Uradni list
Evropske unije

SL
Serija L

2025/2574

23.12.2025

# IZVEDBENI SKLEP KOMISIJE (EU) 2025/2574

## z dne 19. decembra 2025

## o spremembi Izvedbenega sklepa Komisije (EU) 2021/1772 v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu

*(notificirano pod dokumentarno številko C(2025) 8771)*

**(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]) ter zlasti člena 45(3) Uredbe,

ob upoštevanju naslednjega:

### 1. UVOD

(1) V Izvedbenem sklepu Komisije (EU) 2021/1772 ([2]) je bilo ugotovljeno, da Združeno kraljestvo za namene člena 45 Uredbe (EU) 2016/679 zagotavlja ustrezno raven varstva osebnih podatkov, ki se v okviru področja uporabe navedene uredbe ([3]) prenašajo iz Evropske unije v Združeno kraljestvo.

(2) Komisija je pri sprejemanju Izvedbenega sklepa (EU) 2021/1772 upoštevala, da bi po izteku prehodnega obdobja, določenega v Sporazumu o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo ([4]), ter po prenehanju uporabe začasne določbe iz 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 ([5]) Združeno kraljestvo sprejelo, uporabljalo in izvajalo novo ureditev varstva podatkov, ki se razlikuje od ureditve, ki je veljala, ko ga je zavezovalo pravo Unije.

(3) Ker bi to lahko vključevalo spremembe okvira varstva podatkov, ocenjenega v Izvedbenem sklepu (EU) 2021/1772, ali druge pomembne spremembe, se je zdelo primerno določiti, da se navedeni sklep uporablja štiri leta od začetka veljavnosti. Izvedbeni sklep (EU) 2021/1772 bi moral tako prenehati veljati 27. junija 2025, razen če se njegova veljavnost podaljša po postopku iz člena 93(2) Uredbe (EU) 2016/679.

([1]) UL L 119, 4.5.2016, str. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

([2]) Izvedbeni sklep 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 (UL L 360, 11.10.2021, str. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

([3]) Glej člen 1(1) Izvedbenega sklepa (EU) 2021/1772. V skladu s členom 1(2) navedenega sklepa se ta 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 s točko 4(1) dodatka 2 k zakonu Združenega kraljestva o varstvu podatkov iz leta 2018.

([4]) UL C 384I, 12.11.2019, str. 1.

([5]) UL L 149, 30.4.2021, str. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Za odločitev o morebitnem podaljšanju veljavnosti Izvedbenega sklepa (EU) 2021/1772 mora Komisija oceniti, ali je ugotovitev, da Združeno kraljestvo zagotavlja ustrezno raven varstva osebnih podatkov, še stvarno in pravno utemeljena glede na spremembe, ki so se zgodile od sprejetja Izvedbenega sklepa (EU) 2021/1772 v zvezi z elementi, navedenimi v členu 45(2) Uredbe (EU) 2016/679.

(5) Zlasti je vlada Združenega kraljestva 23. oktobra 2024 v parlamentu Združenega kraljestva predstavila predlog zakona o podatkih (uporaba in dostop) (Data (Use and Access) Bill) ([6]), v katerem je predlagala spremembe splošne uredbe Združenega kraljestva o varstvu podatkov (United Kingdom General Data Protection Regulation, v nadaljnjem besedilu: UK GDPR) in zakona o varstvu podatkov iz leta 2018 (Data Protection Act 2018), ocenjenih v Izvedbenem sklepu (EU) 2021/1772. Komisija je 24. junija 2025 sprejela Izvedbeni sklep (EU) 2025/1226 ([7]), s katerim je bila veljavnost Izvedbenega sklepa (EU) 2021/1772 podaljšana za šest mesecev, in sicer do 27. decembra 2025. Zaradi tega časovno omejenega tehničnega podaljšanja je lahko dokončala oceno ustrezne ravni varstva osebnih podatkov, ki jo zagotavlja Združeno kraljestvo, na podlagi stabilnega pravnega okvira, tj. po zaključku ustreznega zakonodajnega postopka ([8]).

(6) Komisija je od sprejetja Izvedbenega sklepa (EU) 2021/1772 stalno spremljala pomembne spremembe v Združenem kraljestvu ([9]). V skladu z uvodno izjavo 281 Izvedbenega sklepa (EU) 2021/1772 je bila 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 z navedenim sklepom, učinkovitost uveljavljanja pravic posameznikov, vključno z vsem pomembnimi 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. Komisija je pri spremljanju upoštevala med drugim razvoj sodne prakse in nadzor, ki ga izvajajo urad informacijskega pooblaščenca in drugi neodvisni organi.

(7) Komisija na podlagi ocene tega razvoja, vključno s spremembami UK GDPR in zakona o varstvu podatkov iz leta 2018, uvedenimi z zakonom o podatkih (uporaba in dostop), ugotavlja, da Združeno kraljestvo še naprej zagotavlja ustrezno raven varstva osebnih podatkov, ki se v okviru področja uporabe Uredbe (EU) 2016/679 prenašajo iz Evropske unije v Združeno kraljestvo.

(8) Komisija tudi ugotavlja, da glede na spremembe ustreznih določb prava Združenega kraljestva ([10]) izključitev osebnih podatkov, 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 s točko 4(1) dodatka 2 k zakonu Združenega kraljestva o varstvu podatkov, s področja uporabe Izvedbenega sklepa (EU) 2021/1772 ni več upravičena, kot je pojasnjeno v uvodni izjavi 37 tega sklepa.

([6]) Na voljo na povezavi: https://bills.parliament.uk/bills/3825/news.

([7]) Izvedbeni sklep Komisije (EU) 2025/1226 z dne 24. junija 2025 o spremembi Izvedbenega sklepa (EU) 2021/1772 v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu (UL L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) Zakon o podatkih (uporaba in dostop) (Data (Use and Access) Act) je 19. junija 2025 prejel kraljevo privolitev.

([9]) Člen 45(4) Uredbe (EU) 2016/679.

([10]) Sodišče England and Wales Court of Appeal je maja 2021 ugotovilo, da je izjema glede priseljevanja, kot je bila takrat oblikovana v točki 4(1) dodatka 2 k zakonu Združenega kraljestva o varstvu podatkov, nezdružljiva s pravom Združenega kraljestva, saj zakonodajni ukrep ni vseboval posebnih določb, ki bi določale zaščitne ukrepe iz člena 23(2) UK GDPR. Vlada Združenega kraljestva je za izvršitev sodbe revidirala izjemo glede priseljevanja s tem, da je sprejela predpise o zakonu o varstvu podatkov iz leta 2018 (sprememba izjem iz dodatka 2) iz leta 2022 (Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022). Vendar je bila revidirana izjema ponovno izpodbijana, ker ni izpolnjevala vseh zahtev iz člena 23(2) UK GDPR. Sodišče Court of Appeal je v sodbi z dne 11. decembra 2023 revidirano izjemo glede priseljevanja ponovno razglasilo za nezdružljivo s členom 23(2) UK GDPR. Vlada Združenega kraljestva je za izvršitev sodbe nato sprejela predpise o zakonu o varstvu podatkov iz leta 2018 (sprememba izjem iz dodatka 2) iz leta 2024 (Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024), ki so začeli veljati 8. marca 2024.

## 2. POMEMBNE SPREMEMBE V ZVEZI S PRAVILI, KI SE UPORABLJAJO ZA OBDELAVO OSEBNIH PODATKOV

### 2.1 Okvir varstva podatkov v Združenem kraljestvu

(9) Pravni okvir za varstvo osebnih podatkov v Združenem kraljestvu je ob sprejetju Izvedbenega sklepa (EU) 2021/1772 zajemal:

— UK GDPR ([11]), kot je bila vključena v zakonodajo Združenega kraljestva na podlagi zakona iz leta 2018 o izstopu iz Evropske unije (European Union (Withdrawal) Act 2018) ([12]) in spremenjena s predpisi o varstvu podatkov, zasebnosti in elektronskih komunikacijah (spremembe itd., izstop iz EU) iz leta 2019 (v nadaljnjem besedilu: predpisi DPPEC) ([13]),

— zakon o varstvu podatkov iz leta 2018 ([14]), kot je bil spremenjen s predpisi DPPEC.

(10) Čeprav sta oba zakona, ki sta natančno odražala ustrezna pravila, ki se uporabljajo v Evropski uniji, še naprej del zakonodaje Združenega kraljestva o varstvu podatkov, sta od takrat doživela omejene spremembe, iz česar je razvidno, da Združeno kraljestvo ni več zavezano pravu Evropske unije.

