2]) Izvedbeni sklep Sveta (EU) 2018/789 z dne 25. maja 2018 o dovoljenju Madžarski, da uvede posebni ukrep, ki odstopa od člena 193 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 134, 31.5.2018, str. 10).

(7) Na podlagi informacij, ki jih je predložila Madžarska, uporaba mehanizma obrnjene davčne obveznosti za te vrste transakcij učinkovito poenostavlja pobiranje davkov in preprečuje davčne utaje. Izvajanje posebnega ukrepa omejuje izgube javnih prihodkov in ustvarja dodatne proračunske prihodke. Poleg tega bi lahko gospodarski učinki pandemije COVID-19 v bližnji prihodnosti povzročili močno povečanje števila likvidacij, zaradi česar bi bilo treba posebni ukrep podaljšati.

(8) Zahtevano odstopanje bi moralo biti časovno omejeno, davčna uprava pa bi vseeno morala imeti čas, da uvede druge običajne ukrepe za reševanje problema in zmanjšanje izgub v javnem proračunu, zlasti tistih, povezanih z goljufivim ravnanjem, preden se posebni ukrep izteče, s čimer bi dodatno podaljšanje posebnega ukrepa postalo nepotrebno. Odstopanje, ki dovoljuje uporabo mehanizma obrnjene davčne obveznosti, je odobreno samo izjemoma za določena področja goljufij in pomeni sredstvo v skrajni sili. Dovoljenje bi bilo zato treba podaljšati samo do 31. decembra 2024.

(9) Posebni ukrep ne bo imel negativnega učinka na lastna sredstva Unije iz naslova DDV.

(10) Izvedbeni sklep (EU) 2018/789 bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

V členu 2 Izvedbenega sklepa (EU) 2018/789 se drugi odstavek nadomesti z naslednjim:

„Ta sklep preneha veljati 31. decembra 2024.“

Člen 2

Ta sklep začne učinkovati z dnem uradne obvestitve.

Člen 3

Ta sklep je naslovljen na Madžarsko.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

IZVEDBENI SKLEP SVETA (EU) 2021/1776

z dne 5. oktobra 2021

o spremembi Odločbe 2009/791/ES o dovoljenju Zvezni republiki Nemčiji, da še naprej uporablja ukrep z odstopanjem od člena 168 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost ([1]) in zlasti člena 395(1), prvi pododstavek, Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Člena 168 in 168a Direktive 2006/112/ES določata, da imajo davčni zavezanci pravico odbiti davek na dodano vrednost (DDV), obračunan pri dobavi blaga in storitev, prejetih za namene njihovih obdavčenih transakcij. Zvezni republiki Nemčiji (v nadaljnjem besedilu: Nemčija) se je dovolila uvedba ukrepa odstopanja, namenjenega izključitvi pravice do odbitka DDV na blago in storitve, kadar davčni zavezanec to blago in storitve uporablja več kot 90-odstotno za svoje zasebne namene ali za namene svojih zaposlenih ali na splošno za neposlovne namene ali negospodarske dejavnosti.

(2) Prvotno je bilo z Odločbo Sveta 2000/186/ES ([2]) Nemčiji dovoljeno, da uvede in uporablja ukrepa, ki odstopata od členov 6 in 17 Direktive Sveta 77/388/EGS ([3]), do 31. decembra 2002. Z Odločbo Sveta 2003/354/ES ([4]) je bilo Nemčiji dovoljeno, da uporablja ukrep, ki odstopa od člena 17 Direktive 77/388/EGS, do 30. junija 2004. Z Odločbo Sveta 2004/817/ES ([5]) je bilo navedeno dovoljenje podaljšano do 31. decembra 2009.

(3) Z Odločbo Sveta 2009/791/ES ([6]) je bilo Nemčiji dovoljeno, da še naprej uporablja ukrep, ki odstopa od člena 168 Direktive 2006/112/ES. Po več zaporednih podaljšanih preneha navedeno dovoljenje veljati 31. decembra 2021.

(4) Z Direktivo Sveta 2009/162/EU ([7]) se je v Direktivo 2006/112/ES vstavil člen 168a, da bi se odbitek omejil na delež dejanske poslovne uporabe in bi se tako učinkoviteje uporabilo načelo, po katerem odbitek nastane le, če se zadevno blago in storitve uporabljajo za poslovne namene davčnega zavezanca. Člen 1 Odločbe 2009/791/ES se je spremenil, da vključuje sklic na člen 168a Direktive 2006/112/ES. Naslov Odločbe 2009/791/ES se mora zato sklicevati tudi na člen 168a Direktive 2006/112/ES.

([1]) UL L 347, 11.12.2006, str. 1.

([2]) Odločba Sveta 2000/186/ES z dne 28. februarja 2000 o dovoljenju Zvezni republiki Nemčiji, da uporabi ukrepa z odstopanjem od členov 6 in 17 Šeste direktive 77/388/EGS o usklajevanju zakonodaje držav članic o prometnih davkih – Skupni sistem davka na dodano vrednost: enotna osnova za odmero (UL L 59, 4.3.2000, str. 12).

([3]) Šesta direktiva Sveta 77/388/EGS z dne 17. maja 1977 o usklajevanju zakonodaje držav članic o prometnih davkih – Skupni sistem davka na dodano vrednost: enotna osnova za odmero (UL L 145, 13.6.1977, str. 1).

([4]) Odločba Sveta 2003/354/ES z dne 13. maja 2003 o dovoljenju Nemčiji, da uporabi ukrep z odstopanjem od člena 17 Šeste direktive 77/388/EGS o usklajevanju zakonodaje držav članic o prometnih davkih (UL L 123, 17.5.2003, str. 47).

([5]) Odločba Sveta 2004/817/ES z dne 19. novembra 2004 o dovoljenju Nemčiji, da uporabi ukrep z odstopanjem od člena 17 Šeste direktive 77/388/EGS o usklajevanju zakonodaje držav članic o prometnih davkih (UL L 357, 2.12.2004, str. 33).

([6]) Odločba Sveta 2009/791/ES z dne 20. oktobra 2009 o dovoljenju Zvezni republiki Nemčiji, da še naprej uporablja ukrep z odstopanjem od člena 168 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 283, 30.10.2009, str. 55).

([7]) Direktiva Sveta 2009/162/EU z dne 22. decembra 2009 o spremembi nekaterih določb Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 10, 15.1.2010, str. 14).

(5) Nemčija je z dopisom, ki ga je Komisija evidentirala dne 19. februarja 2021, Komisiji predložila zahtevo (v nadaljnjem besedilu: zahteva) za podaljšanje dovoljenja za nadaljnjo uporabo ukrepa, ki odstopa od členov 168 in 168a Direktive 2006/112/ES, da bi iz pravice do odbitka v celoti izključila DDV na blago in storitve, ki jih davčni zavezanec več kot 90-odstotno uporablja za zasebne ali neposlovne namene, vključno z negospodarskimi dejavnostmi (v nadaljnjem besedilu: posebni ukrep) . Zahtevi je priložila poročilo o uporabi posebnega ukrepa, ki vsebuje pregled stopnje razdelitve, ki se uporabi za pravico do odbitka DDV, kakor je določeno v členu 2 Odločbe 2009/791/ES.