(11) Prvič, v zakonu o ohranjenem pravu EU (razveljavitev in reforma) iz leta 2023 (Retained EU Law (Revocation and Reform) Act 2023, v nadaljnjem besedilu: zakon o ohranjenem pravu EU) ([15]) je pojasnjeno, da splošna načela prava EU po koncu leta 2023 niso več del notranjega prava Združenega kraljestva ([16]). Poleg tega sodiščem Združenega kraljestva ni več treba razlagati nespremenjenega poenotenega (unificiranega) prava, prej imenovanega ohranjeno pravo EU, v skladu s splošnimi načeli prava EU, temveč je treba tako pravo razlagati v skladu z notranjim pravom Združenega kraljestva ([17]). Še vedno pa morajo nespremenjeno poenoteno (unificirano) pravo razlagati v skladu z ustrezno sodno prakso Sodišča Evropske unije, izdano pred koncem prehodnega obdobja ([18]), kot je navedeno tudi v uvodni izjavi 13 Izvedbenega sklepa (EU) 2021/1772. Zakon o varstvu podatkov iz leta 2018 je bil spremenjen z zakonom o podatkih (uporaba in dostop), da bi se pojasnil učinek zakona o ohranjenem pravu EU na zakonodajo Združenega kraljestva o varstvu podatkov. Člen 183A(1) zakona o varstvu podatkov iz leta 2018 na primer kot splošno pravilo določa, da se za vsako novo zakonodajo (sprejeto 20. avgusta 2025 ali pozneje), s katero se uvedejo nove naloge ali pooblastila za obdelavo osebnih podatkov, domneva, da zanjo velja zakonodaja Združenega kraljestva o varstvu podatkov. To pomeni, da okvir Združenega kraljestva za varstvo podatkov še naprej prevladuje nad drugo zakonodajo. V skladu s členom 183A(2), točka (b), zakona o varstvu podatkov iz

([11]) Splošna uredba o varstvu podatkov, na voljo na povezavi: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) Z zakonom iz leta 2018 o izstopu iz Evropske unije, na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/16/contents, je bila zakonodaja Unije, ki se je ob koncu prehodnega obdobja v Združenem kraljestvu uporabljala neposredno, vključena v pravo Združenega kraljestva. To ohranjeno pravo EU je vključevalo Uredbo (EU) 2016/679 v celoti, vključno z njenimi uvodnimi izjavami (glej pojasnjevalne opombe k zakonu iz leta 2018 o izstopu iz Evropske unije, točka 83, na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). V skladu z navedenim zakonom so morala sodišča v Združenem kraljestvu nespremenjeno ohranjeno pravo EU razlagati v skladu z ustrezno sodno prakso Sodišča Evropske unije in splošnimi načeli prava Unije, kot so ta učinkovala neposredno pred iztekom prehodnega obdobja (tako imenovana ohranjena sodna praksa EU in ohranjena splošna načela prava EU).

([13]) Predpisi o varstvu podatkov, zasebnosti in elektronskih komunikacijah (spremembe itd., izstop iz EU) iz leta 2019, na voljo na povezavi: https://www.legislation.gov.uk/uksi/2019/419/contents/made, kot so bili spremenjeni s predpisi DPPEC iz leta 2020, na voljo na povezavi: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. Predpisi DPPEC spreminjajo Uredbo (EU) 2016/679, kot je bila vključena v pravo Združenega kraljestva z zakonom iz leta 2018 o izstopu iz Evropske unije (European Union (Withdrawal) Act 2018), zakonom o varstvu podatkov iz leta 2018 in drugo zakonodajo o varstvu podatkov, da ustreza nacionalnemu okviru.

([14]) Zakon o varstvu podatkov iz leta 2018, na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/12/contents. Pred izstopom Združenega kraljestva iz Evropske unije in v prehodnem obdobju so bila v zakonu o varstvu podatkov iz leta 2018 določena nacionalna pravila, kadar je to dovoljevala Uredba (EU) 2016/679, pri čemer je opredeljeval in omejeval uporabo pravil iz Uredbe (EU) 2016/679 ter prenesel Direktivo (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, ELI: http://data.europa.eu/eli/dir/2016/680/oj) v nacionalno zakonodajo.

([15]) Na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Člen 5 zakona iz leta 2018 o izstopu iz Evropske unije, kot je bil spremenjen z zakonom o ohranjenem pravu EU.

([17]) Člen 5(A2) zakona iz leta 2018 o izstopu iz Evropske unije, kot je bil spremenjen z zakonom o ohranjenem pravu EU.

([18]) Člen 6(3) in (7) zakona iz leta 2018 o izstopu iz Evropske unije, kot je bil spremenjen z zakonom o ohranjenem pravu EU.

leta 2018 se ta domneva ne uporabi, če se parlament Združenega kraljestva namerno odloči, da bo tako izrecno določil v zakonodaji, s čimer ohranja parlamentarno suverenost. Poleg tega je v členu 186(2A) zakona o varstvu podatkov iz leta 2018 pojasnjeno, da nad omejitvami pravic posameznikov, na katere se nanašajo osebni podatki, iz člena 186(3) zakona o varstvu podatkov iz leta 2018 ne prevlada člen 186(1) navedenega zakona, ki določa, da predpisi, s katerimi se prepoveduje ali omejuje razkritje informacij, ne prevladajo nad nekaterimi pravicami varstva podatkov. To zagotavlja na primer, da omejitve pravic posameznikov, na katere se nanašajo osebni podatki, ki so določene v zakonu o varstvu podatkov iz leta 2018, same po sebi niso zajete v splošni določbi o „prevladi nad varstvom podatkov“ iz člena 186(1) navedenega zakona.

(12) Drugič, zakonodaja Združenega kraljestva o varstvu podatkov je bila od sprejetja Izvedbenega sklepa (EU) 2021/1772 spremenjena s predpisi o varstvu podatkov (temeljne pravice in svoboščine) (sprememba) iz leta 2023 (Data Protection (Fundamental Rights and Freedoms) (Amendment) Regulations 2023) ([19]). V teh predpisih so sklici na temeljne pravice ali temeljne svoboščine v UK GDPR in zakonu o varstvu podatkov iz leta 2018 (prej opredeljeni tako, da so zajemali temeljne pravice in temeljne svoboščine EU ([20])) opredeljeni kot sklici na pravice iz Evropske konvencije o človekovih pravicah, ki so v notranjem pravu Združenega kraljestva uveljavljene z zakonom o človekovih pravicah iz leta 1998 (Human Rights Act 1998) ([21]). 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 varstvo osebnih podatkov, ki je del te pravice) in pravico do poštenega sojenja ([22]).

(13) Nazadnje, UK GDPR in zakon o varstvu podatkov iz leta 2018 sta doživela ciljne reforme, določene v petem in šestem delu zakona o podatkih (uporaba in dostop). Čeprav področje uporabe zakona o podatkih (uporaba in dostop) krepko presega varstvo osebnih podatkov, omejeno spreminja več vidikov ureditve varstva podatkov, kot so med drugim pravila o obdelavi podatkov za namene znanstvenega raziskovanja, pravne podlage za obdelavo podatkov, pravila v zvezi z načelom omejitve namena in pogoji za avtomatizirano sprejemanje odločitev. Poleg tega zakon o podatkih (uporaba in dostop) spreminja strukturo upravljanja urada informacijskega pooblaščenca. Z izvedbo teh ukrepov bo urad informacijskega pooblaščenca nadomeščen z novim subjektom, tj. informacijsko komisijo. Vloga in funkcije regulativnega organa kot neodvisnega nadzornega organa za varstvo podatkov v Združenem kraljestvu bodo ostale nespremenjene. Zakon uvaja tudi nova izvršilna pooblastila za regulativni organ.

(14) V tem sklepu so ocenjene zakonodajne, regulativne in druge spremembe, pomembne za v Izvedbenem sklepu (EU) 2021/1772 sprejeto sklepno ugotovitev o ravni varstva, ki jo zagotavlja Združeno kraljestvo. Ocena iz Izvedbenega sklepa (EU) 2021/1772 še naprej velja za tiste vidike okvira varstva podatkov v Združenem kraljestvu, ki po sprejetju Izvedbenega sklepa (EU) 2021/1772 niso bili spremenjeni ali na katere druge spremembe niso vplivale.