(6) Na podlagi člena 395(2), drugi pododstavek, Direktive 2006/112/ES je Komisija z dopisi z dne 17. marca 2021 zahtevo Nemčije posredovala drugim državam članicam. Z dopisom z dne 18. marca 2021 je Komisija uradno obvestila Nemčijo, da ima vse informacije, potrebne za presojo zahteve.

(7) Po mnenju Nemčije se je posebni ukrep izkazal za zelo učinkovitega pri poenostavitvi pobiranja DDV ter preprečevanju davčnih utaj in izogibanja davkom. Posebni ukrep zmanjšuje upravno breme za podjetja in davčne uprave, saj ni potrebe po kakršnem koli spremljanju poznejše rabe blaga in storitev, za katere se odbitek ni uveljavljal v času njihovega nakupa. Nemčiji bi bilo zato treba dovoliti, da posebni ukrep uporablja še naprej za nadaljnje omejeno obdobje do 31. decembra 2024.

(8) Če bi Nemčija menila, da je potrebno podaljšanje po letu 2024, bi morala Komisiji do 31. marca 2024 predložiti zahtevo, skupaj s poročilom o uporabi posebnega ukrepa, ki bi moralo vsebovati pregled uporabljene stopnje razdelitve.

(9) Posebni ukrep ne bo imel negativnega učinka na lastna sredstva Unije iz naslova DDV.

(10) Odločbo 2009/791/ES bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Odločba 2009/791/ES se spremeni:

(1) naslov se nadomesti z naslednjim:

„Odločba Sveta 2009/791/ES z dne 20. oktobra 2009 o dovoljenju Zvezni republiki Nemčiji, da še naprej uporablja ukrep z odstopanjem od členov 168 in 168a Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost“;

(2) člen 2 se nadomesti z naslednjim:

„*Člen 2*

Ta odločba preneha veljati 31. decembra 2024.

Vsaka zahteva za podaljšanje ukrepa odstopanja iz te odločbe se Komisiji predloži do 31. marca 2024.

Takšni zahtevi se priloži poročilo o uporabi tega ukrepa, ki vsebuje pregled stopnje razdelitve, ki se uporabi za pravico do odbitka DDV na podlagi te odločbe.“

Člen 2

Ta sklep začne učinkovati z dnem uradne obvestitve.

Člen 3

Ta sklep je naslovljen na Zvezno republiko Nemčijo.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

IZVEDBENI SKLEP SVETA (EU) 2021/1777

z dne 5. oktobra 2021

o dovoljenju Italiji, da uporabi nižje stopnje obdavčevanja za plinsko olje za ogrevanje in električno energijo, dobavljeno v občini Campione d'Italia

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2003/96/ES z dne 27. oktobra 2003 o prestrukturiranju okvira Skupnosti za obdavčitev energentov in električne energije ([1]) ter zlasti člena 19 Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Italija je z dopisom z dne 7. avgusta 2020 zaprosila za dovoljenje za uporabo nižjih stopenj obdavčevanja za plinsko olje za ogrevanje in za električno energijo, dobavljeno na ozemlju občine Campione d'Italia na podlagi člena 19 Direktive 2003/96/ES za obdobje od 1. januarja 2021 do 31. decembra 2026. Italija ja 19. januarja 2021 predložila dodatne informacije in pojasnila v podporo prošnji.

(2) Občina Campione d'Italia je italijanska enklava v Švici z zelo majhnim geografskim obsegom in majhno populacijo. Območje je gorato, kar omejuje razvoj mest, industrijske dejavnosti in njegovo splošno dostopnost. Glede na geografsko lego, slabe podnebne razmere in to, da ni dostopa do omrežja zemeljskega plina, so stroški dobave energentov v občini Campione d'Italia visoki, ne glede na to, ali se dobavljajo iz Švice ali Italije. Poleg tega so se zaradi vstopa občine Campione d'Italia v carinsko območje Unije 1. januarja 2020 povečali energetski stroški za gospodinjstva in podjetja. Hkrati se občina Campione d'Italia spopada s hudo gospodarsko krizo, ki jo je pandemija COVID-19 še zaostrila.

(3) Da bi znižali visoke energetske stroške v Campione d'Italia bi bilo treba zmanjšati obdavčevanje nekaterih energentov.

(4) Komisija je proučila zaprošeni ukrep in ugotovila, da ne izkrivlja konkurence in ne ovira pravilnega delovanja notranjega trga, tako da se ne šteje za nezdružljivega s politiko Unije na področju okolja, energije in prometa. Nižji stopnji obdavčevanja za plinsko olje in električno energijo bi ostali enaki najnižjim stopnjam obdavčitve iz Direktive 2003/96/ES ali višji od njih in bi delno izravnali višje energetske stroške v občini Campione d'Italia. Znižanje dajatev ni kumulativno z drugimi vrstami znižanja dajatev.

(5) Italiji bi bilo zato treba dovoliti, da uporabi nižji stopnji obdavčitve za plinsko olje za ogrevanje in električno energijo, dobavljene v občini Campione d'Italia.

(6) Da bi zagotovili uresničitev ciljev ukrepa odstopanja, zlasti glede preprečevanja negativnih učinkov trenutnih gospodarskih, socialnih in geografskih okoliščin občine Campione d'Italia ter glede zagotavljanja enakih konkurenčnih pogojev z ublažitvijo visokih stroškov energije, je primerno, da se ta sklep uporablja od 1. januarja 2021. Z določitvijo datuma začetka uporabe, ki je pred datumom začetka veljavnosti ukrepa odstopanja, se spoštujejo legitimna pričakovanja udeležencev na trgu in posameznikov, saj ukrep odstopanja ne posega v njihove pravice in obveznosti.

([1]) UL L 283, 31.10.2003, str. 51.

(7) Vsako dovoljenje, odobreno na podlagi člena 19(2) Direktive 2003/96/ES, je strogo časovno omejeno. Da bi se občini Campione d'Italia zagotovila zadostna stopnja gotovosti, bi bilo treba dovoljenje dodeliti za obdobje šestih let. Če Svet na podlagi člena 113 Pogodbe o delovanju Evropske unije uvede spremenjeni splošni sistem za obdavčitev energentov in to dovoljenje glede na te spremembe ni več ustrezno, je treba za ohranitev nadaljnjega splošnega razvoja obstoječega pravnega okvira predvideti možnost, da to dovoljenje preneha veljati na dan začetka veljavnosti zadevnih splošnih pravil.

(8) Ta sklep ne posega v uporabo pravil Unije o državni pomoči –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Italiji se dovoli, da uporabi nižji stopnji obdavčenja za plinsko olje za ogrevanje in za električno energijo, dobavljene v občini Campione d'Italia, pod pogojem, da se upoštevajo najnižje ravni obdavčitve iz členov 9 in 10 Direktive 2003/96/ES.