(15) Zakonodajne, regulativne in druge pomembne spremembe so podrobno analizirane v naslednjih oddelkih na podlagi standarda ustreznosti, v skladu s katerim mora Komisija ugotoviti, ali zadevna tretja država zagotavlja raven varstva, ki je „v osnovi enakovredna“ tisti, zagotovljeni v Evropski uniji ([23]). Kot je pojasnilo Sodišče Evropske unije, v ta namen ni nujno, da se ugotovi povsem enaka raven varstva ([24]). 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 ([25]). Standard ustreznosti torej ne zahteva dobesednega prepisa pravil Unije. Bolj kot to preskus temelji na proučitvi, ali tuji pravni sistem kot celota prek vsebine pravic varstva podatkov in njihovega dejanskega izvajanja, nadzora in izvrševanja zagotavlja zahtevano raven varstva ([26]).

([19]) Na voljo na povezavi: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) Temeljne pravice in temeljne svoboščine EU so bile v pravu Združenega kraljestva ohranjene s členom 4 zakona iz leta 2018 o izstopu iz Evropske unije, ki je bil konec leta 2023 razveljavljen z zakonom o ohranjenem pravu EU.

([21]) Člen 2(3) predpisov o varstvu podatkov (temeljne pravice in svoboščine) (sprememba) iz leta 2023.

([22]) Členi 6, 8, 10 in 13 EKČP (glej tudi dodatek 1 k zakonu o človekovih pravicah iz leta 1998).

([23]) Uvodna izjava 104 Uredbe (EU) 2016/679.

([24]) Sodba Schrems (v nadaljnjem besedilu: Schrems I), C-362/14, ECLI:EU:C:2015:650, točka 73.

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

([26]) Glej Sporočilo Komisije Evropskemu parlamentu in Svetu Izmenjava in varstvo osebnih podatkov v globaliziranem svetu (COM(2017) 7 z dne 10. januarja 2017, oddelek 3.1, str. 6 in 7), na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52017DC0007&from=SL.

2.1.1 *Opredelitev pojmov*

(16) Osnovni pojmi varstva podatkov, ki odražajo terminologijo Uredbe (EU) 2016/679, se v ureditvi varstva podatkov v Združenem kraljestvu še naprej uporabljajo. Ti pojmi so bili ocenjeni v uvodni izjavi 23 Izvedbenega sklepa (EU) 2021/1772.

(17) Čeprav v zakonu o podatkih (uporaba in dostop) velika večina opredelitev pojmov ostaja nespremenjena, so bile uvedene posebne opredelitve v zvezi z obdelavo osebnih podatkov za znanstvene, zgodovinske in statistične namene v členu 4(2), (3), (4) in (5) UK GDPR. V odstavku 2 je „obdelava v znanstvene namene“ opredeljena kot obdelava osebnih podatkov, izvedena za namene raziskave, ki se lahko razumno opiše kot znanstvena. Ta raziskava se lahko financira iz javnih ali zasebnih virov in izvaja kot komercialna ali nekomercialna dejavnost. V odstavku 3, ki izraža vsebino uvodne izjave 159 Uredbe (EU) 2016/679, je neizčrpen seznam primerov raziskovalnih dejavnosti, ki se štejejo za raziskave v znanstvene namene, vključno s tehničnim razvojem, predstavitvijo, temeljnimi raziskavami in uporabnimi raziskavami. V odstavku 4 je pojasnjeno, da „zgodovinske raziskave“ zajemajo tudi genealoške raziskave, ki se jim tudi v uvodni izjavi 160 Uredbe (EU) 2016/679 priznava zgodovinski namen. V odstavku 5 je obdelava v statistične namene opredeljena kot obdelava podatkov za statistične raziskave ali pripravo statističnih rezultatov, kadar so podatki zbirni v taki meri, da niso več osebni podatki. Poleg tega se obdelani podatki ali informacije, ki iz njih izhajajo, ne smejo uporabiti za sprejemanje odločitev ali izvajanje ukrepov v zvezi s posameznikom. Ta opredelitev je usklajena z razumevanjem statističnih namenov iz uvodne izjave 162 Uredbe (EU) 2016/679.

(18) Skratka, čeprav se s spremembami člena 4 UK GDPR dodajajo posebne opredelitve obdelave podatkov v znanstvene, zgodovinske in statistične namene, so te opredelitve skladne s črko in duhom Uredbe (EU) 2016/679, kot je razvidno iz nekaterih uvodnih izjav 159, 160 in 162.

(19) Z zakonom o podatkih (uporaba in dostop) je bil z vključitvijo odstavka 6 v člen 4 UK GDPR vzpostavljen tudi poseben okvir za pridobitev privolitve posameznika, na katerega se nanašajo osebni podatki, za obdelavo osebnih podatkov v znanstvene namene. Nova določba z zelo podobnim besedilom, kot je besedilo uvodne izjave 33 Uredbe (EU) 2016/679, ki priznava, da na področju znanstvenih raziskav privolitve ni vedno mogoče pridobiti za določen namen obdelave, omogoča širše oblike privolitve, saj dopušča, da posamezniki, na katere se nanašajo osebni podatki, dajo veljavno privolitev tudi takrat, ko natančnih namenov raziskave v času zbiranja podatkov ni mogoče v celoti opredeliti, pod pogojem, da je pridobivanje privolitve skladno s splošno priznanimi etičnimi standardi, ustreznimi za določeno raziskovalno področje. Posamezniki, na katere se nanašajo osebni podatki, pa morajo vsekakor imeti možnost, da privolijo v obdelavo osebnih podatkov le za določene dele raziskave, kadar je to mogoče.

(20) V zakonu o podatkih (uporaba in dostop) so v novem poglavju 8A UK GDPR nazadnje dodatno podrobno opredeljeni zaščitni ukrepi, prej določeni v členu 89 UK GDPR in členu 19 zakona o varstvu podatkov iz leta 2018, za obdelavo podatkov v namene arhiviranja v javnem interesu, znanstveno- ali zgodovinskoraziskovalne namene in statistične namene ([27]). Ti zaščitni ukrepi so podobni zaščitnim ukrepom v skladu s členom 89 Uredbe (EU) 2016/679 ter zajemajo zahtevo, da se sprejmejo tehnični in organizacijski ukrepi, s katerimi se zagotovi spoštovanje načela najmanjšega obsega podatkov.

2.2 **Zaščitni ukrepi, pravice in obveznosti**

2.2.1 *Zakonitost in poštenost obdelave*

(21) V skladu z okvirom varstva podatkov v Združenem kraljestvu se morajo podatki še naprej obdelovati zakonito, pošteno in legitimno, kot je ocenjeno v uvodnih izjavah 24 do 26 Izvedbenega sklepa (EU) 2021/1772.

([27]) Členi 84A do 84D UK GDPR, kot so uvedeni s členom 86 zakona o podatkih (uporaba in dostop).

(22) Načeli zakonitosti in poštenosti ter razlogi za zakonito obdelavo so v pravu Združenega kraljestva še naprej zagotovljeni s členom 5(1), točka (a), in členom 6(1) UK GDPR, kot je ocenjeno v Izvedbenem sklepu (EU) 2021/1772. Čeprav te določbe ostajajo v glavnem enake ([28]) ustreznim določbam Uredbe (EU) 2016/679, zakon o podatkih (uporaba in dostop) najprej spreminja člen 6(1) UK GDPR z uvedbo dodatne zakonite podlage za obdelavo osebnih podatkov v skladu s členom 6(1), točka (ea) ([29]). V skladu s to določbo je obdelava zakonita, če in kolikor je „potrebna zaradi priznanega zakonitega interesa“. V nasprotju s pravno podlago zakonitega interesa iz člena 6(1), točka (f), UK GDPR v skladu z novouvedeno pravno podlago priznanega zakonitega interesa zakonitih interesov upravljavca in interesov ali temeljnih pravic in svoboščin posameznika, na katerega se nanašajo osebni podatki, ni treba pretehtati za vsak primer posebej, s čimer se zasebnim upravljavcem, zagotavlja večja pravna varnost. Novouvedeni člen 6(5) UK GDPR določa, da je obdelava potrebna zaradi priznanega zakonitega interesa le, če izpolnjuje pogoj iz Priloge 1 ([30]), kjer so nato navedeni primeri, v katerih se obdelava šteje za potrebno zaradi priznanega zakonitega interesa, na primer kadar je izvedena v odgovor na zahtevo, predloženo javnemu organu, ki potrebuje podatke za izvajanje naloge v javnem interesu, katere pravna podlaga ustreza zahtevam iz člena 6(3) UK GDPR, kadar je obdelava potrebna za zaščito nacionalne ali javne varnosti ali obrambe, odziv na izredne razmere, odkrivanje, preiskovanje ali preprečevanje kaznivih dejanj ali zaščito ranljivih posameznikov ([31]).