Člen 2

Ta sklep se uporablja od 1. januarja 2021 do 31. decembra 2026.

Če Svet na podlagi člena 113 ali druge relevantne določbe Pogodbe o delovanju Evropske unije uvede spremenjeni splošni sistem za obdavčitev energentov in dovoljenje iz člena 1 tega sklepa glede na te spremembe ni več ustrezno, ta sklep preneha veljati na dan začetka veljavnosti zadevnih splošnih pravil.

Člen 3

Ta sklep je naslovljen na Italijansko republiko.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

IZVEDBENI SKLEP SVETA (EU) 2021/1778

z dne 5. oktobra 2021

o dovoljenju Zvezni republiki Nemčiji, da uporabi posebni ukrep, ki odstopa od člena 193 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost ([1]) in zlasti člena 395(1), prvi pododstavek, Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Člen 193 Direktive 2006/112/ES določa, da je davčni zavezanec, ki dobavlja blago ali opravlja storitve, po splošnem pravilu dolžan plačati davek na dodano vrednost (DDV) davčnim organom.

(2) Zvezna republika Nemčija (v nadaljnjem besedilu: Nemčija) je z dopisom, ki ga je Komisija evidentirala 15. marca 2021, Komisiji predložila zahtevo za dovoljenje, da uporabi posebni ukrep, ki odstopa od člena 193 Direktive 2006/112/ES, kar zadeva osebe, ki so dolžne plačati DDV, v primeru prenosa pravic do emisije, s katerimi se trguje v nacionalnem sistemu trgovanja na podlagi zakona o trgovanju z emisijami iz goriv („Gesetz über einen nationalen Zertifikatehandel für Brennstoffemissionen“ – BEHG) z dne 12. decembra 2019 (v nadaljnjem besedilu: zahteva).

(3) Na podlagi člena 395(2), drugi pododstavek, Direktive 2006/112/ES je Komisija z dopisi z dne 7. aprila 2021 zahtevo posredovala drugim državam članicam, z dopisom z dne 8. aprila 2021 pa je uradno obvestila Nemčijo, da ima na voljo vse informacije, potrebne za presojo zahteve.

(4) Člen 199a(1), točki (a) in (b), Direktive 2006/112/ES državam članicam omogoča, da davčne zavezance, ki prejmejo prenose pravic za emisije toplogrednih plinov, kot so opredeljene v členu 3 Direktive 2003/87/ES Evropskega parlamenta in Sveta ([2]), in prenose drugih enot, ki jih subjekti lahko uporabijo za skladnost z navedeno direktivo, določijo za osebe, ki so dolžne plačati DDV (v nadaljnjem besedilu: mehanizem obrnjene davčne obveznosti). Te določbe so bile vključene v Direktivo 2006/112/ES z Direktivo Sveta 2010/23/EU ([3]), da bi prispevale k boju proti goljufijam na področju DDV. Uporaba mehanizma obrnjene davčne obveznosti za trgovanje z emisijami toplogrednih plinov v skladu s členom 199a(1), točki (a) in (b), Direktive 2006/112/ES je omejena na pravice, s katerimi se trguje v okviru sistema EU za trgovanje z emisijami (EU ETS).

(5) Nemčija je na podlagi BEHG vzpostavila pravni okvir za nacionalni sistem trgovanja z emisijami, ki zajema emisije, ki ne spadajo v EU ETS. Zato člen 199a(1), točki (a) in (b), Direktive 2006/112/ES ne določa pravne podlage za uporabo mehanizma obrnjene davčne obveznosti za trgovanje na podlagi BEHG.

([1]) UL L 347, 11.12.2006, str. 1.

([2]) Direktiva 2003/87/ES Evropskega parlamenta in Sveta z dne 13. oktobra 2003 o vzpostavitvi sistema za trgovanje s pravicami do emisije toplogrednih plinov v Uniji in o spremembi Direktive Sveta 96/61/ES (UL L 275, 25.10.2003, str. 32).

([3]) Direktiva Sveta 2010/23/EU z dne 16. marca 2010 o spremembi Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost v zvezi z neobvezno in začasno uporabo mehanizma obrnjene davčne obveznosti za opravljanje nekaterih storitev, dovzetnih za goljufije (UL L 72, 20.3.2010, str. 1).

(6) Po navedbah Nemčije je trgovanje s pravicami zelo izpostavljeno goljufijam na področju DDV. Trgovanje s pravicami do emisij iz goriv na podlagi BEHG bi bilo mogoče izkoriščati za goljufive namene na enak način kot v okviru EU ETS. Pravice do emisije se lahko izmenjujejo hitro, večkrat zapored in enostavno. Zato organi zelo težko odkrijejo take spremembe lastništva in zagotovijo, da se pobira ustrezen znesek davka. Pridobitelj pravic, ki je davčni zavezanec s pravico do odbitka, bi lahko odbil nastali DDV, ne da bi dobavitelj zaračunani prometni davek plačal davčnim organom. Zlasti udeležba „neplačujočih gospodrskih subjektov“, ki hitro izginejo ali nimajo nobenega premoženja, preprečuje, da bi organi pobrali utajeni davek, kar ima negativen učinek na proračun. Zaradi odprave izgub javnih prihodkov je Nemčija zahtevala dovoljenje za odstopanje od člena 193 Direktive 2006/112/ES, da bi uvedla mehanizem obrnjene davčne obveznosti za prenos pravic do emisije.

(7) Določitev prejemnika, ki je davčni zavezanec, za osebo, ki je dolžna plačati DDV v teh posebnih primerih, bi poenostavila postopek pobiranja DDV in preprečila davčne utaje in izogibanje davkom. Zato bi bilo treba Nemčiji dovoliti, da za prenos pravic do emisije, s katerimi se trguje v nacionalnem sistemu trgovanja na podlagi BEHG, uporabi mehanizem obrnjene davčne obveznosti (v nadaljnjem besedilu: posebni ukrep).

(8) Posebni ukrep bi moral biti časovno omejen. Nemčiji bi bilo zato treba dovoliti, da posebni ukrep uporablja do 31. decembra 2024.

(9) Glede na obseg in novost posebnega ukrepa je pomembno oceniti njegov učinek. Če bi torej Nemčija želela podaljšati posebni ukrep po letu 2024, bi morala Komisiji do 31. marca 2024 predložiti poročilo, ki vsebuje pregled posebnega ukrepa, skupaj z zahtevo za podaljšanje. Navedeno poročilo bi moralo vsebovati oceno učinka posebnega ukrepa na boj proti goljufijam na področju DDV ter število trgovcev in transakcij, na katere posebni ukrep vpliva.