(23) Čeprav zakon o podatkih (uporaba in dostop) tako razširja seznam pravnih podlag za obdelavo osebnih podatkov, ki so na voljo upravljavcu, pa za novo uvedeno pravno podlago priznanega zakonitega interesa velja več pomembnih omejitev. Prvič, priznani zakoniti interesi so omejeni na posebne primere, ki so v zakonu izčrpno navedeni. Drugič, javni organi se pri izvajanju svojih nalog ne morejo opirati na to pravno podlago ([32]). Tretjič, nanaša se le na področja, na katerih obstaja jasen javni interes za dejavnost obdelave (v skladu s pogoji iz Priloge 1), tj. kadar obdelava izpolnjuje cilje iz člena 23 UK GDPR (ki ustreza členu 23 Uredbe (EU) 2016/679), zato se nanjo ni mogoče sklicevati v komercialne namene. Četrtič, zakon o podatkih (uporaba in dostop) daje pristojnemu ministru pravico, da seznam v Prilogi 1 spremeni s predpisi ([33]), vendar lahko ta minister take predpise sprejme le po

([28]) Za pojasnitev – z zakonom o podatkih (uporaba in dostop) je v člen 6 UK GDPR uveden tudi nov odstavek, v katerem so navedeni primeri vrst obdelave, ki se lahko štejejo za potrebne za namen zakonitega interesa v smislu člena 6(1), točka (f), UK GDPR. Ti primeri (neposredno trženje, posredovanje podatkov znotraj povezane družbe v upravne namene ter varnost omrežij in informacijskih sistemov) so navedeni tudi v uvodnih izjavah 47 in 48 Uredbe (EU) 2016/679 kot primeri, v katerih bi se štelo, da je obdelava v zakonitem interesu upravljavca.

([29]) Člen 70(2), točka (b), zakona o podatkih (uporaba in dostop). S členom 70(5) zakona o podatkih (uporaba in dostop) je bila pravica do ugovora iz člena 21 UK GDPR razširjena na novi člen 6(1), točka (ea), UK GDPR.

([30]) Člen 70(4) zakona o podatkih (uporaba in dostop).

([31]) Glej dodatek 4 k zakonu o podatkih (uporaba in dostop). Po navedbah organov Združenega kraljestva primeri, v katerih bodo zasebni subjekti morda morali obdelati osebne podatke za preprečevanje ali odkrivanje kaznivih dejanj, vključujejo podjetje, ki izve za poskuse nezakonitega vdora v svoje računalniške sisteme, ali banko oziroma finančno institucijo, ki izve za goljufive poskuse odprtja računa. Obdelava osebnih podatkov, ki jo izvede zasebni subjekt, je lahko na primer potrebna za zaščito nacionalne varnosti ali obrambe, kadar komercialna organizacija sumi, da spletna dejavnost stranke kaže na vpletenost v teroristično dejavnost. Urad informacijskega pooblaščenca pripravlja posebne smernice o tem, vključno z opredelitvijo ustreznih pojmov. Navaja na primer „nacionalno varnost“, ki bo verjetno zajemala varnost in blaginjo Združenega kraljestva kot celote, njegovega prebivalstva, njegovih institucij in vladnega sistema. Glej osnutek smernic urada informacijskega pooblaščenca o priznanem zakonitem interesu, kot je bil objavljen za javno posvetovanje in ki je na voljo na povezavi: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Člen 6(1), zadnji pododstavek, kot je bil spremenjen s členom 70(2), točka (c), zakona o podatkih (uporaba in dostop).

([33]) Pristojni minister mora pred sprejetjem predpisov upoštevati učinke morebitnih sprememb na interese ter temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ter dejstvo, da otroci (kadar je to ustrezno) glede osebnih podatkov potrebujejo posebno varstvo. Predpisi morajo biti sprejeti z aktom z zakonsko močjo, glede njih pa se izvede postopek pozitivne potrditve, kar pomeni, da jih mora aktivno odobriti parlament Združenega kraljestva. Člen 70(4), pododstavek 8, zakona o podatkih (uporaba in dostop).

posvetovanju z uradom informacijskega pooblaščenca ([34]), priznan zakoniti interes pa lahko na ta seznam doda le, če je taka obdelava prav tako potrebna za zagotavljanje cilja v javnem interesu iz člena 23(1), točke (c) do (j), UK GDPR ([35]). Nazadnje, kot potrjujejo tudi smernice urada informacijskega pooblaščenca ([36]), morajo upravljavci podatkov, ki se sklicujejo na priznan zakoniti interes kot pravno podlago, izpolnjevati vse druge zahteve iz UK GDPR, vključno z zagotavljanjem, da je obdelava potrebna in sorazmerna za doseganje zakonitega interesa.

(24) V zakonu o podatkih (uporaba in dostop) je v členu 6(3), členu 9(2), točka (g), in členu 10(1) UK GDPR, ki ustrezajo zadevnim določbam Uredbe (EU) 2016/679, pojasnjeno, da je lahko podlaga za obdelavo osebnih podatkov, posebnih vrst osebnih podatkov ter osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški zaradi izpolnjevanja pravne obveznosti ali izvajanja naloge v javnem interesu ne le v notranjem pravu, temveč tudi v ustreznem mednarodnem pravu ([37]). Ustrezno mednarodno pravo je nato z novo uvedenim členom 9A UK GDPR v povezavi z dodatkom A1 omejeno na en sam sporazum, in sicer na sporazum 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), podpisan 3. oktobra 2019 (v nadaljnjem besedilu: sporazum med Združenim kraljestvom in ZDA) ([38]). Zaščitni ukrepi iz navedenega sporazuma so bili ocenjeni v uvodnih izjavah 153 do 155 Izvedbenega sklepa (EU) 2021/1772, njihovo izvajanje pa je analizirano v uvodnih izjavah 87 do 93 tega sklepa.

### 2.2.2 *Obdelava posebnih vrst osebnih podatkov*

(25) Okvir varstva podatkov v Združenem kraljestvu še naprej določa posebne zaščitne ukrepe v primerih posebnih vrst podatkov, kot je ocenjeno v uvodnih izjavah 27 do 42 Izvedbenega sklepa (EU) 2021/1772.

(26) Opredelitev posebnih vrst osebnih podatkov in posebna pravila, ki se uporabljajo za njihovo obdelavo, iz UK GDPR in zakona o varstvu podatkov iz leta 2018 ostajajo v veljavi. Zakon o podatkih (uporaba in dostop) pa hkrati pristojnemu ministru podeljuje nova pooblastila za sprejemanje predpisov, da doda posebne vrste podatkov, prilagodi pogoje, ki veljajo za njihovo uporabo, in po potrebi doda nove opredelitve ([39]). Pomembno je, da pristojnemu ministru ne dovoljuje, da bi odstranil ali spremenil obstoječe posebne vrste podatkov ali spremenil pogoje za obdelavo teh vrst ([40]). Vlada lahko tako z novo uvedenim pooblastilom za sprejemanje predpisov le dodaja nove vrste občutljivih podatkov in določa pogoje za njihovo obdelavo, kar naj bi ji omogočilo, da se po potrebi odzove na prihodnji tehnološki in družbeni razvoj.

(27) Zato te spremembe ne vplivajo na raven varstva posebnih vrst osebnih podatkov, za katero je bilo v Izvedbenem sklepu (EU) 2021/1772 ugotovljeno, da je v osnovi enakovredna varstvu v EU.

([34]) Člen 182(2) zakona o varstvu podatkov iz leta 2018.

([35]) Člen 70(4), pododstavek 9, zakona o podatkih (uporaba in dostop).

([36]) Glej smernice urada informacijskega pooblaščenca o zakonitih interesih, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Člen 72 zakona o podatkih (uporaba in dostop).

([38]) Sporazum 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, 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.

([39]) Člen 74 zakona o podatkih (uporaba in dostop). Glede takih predpisov se izvede postopek pozitivne potrditve, kar pomeni, da jih mora aktivno odobriti parlament Združenega kraljestva.

([40]) Glej novi člen 11A(1), točka (b), in (2) UK GDPR ter pojasnjevalne opombe k predlogu zakona o podatkih (uporaba in dostop), točka 571, na voljo na povezavi: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3 *Omejitev namena*

(28) V ureditvi varstva osebnih podatkov v Združenem kraljestvu se še naprej zahteva, da se podatki obdelujejo za določen namen in se nato uporabljajo samo, če to ni nezdružljivo s prvotnim namenom obdelave, kot je ocenjeno v uvodnih izjavah 43 do 48 Izvedbenega sklepa (EU) 2021/1772.