(10) Posebni ukrep ne bo imel negativnega učinka na lastna sredstva Unije iz naslova DDV –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Z odstopanjem od člena 193 Direktive 2006/112/ES se Zvezni republiki Nemčiji dovoli, da določi, da je oseba, ki je dolžna plačati DDV, davčni zavezanec, na katerega se prenesejo pravice do emisije, s katerimi se trguje v nacionalnem sistemu trgovanja na podlagi zakona o trgovanju z emisijami iz goriv („Gesetz über einen nationalen Zertifikatehandel für Brennstoffemissionen“) z dne 12. decembra 2019.

Člen 2

Ta sklep preneha veljati 31. decembra 2024.

Vsaka zahteva za podaljšanje posebnega ukrepa iz tega sklepa se Komisiji predloži do 31. marca 2024, priloži pa se ji poročilo o uporabi tega ukrepa, ki vsebuje oceno učinka ukrepa na boj proti goljufijam na področju DDV ter število trgovcev in transakcij, na katere ukrep vpliva.

Člen 3

Ta sklep začne učinkovati z dnem uradne obvestitve.

Člen 4

Ta sklep je naslovljen na Zvezno republiko Nemčijo.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

IZVEDBENI SKLEP SVETA (EU) 2021/1779

z dne 5. oktobra 2021

o spremembi Izvedbenega sklepa 2009/1013/EU o dovoljenju Republiki Avstriji, da še naprej uporablja ukrep, ki odstopa od člena 168 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost ([1]) in zlasti člena 395(1), prvi pododstavek, Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Z Izvedbenim sklepom Sveta 2009/1013/EU ([2]) je bilo Republiki Avstriji (v nadaljnjem besedilu: Avstrija) dovoljeno, da uporablja posebni ukrep, ki odstopa od Direktive 2006/112/ES (v nadaljnjem besedilu: posebni ukrep). Po zaporednih podaljšanjih navedeno dovoljenje preneha veljati 31. decembra 2021.

(2) Z Direktivo Sveta 2009/162/EU ([3]) se je v Direktivo 2006/112/ES vstavil člen 168a, da bi se odbitek omejil na delež dejanske uporabe za poslovne namene in se tako učinkoviteje uporabilo načelo, po katerem odbitek nastane le, če se zadevno blago in storitve uporabljajo za poslovne namene davčnega zavezanca. Člen 1 Izvedbenega sklepa 2009/1013/EU se je spremenil, da vključuje sklic na člen 168a Direktive 2006/112/ES. Zato se mora naslov Izvedbenega sklepa 2009/1013/EU sklicevati tudi na člen 168a Direktive 2006/112/ES.

(3) Posebni ukrep odstopa od členov 168 in 168a Direktive 2006/112/ES, ki urejata pravico davčnih zavezancev do odbitka davka na dodano vrednost (DDV), obračunanega pri dobavi blaga in storitev, prejetih za namene njihovih obdavčenih transakcij. Namen posebnega ukrepa je, da se DDV na blago in storitve izvzame iz pravice do odbitka, kadar davčni zavezanec to blago in storitve uporablja več kot 90-odstotno za zasebne namene ali za namene svojih zaposlenih ali na splošno za neposlovne namene ali negospodarske dejavnosti.

(4) Cilj posebnega ukrepa je poenostaviti postopek obračunavanja in pobiranja DDV. Ukrep le v zanemarljivem obsegu vpliva na znesek dolgovanega davka pri končni potrošnji.

(5) Z dopisom, ki ga je Komisija evidentirala 19. marca 2021, je Avstrija zahtevala dovoljenje za nadaljnjo uporabo posebnega ukrepa (v nadaljnjem besedilu: zahteva).

(6) Na podlagi člena 395(2), drugi pododstavek, Direktive 2006/112/ES je Komisija z dopisom z dne 7. aprila 2021 zahtevo posredovala drugim državam članicam. Komisija je z dopisom z dne 8. aprila 2021 Avstrijo obvestila, da ima na voljo vse informacije, potrebne za presojo zahteve.

(7) Po mnenju Avstrije se je posebni ukrep izkazal za zelo učinkovitega pri poenostavitvi pobiranja DDV ter preprečevanju davčnih utaj in izogibanja davkom. Ukrep zmanjšuje upravno breme za podjetja in davčne uprave, saj ni potrebe po kakršnem koli spremljanju poznejše rabe blaga in storitev, za katere se odbitek ni uveljavljal v času njihovega nakupa. Avstriji bi bilo zato treba dovoliti, da posebni ukrep uporablja še naprej za nadaljnje omejeno obdobje do 31. decembra 2024.

([1]) UL L 347, 11.12.2006, str. 1.

([2]) Izvedbeni sklep Sveta 2009/1013/EU z dne 22. decembra 2009 o dovoljenju Republiki Avstriji, da še naprej uporablja ukrep, ki odstopa od člena 168 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 348, 29.12.2009, str. 21).

([3]) Direktiva Sveta 2009/162/EU z dne 22. decembra 2009 o spremembi nekaterih določb Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 10, 15.1.2010, str. 14).

(8) Če bo Avstrija menila, da je potrebno podaljšanje po letu 2024, bi morala Komisiji do 31. marca 2024 predložiti zahtevo, skupaj s poročilom o uporabi posebnega ukrepa, ki bi moralo vsebovati pregled uporabljene stopnje razdelitve.

(9) Posebni ukrep ne bo imel negativnega učinka na lastna sredstva Unije iz DDV.

(10) Izvedbeni sklep 2009/1013/EU bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Izvedbeni sklep 2009/1013/EU se spremeni:

(1) naslov se nadomesti z naslednjim:

„Izvedbeni sklep Sveta 2009/1013/EU z dne 22. decembra 2009 o dovoljenju Republiki Avstriji, da še naprej uporablja ukrep, ki odstopa od členov 168 in 168a Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost“;

(2) člena 1 in 2 se nadomestita:

„Člen 1

Z odstopanjem od členov 168 in 168a Direktive 2006/112/ES se Republiki Avstriji dovoli, da davek na dodano vrednost (DDV) na blago in storitve v celoti izključi iz pravice do odbitka DDV, kadar se zadevno blago in storitve uporabljajo več kot 90-odstotno za zasebne namene davčnega zavezanca ali njegovih zaposlenih ali za neposlovne namene ali negospodarske dejavnosti na splošno.

Člen 2

Ta sklep preneha veljati 31. decembra 2024.

Vsaka zahteva za podaljšanje ukrepa odstopanja iz tega sklepa se Komisiji predloži do 31. marca 2024.

Takšni zahtevi se priloži poročilo o uporabi tega ukrepa, ki vsebuje pregled stopnje razdelitve, ki se uporabi za pravico do odbitka DDV na podlagi tega sklepa.“

Člen 2

Ta sklep začne učinkovati z dnem uradne obvestitve.

Člen 3

Ta sklep je naslovljen na Republiko Avstrijo.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

IZVEDBENI SKLEP SVETA (EU) 2021/1780

z dne 5. oktobra 2021

o spremembi Odločbe 2009/790/ES o dovoljenju Republiki Poljski, da uporabi ukrep z odstopanjem od člena 287 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Direktive Sveta 2006/112/ES z dne 28. novembra 2006 o skupnem sistemu davka na dodano vrednost ([1]) in zlasti člena 395(1), prvi pododstavek, Direktive,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Na podlagi člena 287, točka 14, Direktive 2006/112/ES lahko Republika Poljska (v nadaljnjem besedilu: Poljska) oprosti plačila davka na dodano vrednost (DDV) tiste davčne zavezance, katerih letni promet ne presega 10 000 EUR v protivrednosti v nacionalni valuti po menjalnem tečaju na dan njenega pristopa.

(2) Z Odločbo Sveta 2009/790/ES ([2]) se Poljski dovoli, da uvede posebni ukrep, ki odstopa od člena 287 Direktive 2006/112/ES, da lahko oprosti plačila DDV davčne zavezance, katerih letni promet ne presega 40 000 EUR v protivrednosti v nacionalni valuti (v nadaljnjem besedilu: ukrep odstopanja).

(3) Z Izvedbenim sklepom Sveta (EU) 2018/1919 ([3]) se je Poljski dovolila nadaljnja uporaba ukrepa odstopanja, in sicer do 31. decembra 2021 ali do začetka veljavnosti direktive o spremembi določb členov 281 do 294 Direktive 2006/112/ES, pri čemer se upošteva zgodnejši datum.

(4) Poljska je z dopisom, ki ga je Komisija evidentirala 1. marca 2021, Komisiji predložila zahtevo za dovoljenje, da še naprej uporablja ukrep odstopanja, in sicer do 31. decembra 2024 (v nadaljnjem besedilu: zahteva).

(5) Na podlagi člena 395(2), drugi pododstavek, Direktive 2006/112/ES je Komisija z dopisom z dne 25. marca 2021 zahtevo Poljske posredovala drugim državam članicam, razen Cipra, z dopisom z dne 26. marca 2021 pa Cipru. Komisija je z dopisom z dne 29. marca 2021 Poljsko uradno obvestila, da ima vse informacije, potrebne za presojo zahteve.

(6) Ukrep odstopanja je v skladu s cilji sporočila Komisije z dne 25. junija 2008 z naslovom „Najprej pomisli na male‘ – ‚Akt za mala podjetja‘ za Evropo“.

(7) Glede na informacije, ki jih je predložila Poljska, bo imel ukrep odstopanja zanemarljiv učinek na skupni znesek davčnih prihodkov Poljske, pobranih na ravni končne potrošnje. Davčni zavezanci bodo še vedno imeli možnost izbrati splošno ureditev glede DDV.

(8) Po začetku veljavnosti Uredbe Sveta (EU, Euratom) 2021/769 ([4]), Poljska ne bo izračunavala nadomestil od poročila o osnovi za lastna sredstva iz naslova DDV za proračunsko leto 2021 dalje.

([1]) UL L 347, 11.12.2006, str. 1.

([2]) Odločba Sveta 2009/790/ES z dne 20. oktobra 2009 o dovoljenju Republiki Poljski, da uporabi ukrep z odstopanjem od člena 287 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 283, 30.10.2009, str. 53).

([3]) Izvedbeni sklep Sveta (EU) 2018/1919 z dne 4. decembra 2018 o spremembi Odločbe 2009/790/ES o dovoljenju Republiki Poljski, da uporabi ukrep z odstopanjem od člena 287 Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost (UL L 311, 7.12.2018, str. 32).

([4]) Uredba Sveta (EU, Euratom) 2021/769 z dne 30. aprila 2021 o spremembi Uredbe (EGS, Euratom) št. 1553/89 o dokončni enotni ureditvi zbiranja lastnih sredstev, pridobljenih iz davka na dodano vrednost (UL L 165, 11.5.2021. str. 9)

(9) Ker bi lahko ukrep odstopanja pozitivno vplival na poenostavitev obveznosti v zvezi z DDV z zmanjšanjem upravnega bremena in stroškov za mala podjetja, bi bilo treba Poljski dovoliti, da ukrep odstopanja uporablja še za nadaljnje obdobje.

(10) Direktiva Sveta (EU) 2020/285 ([5]) je spremenila člene 281 do 294 Direktive 2006/112/ES glede posebne ureditve za mala podjetja s čimer so določena nova pravila za mala podjetja, vključno z najvišjim pragom države članice za letni promet v višini 85 000 EUR ali protivrednosti v nacionalni valuti.

(11) Dovoljenje za uporabo ukrepa odstopanja bi moralo biti časovno omejeno. Rok bi moral zadostovati za oceno učinkovitosti in ustreznosti praga. Poleg tega se z Direktivo (EU) 2020/285 od držav članic zahteva da do 31. decembra 2024 sprejmejo in objavijo zakone in druge predpise, potrebne za uskladitev s členom 1 navedene direktive, in jih uporabljajo od 1. januarja 2025. Zato bi bilo primerno dovoliti Poljski, da ukrep odstopanja uporablja do 31. decembra 2024.

(12) Odločbo 2009/790/ES bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Člen 2 Odločbe 2009/790/ES se nadomesti z naslednjim:

„*Člen 2*

Ta odločba se uporablja od 1. januarja 2010 do 31. decembra 2024.“

Člen 2

Ta sklep začne učinkovati z dnem uradne obvestitve.

Člen 3

Ta sklep je naslovljen na Republiko Poljsko.

V Luxembourgu, 5. oktobra 2021

Za Svet
predsednik
A. ŠIRCELJ

([5]) Direktiva Sveta (EU) 2020/285 z dne 18. februarja 2020 o spremembi Direktive 2006/112/ES o skupnem sistemu davka na dodano vrednost glede posebne ureditve za mala podjetja in Uredbe (EU) št. 904/2010 glede upravnega sodelovanja in izmenjave informacij za namene spremljanja pravilne uporabe posebne ureditve za mala podjetja (UL L 62, 2.3.2020, str. 13).

IZVEDBENI SKLEP SVETA (EU) 2021/1781

z dne 7. oktobra 2021

o začasni opustitvi uporabe nekaterih določb Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta v zvezi z Gambijo

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (ES) št. 810/2009 Evropskega parlamenta in Sveta z dne 13. julija 2009 o vizumskem zakoniku Skupnosti (Vizumski zakonik) ([1]) in zlasti člena 25a(5), točka (a), Uredbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju naslednjega:

(1) Konec februarja 2019 so se gambijski organi enostransko odločili, da uvedejo moratorij na vse operacije prisilnega vračanja, zaradi česar je bilo v večini leta 2019 preprečeno učinkovito vračanje. Po odpravi moratorija januarja 2020 se države članice soočajo s ponavljajočimi se ovirami, ki jih Gambija postavlja pri organizaciji in izvajanju operacij vračanja. Nepredvidljive ravni sodelovanja Gambije so tudi ovirale vse faze postopka vračanja, tudi kadar so se uporabljale obstoječe dobre prakse in druge operativne ureditve, o katerih sta se predhodno dogovorili Unija in Gambija. Gambijski organi so 6. aprila 2021 sporočili, da država do nadaljnjega ne more sprejemati oseb v postopku vračanja in nato junija 2021 potrdili obstoj „moratorija na prisilno vračanje ali repatriacijo do časa po decembrskih volitvah“.