(29) Prvič, z zakonom o podatkih (uporaba in dostop) je vnesenih nekaj ciljnih sprememb načela omejitve namena iz člena 5(1), točka (b), UK GDPR. Z njimi se pojasnjuje uporaba tega načela, ne da bi se spremenila njegova vsebina. Člen 71(1), (2) in (3) zakona o podatkih (uporaba in dostop) določa, da se načelo omejitve namena uporablja, kadar se podatki zbirajo od posameznika, na katerega se nanašajo osebni podatki, ali kako drugače, in sicer le, kadar osebne podatke nadalje obdeluje isti upravljavec ali se ti obdelujejo v njegovem imenu (kar pomeni, da se v primeru zamenjave upravljavca ne uporablja), in da obdelava ni zakonita zgolj zato, ker je združljiva z nameni, za katere so bili osebni podatki zbrani.

(30) Drugič, v zakonu o podatkih (uporaba in dostop) so pojasnjena pravila o nadaljnji obdelavi osebnih podatkov, s tem da so združena v novo dodani člen 8A UK GDPR, ki določa celotno ureditev nadaljnje obdelave osebnih podatkov. V členu 8A(2) UK GDPR so navedeni elementi, ki jih je treba upoštevati pri ugotavljanju, ali je nov namen obdelave združljiv s prvotnim namenom. Ti elementi so bili prej navedeni v členu 6(4) UK GDPR, ki ustreza členu 6(4) Uredbe (EU) 2016/679 ([41]). Člen 8A(3) UK GDPR v eni določbi združuje primere, v katerih je treba obdelavo osebnih podatkov za nov namen obravnavati kot združljivo s prvotnim namenom. Zajema primere, v katerih posameznik, na katerega se nanašajo osebni podatki, privoli v obdelavo osebnih podatkov za nov namen ali v katerih je obdelava potrebna za uresničevanje cilja iz člena 23(1) ([42]) ali se obdelava izvaja za znanstveno- ali zgodovinskoraziskovalne namene, namene arhiviranja v javnem interesu ali statistične namene ([43]). V zakonu o podatkih (uporaba in dostop) je nazadnje pojasnjeno, da se vsaka obdelava, ki se izvaja za zagotovitev skladnosti obdelave z načeli varstva podatkov iz člena 5(1) UK GDPR ali za dokazovanje, da je skladna, šteje za združljivo s prvotnim namenom. Navedeni primeri še naprej ustrezajo temu, kar se šteje za združljivo nadaljnjo obdelavo tudi v Uredbi (EU) 2016/679.

(31) Tretjič, zakon o podatkih (uporaba in dostop) v členu 8A(3), točka (d), UK GDPR uvaja tudi nove dodatne primere, v katerih se nadaljnja obdelava osebnih podatkov za nov namen šteje za združljivo s prvotnim namenom. Ti primeri so navedeni v Prilogi 2 k UK GDPR ([44]) in med drugim zajemajo primere, ko se obdelava izvede v odgovor na zahtevo, predloženo javnemu organu, ki potrebuje podatke za izvajanje naloge v javnem interesu, katere pravna podlaga ustreza zahtevam iz člena 6(3) UK GDPR, kadar je obdelava potrebna za zaščito javne varnosti, odziv na izredne razmere, odkrivanje, preiskovanje ali preprečevanje kaznivih dejanj, zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, in drugih, zaščito ranljivih posameznikov, davčne namene ali, po potrebi, izpolnjevanje pravne obveznosti ([45]).

(32) Zakon o podatkih (uporaba in dostop) torej sicer razširja seznam primerov, v katerih se nadaljnja obdelava za drug namen šteje za združljivo s prvotnim namenom obdelave, vendar za to razširitev veljajo pomembne omejitve. Prvič, omejena je na posebne primere, ki so v zakonu izčrpno navedeni. Drugič, nanaša se le na področja, na katerih obstaja jasen javni interes za dejavnost obdelave, tj. kadar nadaljnja obdelava izpolnjuje cilje iz člena 23 UK GDPR

([41]) Ti elementi tako kot v Uredbi (EU) 2016/679 zajemajo kakršno koli povezavo med prvotnim in novim namenom, okoliščine, v katerih so bili osebni podatki zbrani, vključno z razmerjem med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem, naravo obdelave in morebitno vključene posebne vrste podatkov, morebitne posledice načrtovane obdelave za posameznika, na katerega se nanašajo osebni podatki, ter obstoj ustreznih zaščitnih ukrepov.

([42]) Glej tudi člen 6(4) Uredbe (EU) 2016/679.

([43]) Uvodna izjava 50 Uredbe (EU) 2016/679.

([44]) Priloga 2 k UK GDPR je uvedena z dodatkom 5 k zakonu o podatkih (uporaba in dostop), glej člen 71(6) tega zakona.

([45]) Glej dodatek 5 k zakonu o podatkih (uporaba in dostop).

(ki ustreza členu 23 Uredbe (EU) 2016/679). Zato se nanjo ni mogoče sklicevati za komercialne namene. Tretjič, zakon o podatkih (uporaba in dostop) daje pristojnemu ministru pravico, da seznam v Prilogi 2 spremeni s predpisi ([46]), vendar lahko ta minister vrste obdelave na ta seznam doda le, če je taka obdelava prav tako potrebna za zagotavljanje cilja v javnem interesu iz člena 23(1), točke (c) do (j), UK GDPR ([47]). Četrtič, kadar zbiranje osebnih podatkov s strani upravljavca temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki, se obdelava za nov namen v primerih iz Priloge 2 šteje za združljivo s prvotnim namenom le, če ni mogoče razumno pričakovati, da bi upravljavec od posameznika, na katerega se nanašajo osebni podatki, pridobil novo privolitev ([48]).

2.2.4 *Pravice posameznikov*

(33) Posamezniki, na katere se nanašajo osebni podatki, v okviru varstva osebnih podatkov v Združenem kraljestvu še naprej brez bistvenih sprememb uživajo enake pravice posameznikov kot na podlagi Uredbe (EU) 2016/679 ([49]), ki jih lahko uresničujejo zoper upravljavca ali obdelovalca, zlasti pravico dostopa do podatkov, pravico ugovarjati obdelavi ter pravico do popravka in izbrisa podatkov, kot je ocenjeno v uvodnih izjavah 51 do 54 Izvedbenega sklepa (EU) 2021/1772.

(34) Zakon o podatkih (uporaba in dostop) pojasnjuje nekatere načine, na podlagi katerih se te pravice lahko uveljavljajo. Po eni strani s spremembo člena 12 in uvedbo novega člena 12A UK GDPR ([50]) določa roke, v katerih morajo upravljavci odgovoriti na zahteve posameznika, na katerega se nanašajo osebni podatki. Člen 12 UK GDPR je natančneje spremenjen tako, da upravljavcu v odgovor na zahtevo posameznika, na katerega se nanašajo osebni podatki, ni več treba zagotoviti informacij o sprejetih ukrepih (ali razlogih za neukrepanje) v skladu s členi 15 do 22 UK GDPR „v enem mesecu od prejema zahteve“, temveč jih mora zagotoviti „pred koncem veljavnega roka“. Veljavni rok je v novo uvedenem členu 12A UK GDPR dodatno opredeljen kot enomesečno obdobje, ki se začne ob ustreznem času, to je takrat, ko upravljavec prejme zahtevo, ko upravljavec prejme kakršne koli informacije, zahtevane v zvezi z zahtevo na podlagi člena 12(6) UK GDPR, ali ko je plačana pristojbina, zaračunana v zvezi z zahtevo na podlagi člena 12(5) UK GDPR, pri čemer se upošteva najpoznejši od teh datumov ([51]). Člen 12A(3) upravljavcu nadalje dovoljuje, da veljavni rok podaljša za dodatna dva meseca, kadar je to potrebno zaradi zapletenosti zahtev posameznika, na katerega se nanašajo osebni podatki, ali številčnosti takih zahtev. Po drugi strani pa je z zakonom o podatkih (uporaba in dostop) člen 15 UK GDPR spremenjen le glede pravice dostopa do informacij in osebnih podatkov, da bi se upoštevalo pojasnilo iz obstoječe nacionalne sodne prakse – ki temelji na načelu sorazmernosti iz prava EU –, da morajo upravljavci izvesti le razumna in sorazmerna iskanja zahtevanih informacij in osebnih podatkov ([52]). Pričakuje se, da se bo nova določba razlagala v skladu z obstoječo sodno prakso, ki določa, da „[…] se pri preverjanju sorazmernosti pretehta končni cilj iskanja, in sicer morebitna korist, ki bi jo zagotovitev informacij lahko prinesla posamezniku, na katerega se nanašajo osebni podatki, v primerjavi s sredstvi, s katerimi se te informacije pridobijo. Za vsak primer posebej je treba oceniti, ali bi iskanje in zagotavljanje informacij vključevalo nesorazmeren napor v primerjavi s koristmi, ki bi jih te informacije lahko prinesle posamezniku, na katerega se nanašajo osebni podatki“ ([53]).