(2) Komisija je od leta 2019 sprejela ukrepe za izboljšanje ravni sodelovanja Gambije pri ponovnem sprejemu nezakonito prebivajočih državljanov tretjih držav. Ti ukrepi so obsegali več srečanj z gambijskimi organi, tako na tehnični kot tudi na politični ravni, z namenom iskanja obojestransko sprejemljivih rešitev ter dogovora o nadaljnjih projektih podpore v korist Gambije. Vzporedno so potekale izmenjave na visoki ravni med Komisijo in Gambijo. Ponovni sprejem je bil z Gambijo izpostavljen tudi v okviru drugih srečanj, ki so jih organizirale ESZD.

(3) Ob upoštevanju ukrepov, ki jih je Komisija doslej sprejela za izboljšanje ravni sodelovanja, in splošnih odnosov Unije z Gambijo se šteje, da sodelovanje Gambije z Unijo na področju ponovnega sprejema ni zadostno in da je zato potrebno ukrepanje Unije.

(4) Uporabo nekaterih določb Uredbe (ES) št. 810/2009 bi bilo zato treba začasno opustiti za državljane Gambije, za katere v skladu z Uredbo (EU) 2018/1806 Evropskega parlamenta in Sveta velja vizumska obveznost ([2]). To velja zato, da bi se gambijske organe spodbudilo k sprejetju potrebnih ukrepov za izboljšanje sodelovanja na področju ponovnega sprejema.

(5) Določbe, ki se začasno opustijo, so v členu 25a(5), točka (a), vizumskega zakonika: začasna opustitev možnosti opustitve zahtev v zvezi z dokumentarnimi dokazili, ki jih morajo predložiti prosilci za vizum, omenjene v členu 14(6), začasna opustitev splošnega obdobja obravnave 15 koledarskih dni iz člena 23(1) (kar posledično izključuje tudi uporabo pravila o podaljšanju tega obdobja do največ 45 dni v posameznih primerih), začasna opustitev izdajanja vizumov za večkratni vstop v skladu s členom 24(2) in (2c) ter začasna opustitev možnosti oprostitve plačila vizumske takse za imetnike diplomatskih in službenih potnih listov v skladu s členom 16(5), točka (b).

([1]) UL L 243, 15.9.2009, str. 1.

([2]) Uredba (EU) 2018/1806 Evropskega parlamenta in Sveta z dne 14. novembra 2018 o seznamu tretjih držav, katerih državljani morajo pri prehodu zunanjih meja imeti vizume, in držav, katerih državljani so izvzeti iz te obveznosti (UL L 303, 28.11.2018, str. 39).

(6) Člen 21(1) Pogodbe o delovanju Evropske unije (PDEU) določa, da ima vsak državljan Unije pravico do prostega gibanja in prebivanja na ozemlju držav članic ob upoštevanju omejitev in pogojev, določenih s Pogodbama in ukrepi, ki so bili sprejeti za njuno uveljavitev. Te omejitve in pogoje uveljavlja Direktiva 2004/38/ES Evropskega parlamenta in Sveta ([3]). Ta sklep ne vpliva na uporabo navedene direktive, ki pravico do prostega gibanja razširja na družinske člane, neodvisno od njihovega državljanstva, ki državljana Unije spremljajo ali se mu pridružijo. Ta sklep se torej ne uporablja za družinske člane državljana Unije, za katere se uporablja Direktiva 2004/38/ES, ali za družinske člane državljana tretje države, ki na podlagi sporazuma med Unijo in njenimi državami članicami na eni strani ter tretjo državo na drugi strani uživa pravico do prostega gibanja, enakovredno pravici državljanov Unije.

(7) Ukrepi iz tega sklepa ne bi smeli posegati v obveznosti držav članic po mednarodnem pravu kot držav gostiteljic mednarodnih medvladnih organizacij ali mednarodnih konferenc, ki jih skličejo mednarodne medvladne organizacije, ki jih gostijo države članice. Zato se začasna opustitev ne bi smela uporabljati za državljane Gambije, ki zaprosijo za vizum, če je to potrebno, da države članice izpolnijo svoje obveznosti kot države gostiteljice takih organizacij ali konferenc.

(8) V skladu s členoma 1 in 2 Protokola (št. 22) o stališču Danske, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, Danska ne sodeluje pri sprejetju tega sklepa, ki zato zanjo ni zavezujoč in se v njej ne uporablja. Ker ta sklep nadgrajuje schengenski pravni red, se Danska v skladu s členom 4 navedenega protokola v šestih mesecih od dne, ko Svet sprejme ta sklep, odloči, ali ga bo prenesla v svoje nacionalno pravo.

(9) Ta sklep predstavlja razvoj določb schengenskega pravnega reda, pri katerih Irska v skladu s Sklepom Sveta 2002/192/ES ne sodeluje ([4]); Irska torej ne sodeluje pri sprejetju tega sklepa, ki zato zanjo ni zavezujoč in se v njej ne uporablja.

(10) Ta sklep za Islandijo in Norveško predstavlja razvoj določb schengenskega pravnega reda v smislu Sporazuma med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško o pridružitvi obeh k izvajanju, uporabi in razvoju schengenskega pravnega reda ([5]), ki spadajo na področje iz člena 1, točka B, Sklepa Sveta 1999/437/ES ([6]).

(11) Ta sklep za Švico predstavlja razvoj določb schengenskega pravnega reda v smislu Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda ([7]), ki spadajo na področje iz člena 1, točka B, Sklepa 1999/437/ES v povezavi s členom 3 Sklepa Sveta 2008/146/ES ([8]).

([3]) Direktiva Evropskega parlamenta in Sveta 2004/38/ES z dne 29. aprila 2004 o pravici državljanov Unije in njihovih družinskih članov do prostega gibanja in prebivanja na ozemlju držav članic, ki spreminja Uredbo (EGS) št. 1612/68 in razveljavlja Direktive 64/221/EGS, 68/360/EGS, 72/194/EGS, 73/148/EGS, 75/34/EGS, 75/35/EGS, 90/364/EGS, 90/365/EGS in 93/96/EGS (UL L 158, 30.4.2004, str. 77).

([4]) Sklep Sveta 2002/192/ES z dne 28. februarja 2002 o prošnji Irske, da sodeluje pri izvajanju nekaterih določb schengenskega pravnega reda (UL L 64, 7.3.2002, str. 20).

([5]) UL L 176, 10.7.1999, str. 36.

([6]) Sklep Sveta 1999/437/ES z dne 17. maja 1999 o nekaterih izvedbenih predpisih za uporabo Sporazuma, sklenjenega med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško, v zvezi s pridružitvijo teh dveh držav k izvajanju, uporabi in razvoju schengenskega pravnega reda (UL L 176, 10.7.1999, str. 31).

([7]) UL L 53, 27.2.2008, str. 52.

([8]) Sklep Sveta 2008/146/ES z dne 28. januarja 2008 o sklenitvi Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda v imenu Evropske skupnosti (UL L 53, 27.2.2008, str. 1).

(12) Ta sklep za Lihtenštajn predstavlja razvoj določb schengenskega pravnega reda v smislu Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda ([9]), ki spadajo na področje iz člena 1, točka B, Sklepa 1999/437/ES v povezavi s členom 3 Sklepa Sveta 2011/350/EU ([10]).

(13) Ta sklep predstavlja akt, ki temelji na schengenskem pravnem redu oziroma je z njim kako drugače povezan v smislu člena 3(2) Akta o pristopu iz leta 2003 in člena 4(2) Akta o pristopu iz leta 2005 ter člena 4(2) Akta o pristopu iz leta 2011 –

SPREJEL NASLEDNJI SKLEP:

Člen 1

Področje uporabe

1. Ta sklep se uporablja za državljane Gambije, za katere v skladu z Uredbo (EU) 2018/1806 velja vizumska obveznost.

2. Ne uporablja se za državljane Gambije, ki so v skladu s členom 4 ali 6 Uredbe (EU) 2018/1806 izvzeti iz vizumske obveznosti.

3. Ta sklep se ne uporablja za državljane Gambije, ki zaprosijo za vizum in so družinski člani državljana Unije, za katerega se uporablja Direktiva 2004/38/ES, ali družinski člani državljana tretje države, ki na podlagi sporazuma med Unijo in njenimi državami članicami na eni strani ter tretjo državo na drugi strani uživa pravico do prostega gibanja, enakovredno pravici državljanov Unije.

4. Ta sklep se uporablja brez poseganja v primere, ko državo članico zavezujejo mednarodnopravne obveznosti, in sicer:

(a) ko je država gostiteljica mednarodne medvladne organizacije;

(b) ko je država gostiteljica mednarodne konference, sklicane s strani Združenih narodov ali pod pokroviteljstvom Združenih narodov ali drugih mednarodnih medvladnih organizacij, ki jih gosti država članica;

(c) v skladu z večstranskim sporazumom o privilegijih in imunitetah ali

(d) na podlagi Lateranske pogodbe, ki sta jo leta 1929 sklenila Sveti sedež (Vatikanska mestna država) in Italija, kot je bila nazadnje spremenjena.

Člen 2

Začasna opustitev uporabe nekaterih določb Uredbe (ES) št. 810/2009

Začasno se opusti uporaba naslednjih določb Uredbe (ES) št. 810/2009:

(a) člena 14(6);

(b) člena 16(5), točka (b);

([9]) UL L 160, 18.6.2011, str. 21.

([10]) Sklep Sveta 2011/350/EU z dne 7. marca 2011 o sklenitvi Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda, v zvezi z odpravo kontrol na notranjih mejah in prostim gibanjem oseb, v imenu Evropske unije (UL L 160, 18.6.2011, str. 19).

(c) člena 23(1);

(d) člena 24(2) in (2c).

Člen 3

Naslovniki

Ta sklep je naslovljen na Kraljevino Belgijo, Republiko Bolgarijo, Češko republiko, Zvezno republiko Nemčijo, Republiko Estonijo, Helensko republiko, Kraljevino Španijo, Francosko republiko, Republiko Hrvaško, Italijansko republiko, Republiko Ciper, Republiko Latvijo, Republiko Litvo, Veliko vojvodstvo Luksemburg, Madžarsko, Republiko Malto, Kraljevino Nizozemsko, Republiko Avstrijo, Republiko Poljsko, Portugalsko republiko, Romunijo, Republiko Slovenijo, Slovaško republiko, Republiko Finsko in Kraljevino Švedsko.

V Luxembourgu, 7. oktobra 2021

Za Svet
predsednik
M. DIKAUČIČ

PRIPOROČILA

PRIPOROČILO SVETA (EU) 2021/1782

z dne 8. oktobra 2021

o spremembi Priporočila (EU) 2020/912 o začasni omejitvi nenujnih potovanj v EU in morebitni odpravi te omejitve

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 77(2)(b) in (e) ter prvega in drugega stavka člena 292 Pogodbe,

ob upoštevanju naslednjega:

(1) Svet je 30. junija 2020 sprejel Priporočilo o začasni omejitvi nenujnih potovanj v EU in morebitni odpravi te omejitve ([1]) (v nadaljnjem besedilu: Priporočilo Sveta).

(2) Svet je odtlej sprejel priporočila (EU) 2020/1052 ([2]), (EU) 2020/1144 ([3]), (EU) 2020/1186 ([4]), (EU) 2020/1551 ([5]), (EU) 2020/2169 ([6]), (EU) 2021/89 ([7]), (EU) 2021/132 ([8]), (EU) 2021/767 ([9]), (EU) 2021/892 ([10]), (EU) 2021/992 ([11]), (EU) 2021/1085 ([12]), (EU) 2021/1170 ([13]), (EU) 2021/1346 ([14]), (EU) 2021/1459 ([15]) in (EU) 2021/1712 ([16]) o spremembi Priporočila Sveta (EU) 2020/912 o začasni omejitvi nenujnih potovanj v EU in morebitni odpravi te omejitve.

(3) Svet je 20. maja 2021 sprejel Priporočilo (EU) 2021/816 o spremembi Priporočila Sveta (EU) 2020/912 o začasni omejitvi nenujnih potovanj v EU in morebitni odpravi te omejitve ([17]), da bi posodobil merila, ki se uporabljajo za oceno, ali so nenujna potovanja iz tretjih držav varna in bi morala biti dovoljena.

(4) V Priporočilu Sveta je določeno, da bi morale države članice s 1. julijem 2020 začeti usklajeno in postopoma odpravljati začasno omejitev nenujnih potovanj v EU za rezidente tretjih držav iz Priloge I k Priporočilu Sveta. Svet bi moral vsaka dva tedna pregledati in po potrebi posodobiti seznam tretjih držav iz Priloge I po tesnem posvetovanju s Komisijo ter ustreznimi agencijami in službami EU ter po splošni oceni na podlagi metodologije, meril in informacij iz Priporočila Sveta.

([1]) UL L 208 I, 1.7.2020, str. 1.
([2]) UL L 230, 17.7.2020, str. 26.
([3]) UL L 248, 31.7.2020, str. 26.
([4]) UL L 261, 11.8.2020, str. 83.
([5]) UL L 354, 26.10.2020, str. 19.
([6]) UL L 431, 21.12.2020, str. 75.
([7]) UL L 33, 29.1.2021, str. 1.
([8]) UL L 41, 4.2.2021, str. 1.
([9]) UL L 165 I, 11.5.2021, str. 66.
([10]) UL L 198, 4.6.2021, str. 1.
([11]) UL L 221, 21.6.2021, str. 12.
([12]) UL L 235, 2.7.2021, str. 27.
([13]) UL L 255, 16.7.2021, str. 3.
([14]) UL L 306, 31.8.2021, str. 4.
([15]) UL L 320, 10.9.2021, str. 1.
([16]) UL L 341, 24.9.2021, str. 1.
([17]) UL L 182, 21.5.2021, str. 1.