([46]) Člen 8A(5) UK GDPR, kot je bil uveden s členom 71(1) zakona o podatkih (uporaba in dostop).
([47]) Člen 8A(6) UK GDPR, kot je bil uveden s členom 71(1) zakona o podatkih (uporaba in dostop).
([48]) Člen 8A(4), točka (b), UK GDPR, kot je bil uveden s členom 71(1) zakona o podatkih (uporaba in dostop).
([49]) S členom 31 zakona o žrtvah in zapornikih iz leta 2024 (Victims and Prisoners Act 2024) je bil v pravico do izbrisa iz člena 17 UK GDPR vstavljen dodaten razlog, ki posameznikom, na katere se nanašajo osebni podatki, daje pravico, da od upravljavcev zahtevajo izbris svojih osebnih podatkov, kadar so bili ti obdelani na podlagi neutemeljene trditve o posamezniku, na katerega se nanašajo osebni podatki, ki jo je podala zlonamerna oseba. Oseba se šteje za „zlonamerno“, če je bila obsojena za kaznivo dejanje iz člena 31(3) zakona o žrtvah in zapornikih (na primer zaradi nadlegovanja) ali če je zoper njo izdana odredba o prepovedi zalezovanja. Zakon o žrtvah in zapornikih je na voljo na naslednji povezavi: https://www.legislation.gov.uk/ukpga/2024/21/contents. Poleg tega se s členom 77 zakona o podatkih (uporaba in dostop) pravica do obveščenosti iz člena 13 UK GDPR spreminja tako, da upravljavcu posameznika, na katerega se nanašajo osebni podatki, ni več treba obvestiti o nadaljnji obdelavi njegovih osebnih podatkov za nov namen, če gre za znanstveno- ali zgodovinskoraziskovalne namene, namene arhiviranja v javnem interesu ali statistične namene, če se obdelava izvaja v skladu s posebnimi zaščitnimi ukrepi iz novega člena 84B UK GDPR in če bi bila zagotovitev informacij nemogoča ali nesorazmerna.
([50]) Člen 76 zakona o podatkih (uporaba in dostop).
([51]) Člen 12A(1) in (2) UK GDPR, kot je bil uveden s členom 76 zakona o podatkih (uporaba in dostop).
([52]) Člen 15(1A) UK GDPR, kot je bil uveden s členom 78 zakona o podatkih (uporaba in dostop).
([53]) Sodba Dawson-Damer/Taylor Wessing LLP [2017] EWCA Civ 74.

(35) Čeprav torej za roke za odziv na zahteve posameznikov, na katere se nanašajo osebni podatki, in posebne obveznosti upravljavcev podatkov v zvezi s pravico dostopa veljajo podrobnejša pravila, sistem Združenega kraljestva še naprej zagotavlja, da je treba zahteve posameznikov, na katere se nanašajo osebni podatki, obravnavati v razumnih rokih, določenih na podlagi objektivnih dejavnikov. Poleg tega so vsebinske obveznosti upravljavca pri odzivanju na zahteve za dostop določene na podlagi uveljavljenih pravnih standardov, pri katerih se upoštevajo tudi interesi posameznika, na katerega se nanašajo osebni podatki. Nazadnje, v sedanjih smernicah urada informacijskega pooblaščenca je že določeno, da upravljavcu ni treba izvajati iskanj, ki bi bila nerazumna ali nesorazmerna s pomembnostjo zagotavljanja dostopa do informacij ([54]).

(36) Omejitve teh pravic posameznikov, ki so določene v zakonu o varstvu podatkov iz leta 2018 in ki ustrezajo okviru člena 23 UK GDPR, ter omejitve in zaščitni ukrepi, s katerimi se ureja uporaba teh omejitev, so v okviru Združenega kraljestva ([55]) še naprej v veljavi, kot je podrobno opisano v uvodnih izjavah 55 do 67 Izvedbenega sklepa (EU) 2021/1772.

(37) Vlada Združenega kraljestva je zlasti v zvezi z omejitvijo za osebne podatke, ki se obdelujejo zaradi ohranjanja učinkovitega nadzora priseljevanja ali preiskovanja ali odkrivanja dejavnosti, ki bi lahko ogrozile ohranjanje učinkovitega nadzora priseljevanja, če bi uporaba teh določb verjetno posegala v katero koli od teh zadev (izjema glede priseljevanja) ([56]), spremenila točko 4 dodatka 2 k zakonu o varstvu podatkov iz leta 2018 s predpisi o zakonu o varstvu podatkov iz leta 2018 (sprememba izjem iz dodatka 2) iz leta 2022 ([57]) in predpisi o zakonu o varstvu podatkov iz leta 2018 (sprememba izjem iz dodatka 2) iz leta 2024 ([58]), ki dopolnjujejo predpise iz leta 2022 ([59]). S spremembami so v točki 4A in 4B dodatka 2 k zakonu o varstvu podatkov iz leta 2018 vključeni zaščitni ukrepi za izvajanje izjeme glede priseljevanja, kot se zahtevajo s členom 23(2) UK GDPR. Z njimi se zlasti zahteva, (i) da se je treba na izjemo glede priseljevanja sklicevati le za vsak primer posebej, ločeno za vsako od zadevnih določb UK GDPR in vsakič znova, ko pristojni minister razmišlja o neuporabi ali omejitvi uporabe katere od zadevnih določb UK GDPR ([60]), (ii) da se pri uporabi izjeme glede priseljevanja upoštevajo pravice in svoboščine ter morebitne ranljivosti posameznika, na katerega se nanašajo osebni podatki ([61]), (iii) da pristojni minister vodi evidenco o uporabi izjeme glede priseljevanja in posameznika, na katerega se nanašajo osebni podatki, obvesti o njeni uporabi (razen v posebnih okoliščinah, ko bi informacije škodovale cilju izjeme) ([62]), ter (iv) da se pojasni, da je uporaba izjeme glede priseljevanja omejena na obdelavo osebnih podatkov, ki jo izvaja pristojni minister ([63]), tj. ministrstvo za notranje zadeve v okviru svojih nalog, ki se nanašajo na odstavek 4(1) dodatka 2 k zakonu o varstvu podatkov iz leta 2018. Poleg tega se z njimi pojasnjuje tudi presoja, ki je treba izvesti pri ugotavljanju, ali bi uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, verjetno posegalo v učinkovit nadzor priseljevanja ter ali je zato nujno in sorazmerno take pravice omejiti.

([54]) Na voljo na povezavi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) S členom 88(2) zakona o podatkih (uporaba in dostop) je nekoliko spremenjen člen 26(2), točka (f), zakona o varstvu podatkov iz leta 2018 (izjema na področju nacionalne varnosti in obrambe), da bi se pojasnilo, da pravica do vložitve pritožbe pri informacijskem pooblaščencu v skladu s členom 77 UK GDPR ni del določb, katerih uporaba se lahko omeji zaradi nacionalne varnosti ali obrambe.

([56]) Ob sprejetju Izvedbenega sklepa (EU) 2021/1772 veljavnost in razlaga izjeme glede priseljevanja v skladu s pravom Združenega kraljestva še nista bili določeni, po tem ko je sodišče England and Wales Court of Appeal v odločbi z dne 26. maja 2021 ugotovilo, da je izjema glede priseljevanja, kot je bila določena v zakonu o varstvu podatkov iz leta 2018, nezdružljiva s pravom Združenega kraljestva, saj ni vsebovala posebnih določb, ki bi določale zaščitne ukrepe iz člena 23(2) UK GDPR, ki odraža člen 23(2) Uredbe (EU) 2016/679. Zato so bili osebni podatki, ki se prenašajo za namene nadzora priseljevanja v Združeno kraljestvo ali ki sicer spadajo na področje uporabe izjeme glede priseljevanja, izključeni s področja uporabe Izvedbenega sklepa (EU) 2021/1772.

([57]) Predpisi so začeli veljati 31. januarja 2022 in so na voljo na naslednji povezavi: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Predpisi so začeli veljati 8. marca 2024 in so na voljo na naslednji povezavi: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) Izjema glede priseljevanja, kot je bila popravljena s predpisi iz leta 2022, je bila ponovno izpodbijana s sodno presojo, ker še ni izpolnjevala vseh zahtev iz člena 23(2) UK GDPR. Sodišče Court of Appeal je decembra 2023 ugotovilo, da ni združljiva z zahtevami iz člena 23(2) UK GDPR. Na podlagi navedene sodbe predpisi iz leta 2024 dopolnjujejo predpise iz leta 2022 in uvajajo nadaljnje spremembe izjeme glede priseljevanja.

([60]) Točka 4A(2) dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([61]) Točka 4AB(3) in (4) dodatka 2 k zakonu o varstvu podatkov iz leta 2018. Urad informacijskega pooblaščenca, s katerim je bilo opravljeno posvetovanje o osnutku predpisov iz leta 2024, je javno izjavil, da je z njimi zadovoljen. Dopis, ki je bil objavljen kot odziv na posvetovanje in ki potrjuje njegovo stališče, je na voljo na naslednji povezavi: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Točka 4AB(1) in (2) dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

([63]) Točka 4(1) dodatka 2 k zakonu o varstvu podatkov iz leta 2018.

(38) Poleg tega je urad informacijskega pooblaščenca Združenega kraljestva izdal podrobne smernice o uporabi te posebne omejitve ([64]). V njih je zlasti navedeno, da se „izjema glede priseljevanja ne sme uporabljati kot splošna izjema za omejevanje […] pravic za vse podatke, ki jih hranite. Področje uporabe izjeme je omejeno na tiste pravice, ki bi, če bi se uveljavljale za hranjene podatke, škodovale opredeljenim namenom priseljevanja. […]. Zato bi moralo biti običajno stališče upravljavca, da čim bolj izpolnjuje zahteve iz Uredbe (EU) 2016/679 in zakona o varstvu podatkov. […] Preskus poseganja ima visok prag in izjeme ne smete uporabljati na splošno. […] Proučiti morate, ali se z uporabo izjeme sorazmerno odzovete na zahtevo posameznika po varstvu podatkov. Morda menite, da je zaradi nujne družbene potrebe izjemo glede priseljevanja treba uporabiti, vendar morate upoštevati tudi, ali to prevlada nad vašo obveznostjo do posameznikov v skladu z Uredbo (EU) 2016/679. Ti imajo pravice do svojih osebnih podatkov, zlasti pravico dostopa, ki jih morate v vseh okoliščinah upoštevati. Zato je pomembno, da v vsakem primeru proučite, ali pravice posameznika do varstva podatkov prevladajo nad ugotovljenim tveganjem poseganja. Izjemo morate uporabljati sorazmerno z okoliščinami, vsak primer pa morate skrbno proučiti in dokumentirati.“

(39) Na splošno za omejitev priseljevanja iz točke 4 dodatka 2 k zakonu o varstvu podatkov iz leta 2018, kot jo je vlada Združenega kraljestva spremenila v letih 2022 in 2024 ter kot se razlaga s sodno prakso ([65]) in smernicami urada informacijskega pooblaščenca, velja več strogih pogojev, ki določajo njeno uporabo in so zelo podobni pogojem iz prava Unije, zlasti iz člena 23 Uredbe (EU) 2016/679, za omejitev pravic in obveznosti na področju varstva podatkov zaradi pomembnih ciljev v javnem interesu, kot je nadzor priseljevanja.

2.2.5 *Omejitve nadaljnjih prenosov podatkov*

(40) Raven varstva, zagotovljena za osebne podatke, ki se iz Evropske unije prenesejo upravljavcem ali obdelovalcem v Združenem kraljestvu, se z nadaljnjim prenosom takih podatkov prejemnikom v tretji državi še naprej ne poslabšuje. Ureditev mednarodnih prenosov osebnih podatkov iz Združenega kraljestva ostaja zelo podobna pravilom iz poglavja V Uredbe (EU) 2016/679, kot je ocenjeno v uvodnih izjavah 74 do 82 Izvedbenega sklepa (EU) 2021/1772.

(41) Čeprav je bilo z zakonom o podatkih (uporaba in dostop) spremenjeno poglavje 5 UK GDPR o prenosih osebnih podatkov v tretje države ali mednarodne organizacije, je ohranjena temeljna zahteva, da se lahko osebni podatki v tretjo državo ali mednarodno organizacijo prenesejo le, če prenos temelji na (i) predpisih o odobritvi prenosa (nova terminologija za prejšnje poimenovanje „predpisi o ustreznosti“), (ii) ustreznih zaščitnih ukrepih ali (iii) odstopanju za posebne primere. Ta splošna načela za prenose podatkov so izražena v novem členu 44A, ki nadomešča člen 44 UK GDPR ([66]) in določa tudi, da so prenosi osebnih podatkov v tretjo državo ali mednarodno organizacijo dovoljeni le, če se prenos izvede v skladu z drugimi določbami UK GDPR.

(42) V členu 45A(2) UK GDPR je zlasti glede predpisov o odobritvi prenosa določeno, da lahko pristojni minister take predpise sprejme le, če meni, da je preskus varstva podatkov izpolnjen. To pomeni, da je možnost, uvedena s členom 45A(3) UK GDPR, da ta minister pri sprejemanju takih predpisov upošteva zaželenost olajšanja pretoka podatkov, vedno odvisna od tega, ali je izpolnjen preskus varstva podatkov. Pravni standard za preskus varstva podatkov, ki mora biti izpolnjen, je določen v novem členu 45B(1) UK GDPR, v skladu s katerim standard varstva posameznikov, na katere se nanašajo osebni podatki, v državah prejemnicah ali mednarodnih organizacijah ni bistveno nižji od standarda, določenega za posameznike, na katere se nanašajo osebni podatki, v ustrezni zakonodaji Združenega kraljestva o varstvu podatkov. Člen 45B(2) UK GDPR določa neizčrpen seznam elementov, ki jih je treba upoštevati pri presoji, ali je ta preskus izpolnjen, kot so spoštovanje pravne države in človekovih pravic, obstoj in pooblastila organa za varstvo podatkov, ureditev pravnih sredstev ali zunajsodnih pravnih sredstev, pravila o prenosu osebnih podatkov iz države ali s strani organizacije v druge države ali mednarodne

([64]) Na voljo na povezavi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

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

([66]) Člen 85 zakona o podatkih (uporaba in dostop) in dodatek 7 k navedenemu zakonu.

organizacije, ustrezne mednarodne obveznosti države ali organizacije ter ustava, tradicija in kultura države ali organizacije. Čeprav je z novim členom 45B(2) preoblikovan seznam ustreznih elementov, kot je določen v prejšnjem členu 45 UK GDPR, so ohranjeni ključni elementi navedenega seznama, zato ostaja blizu temu, kar je določeno v poglavju V Uredbe (EU) 2016/679. Poleg tega so organi Združenega kraljestva potrdili, da bo pristojni minister upošteval elemente, ki niso navedeni v členu 45B(2), kot so zakoni in prakse v tretji državi glede načina dostopanja javnih organov do osebnih podatkov zaradi nacionalne varnosti ali preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kolikor vplivajo na splošni standard varstva podatkov. Organi Združenega kraljestva poleg tega menijo, da bo pri obravnavanju zadev, ki so neizčrpno navedene v členu 45B(2) UK GDPR, bistven element ustrezna sodna praksa v tretji državi.

(43) Za predpise o odobritvi prenosa še naprej veljajo „splošne“ postopkovne zahteve iz člena 182 zakona o varstvu podatkov iz leta 2018, kot je navedeno v uvodni izjavi 77 Izvedbenega sklepa (EU) 2021/1772. V skladu s tem postopkom se mora pristojni minister, preden predlaga sprejetje predpisov Združenega kraljestva o ustreznosti, posvetovati z informacijskim pooblaščencem ([67]). Ko pristojni minister sprejme navedene predpise, se predložijo parlamentu, ki jih obravnava v postopku tako imenovane negativne potrditve, v katerem lahko oba domova parlamenta predpise proučita in jih v 40 dneh razveljavita ([68]).