(5) Vse od takrat so v Svetu, v tesnem posvetovanju s Komisijo ter ustreznimi agencijami in službami EU, potekale razprave o pregledu seznama tretjih držav iz Priloge I k Priporočilu Sveta ter o uporabi meril in metodologije iz Priporočila Sveta, kot je bilo spremenjeno s Priporočilom (EU) 2021/816. Na podlagi teh razprav bi bilo treba spremeniti seznam tretjih držav iz Priloge I. Konkretno bi bilo treba na seznam dodati Bahrajn in Združene arabske emirate.

(6) Mejni nadzor ni samo v interesu države članice, na katere zunanjih mejah se opravlja, temveč tudi v interesu vseh držav članic, ki so odpravile nadzor meje na svojih notranjih mejah. Zato bi morale države članice zagotoviti, da bodo ukrepi, sprejeti na zunanjih mejah, usklajeni, s čimer bodo zagotovile, da bo schengensko območje dobro delovalo. Države članice bi morale v ta namen od 8. oktobra 2021 še naprej usklajeno odpravljati začasno omejitev nenujnih potovanj v EU za rezidente tretjih držav, posebna upravna območja *ter druge entitete in teritorialna ozemlja* iz Priloge I k Priporočilu Sveta, kot je spremenjeno s tem priporočilom.

(7) V skladu s členoma 1 in 2 Protokola št. 22 o stališču Danske, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, Danska ne sodeluje pri sprejetju tega priporočila, ki zato zanjo ni zavezujoče in se v njej ne uporablja. Ker to priporočilo nadgrajuje schengenski pravni red, se Danska v skladu s členom 4 navedenega protokola v šestih mesecih od dne, ko Svet sprejme to priporočilo, odloči, ali ga bo prenesla v svoje nacionalno pravo.

(8) To priporočilo predstavlja razvoj določb schengenskega pravnega reda, pri katerih Irska v skladu s Sklepom Sveta 2002/192/ES ([18]) ne sodeluje. Irska torej ne sodeluje pri sprejetju tega priporočila, ki zato zanjo ni zavezujoče in se v njej ne uporablja.

(9) To priporočilo za Islandijo in Norveško predstavlja razvoj določb schengenskega pravnega reda v smislu Sporazuma, sklenjenega med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško, v zvezi s pridružitvijo teh dveh držav k izvajanju, uporabi in razvoju schengenskega pravnega reda, ki spadajo na področje iz člena 1, točka A, Sklepa Sveta 1999/437/ES ([19]).

(10) To priporočilo za Švico predstavlja razvoj določb schengenskega pravnega reda v smislu Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda, ki spadajo na področje iz člena 1, točka A, Sklepa 1999/437/ES ([20]) v povezavi s členom 3 Sklepa Sveta 2008/146/ES ([21]).

(11) To priporočilo za Lihtenštajn predstavlja razvoj določb schengenskega pravnega reda v smislu Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda, ki spadajo na področje iz člena 1, točka A, Sklepa 1999/437/ES ([22]) v povezavi s členom 3 Sklepa 2011/350/EU ([23]) –

([18]) Sklep Sveta 2002/192/ES z dne 28. februarja 2002 o prošnji Irske, da sodeluje pri izvajanju nekaterih določb schengenskega pravnega reda (UL L 64, 7.3.2002, str. 20).
([19]) UL L 176, 10.7.1999, str. 31.
([20]) UL L 53, 27.2.2008, str. 52.
([21]) Sklep Sveta 2008/146/ES z dne 28. januarja 2008 o sklenitvi Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda v imenu Evropske skupnosti (UL L 53, 27.2.2008, str. 1).
([22]) UL L 160, 18.6.2011, str. 21.
([23]) Sklep Sveta 2011/350/EU z dne 7. marca 2011 o sklenitvi Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda, v zvezi z odpravo kontrol na notranjih mejah in prostim gibanjem oseb, v imenu Evropske unije (UL L 160, 18.6.2011, str. 19).

SPREJEL NASLEDNJE PRIPOROČILO:

Priporočilo Sveta (EU) 2020/912 o začasni omejitvi nenujnih potovanj v EU in morebitni odpravi te omejitve, kakor je bilo spremenjeno s priporočili (EU) 2020/1052, (EU) 2020/1144, (EU) 2020/1186, (EU) 2020/1551, (EU) 2020/2169, (EU) 2021/89, (EU) 2021/132, (EU) 2021/767, (EU) 2021/816, (EU) 2021/892, (EU) 2021/992, (EU) 2021/1085, (EU) 2021/1170, (EU) 2021/1346, (EU) 2021/1459 in (EU) 2021/1712, se spremeni:

(1) prvi odstavek točke 1 Priporočila Sveta se nadomesti z naslednjim:

„1. Države članice bi morale z 8. oktobrom 2021 začeti usklajeno in postopoma odpravljati začasno omejitev nenujnih potovanj v EU za rezidente tretjih držav iz Priloge I.“;

(2) Priloga I k Priporočilu se nadomesti z naslednjim:

„„*PRILOGA I*

Tretje države, posebna upravna območja ter druge entitete in teritorialna ozemlja, na rezidente katerih ne bi smela vplivati začasna omejitev nenujnih potovanj v EU na zunanjih mejah:

I. DRŽAVE

1. AVSTRALIJA
2. BAHRAJN
3. KANADA
4. ČILE
5. JORDANIJA
6. KUVAJT
7. NOVA ZELANDIJA
8. KATAR
9. RUANDA
10. SAUDOVA ARABIJA
11. SINGAPUR
12. JUŽNA KOREJA
13. UKRAJINA
14. ZDRUŽENI ARABSKI EMIRATI
15. URUGVAJ
16. KITAJSKA (*)

II. POSEBNA UPRAVNA OBMOČJA LJUDSKE REPUBLIKE KITAJSKE

Posebno upravno območje Hongkong

Posebno upravno območje Macao

III. ENTITETE IN TERITORIALNA OZEMLJA, KI JIH NAJMANJ ENA DRŽAVA ČLANICA NE PRIZNAVA KOT DRŽAVE

Tajvan.

(*) S pridržkom potrditve vzajemnosti.““

V Luxembourgu, 8. oktobra 2021

Za Svet
predsednik
M. DIKAUČIČ

ISSN 1977-0804 (elektronska različica)
ISSN 1725-5155 (tiskana različica)

Urad za publikacije
Evropske unije
L-2985 Luxembourg
LUKSEMBURG

SL