(44) V novem odstavku člena 46(1A) UK GDPR je glede ustreznih zaščitnih ukrepov določeno, da se lahko taki prenosi izvedejo le, če so v instrumentih, ki so na voljo v skladu s členom 46(2) in (3) UK GDPR ([69]), zagotovljeni ustrezni zaščitni ukrepi ter če upravljavec, obdelovalec ali ustrezni javni organi, ki delujejo razumno in sorazmerno, menijo, da je preskus varstva podatkov izpolnjen. Z novo vstavljenima odstavkoma 6 in 7 je pojasnjeno, da je preskus varstva podatkov izpolnjen, če zaradi zahtevanih zaščitnih ukrepov standard varstva, določen za posameznike, na katere se nanašajo osebni podatki, po prenosu ni bistveno nižji od standarda v skladu z ustrezno zakonodajo Združenega kraljestva o varstvu podatkov, tj. da se, tako kot velja v skladu z Uredbo (EU) 2016/679, isti pravni standardi uporabljajo za predpise o odobritvi prenosa in ustrezne zaščitne ukrepe. Kaj je razumno in sorazmerno, se v skladu z istim odstavkom določi glede na vse okoliščine ali verjetne okoliščine prenosa ali vrste prenosa, vključno z naravo in obsegom prenesenih osebnih podatkov.

(45) Glede odstopanj za posebne primere je v členu 49 UK GDPR o pogojih, pod katerimi se lahko uporabljajo odstopanja za posebne primere, uvedenih nekaj tehničnih sprememb, s katerimi je določba usklajena s spremembami drugih določb, ki pa ne vplivajo na raven varstva osebnih podatkov v Združenem kraljestvu. Poleg tega je vstavljen nov odstavek 4A, s katerim se zagotavlja enak pravni učinek kot s členom 18(1) zakona o varstvu podatkov iz leta 2018, ki pristojnemu ministru podeljuje pooblastilo, da s predpisi določi okoliščine za prenose podatkov, ki se štejejo za potrebne iz razlogov javnega interesa. Z novim členom 49A je nazadnje zagotovljen enak pravni učinek kot s členom 18(2) zakona o varstvu podatkov iz leta 2018, ki pristojnemu ministru omogoča, da s predpisi uvede omejitve pri prenosih podatkov, kadar ti niso odobreni v skladu s členom 45A (prenosi, odobreni s predpisi) in kadar je to potrebno iz pomembnih razlogov javnega interesa.

(46) Od sprejetja Izvedbenega sklepa (EU) 2021/1772 se je glede izvajanja pravil Združenega kraljestva o mednarodnih prenosih zgodilo več sprememb.

([67]) 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 povezavi https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

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

([69]) Instrumenti za prenos, ki so na voljo v skladu s členom 46(2) in (3) UK GDPR, so pravno zavezujoči in izvršljivi instrumenti med javnimi organi ali telesi, zavezujoča poslovna pravila v skladu s členom 47 UK GDPR, standardne klavzule o varstvu podatkov, določene v predpisih, ki jih sprejme pristojni minister, ali dokumentu, ki ga izda informacijska komisija, odobreni kodeks ravnanja in odobreni mehanizem certificiranja.

(47) V zvezi s predpisi o odobritvi prenosov je bilo doslej sprejetih dvoje novih predpisov, ki odražajo sklepe o ustreznosti, veljavne tudi v Uniji, tj. za prenose v Republiko Korejo in za prenose komercialnim subjektom, ki so pristopili k razširitvi uporabe okvira za varstvo zasebnosti podatkov med EU in ZDA na Združeno kraljestvo. Predpisi o ustreznosti za Republiko Korejo ([70]) so začeli veljati 19. decembra 2022 in omogočajo prenos osebnih podatkov iz Združenega kraljestva v Republiko Korejo. Razširitev uporabe okvira za varstvo zasebnosti podatkov med EU in ZDA na Združeno kraljestvo, za katero so ustrezni predpisi ([71]) začeli veljati 12. oktobra 2023, omogoča prosti pretok osebnih podatkov pooblaščenim organizacijam v ZDA.

(48) Kar zadeva ustrezne zaščitne ukrepe, je Združeno kraljestvo objavilo svoja standardna pogodbena določila o varstvu podatkov, in sicer mednarodni sporazum o prenosu podatkov ([72]) in dodatek k standardnim pogodbenim določilom EU, ki sta začela veljati marca 2022. V mednarodnem sporazumu o prenosu podatkov je določen mehanizem za zagotavljanje ustreznih zaščitnih ukrepov za prenos osebnih podatkov, značilen za Združeno kraljestvo, ki ima več podobnosti s standardnimi pogodbenimi določili EU. Dodatek, ki ga je izdal urad informacijskega pooblaščenca, upravljavcem in obdelovalcem podatkov v Združenem kraljestvu omogoča, da se pri mednarodnih prenosih zanašajo na standardna pogodbena določila EU v skladu z UK GDPR. Urad informacijskega pooblaščenca je izdal tudi orodje za oceno tveganja pri prenosu, da bi organizacije v Združenem kraljestvu lažje ocenile tveganja, povezana z mednarodnimi prenosi.

(49) Združeno kraljestvo je tudi poenostavilo postopek odobritve zavezujočih poslovnih pravil z novimi smernicami in novimi možnostmi za njihovo odobritev. Julija 2022 je urad informacijskega pooblaščenca objavil smernice in referenčne preglednice za pojasnitev pristopa Združenega kraljestva k zavezujočim poslovnim pravilom po brexitu, decembra 2023 pa je bil objavljen dodatek k zavezujočim poslovnim pravilom EU, da bi se zagotovilo, da so ta pravila, odobrena v okviru Unije, izvršljiva v Združenem kraljestvu ([73]).

(50) Nazadnje je Združeno kraljestvo julija 2023 postalo pridruženi član foruma za globalna čezmejna pravila o zasebnosti (Global Cross-Border Privacy Rules) ([74]). Pomembno je, da se zaradi tega članstva ne olajšajo prenosi podatkov iz Združenega kraljestva v druge člane navedenega foruma. Združeno kraljestvo je pojasnilo, da mora vsak prenos osebnih podatkov iz Združenega kraljestva v tretje države ali mednarodne organizacije izpolnjevati pogoje, določene v zakonodaji Združenega kraljestva, kot je opisano zgoraj, zlasti preskus varstva podatkov, v skladu s katerim standardi zagotovljenega varstva „niso bistveno nižji“ od tistih v skladu z UK GDPR.

(51) Kot je Komisija že pojasnila, globalna čezmejna pravila o zasebnosti ne zagotavljajo zadostne ravni varstva osebnih podatkov, ki izvirajo iz EU. Zlasti ne zagotavljajo izvršljivih pravic posameznikov ([75]). Čeprav je Združeno kraljestvo pridruženi član foruma za globalna čezmejna pravila o zasebnosti, je zato še posebej pomembno, da ta pravila niso veljaven mehanizem za prenos v skladu z zakonodajo Združenega kraljestva o varstvu podatkov. Če bi se to spremenilo, bi ogrozilo raven varstva, trenutno zagotovljeno za osebne podatke, ki se iz EU prenašajo v Združeno kraljestvo. Zato bo Komisija še naprej pozorno spremljala nadaljnji razvoj v zvezi s tem.

([70]) Na voljo na povezavi: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Na voljo na povezavi: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Na voljo na povezavi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) Urad informacijskega pooblaščenca je po brexitu prejel številne vloge za zavezujoča poslovna pravila Združenega kraljestva. Številnih odobrenih zavezujočih poslovnih pravil ni bilo več mogoče uporabljati, saj so se lahko po brexitu še naprej uporabljala le tista, v postopku odobritve katerih je sodeloval urad informacijskega pooblaščenca, vendar so morali njihovi imetniki uradu informacijskega pooblaščenca predložiti posodobljeno dokumentacijo o teh pravilih, skladno z UK GDPR.

([74]) Forum za globalna čezmejna pravila o zasebnosti sestavljajo Združene države Amerike, Kanada, Japonska, Republika Koreja, Filipini, Singapur, Tajvan in Avstralija, Mavricij, Mednarodni finančni center Dubaj in Bermudi pa so tako kot Združeno kraljestvo pridruženi člani.

([75]) Glej na primer primerjalno analizo, ki so jo izvedli organi za varstvo podatkov skupine G7 o ključnih elementih certifikacijske sheme Splošne uredbe o varstvu podatkov in sistema čezmejnih pravil o zasebnosti in ki je pokazala „opazne razlike“ med sistemi, vključno z „izvršljivostjo in pravnimi sredstvi, pravili glede neodvisnega nadzora in vladnega dostopa“. Na voljo na povezavi: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Glej uvodno izjavo 79 Izvedbenega sklepa Komisije (EU) 2019/419 z dne 23. januarja 2019 v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov na Japonskem na podlagi zakona o varstvu osebnih informacij (UL L 76, 19.3.2019, str. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Glej tudi mnenje št. 02/2014 Delovne skupine za varstvo podatkov iz člena 29 o referenčnem dokumentu za zahteve za zavezujoča poslovna pravila, predložena nacionalnim organom za varstvo podatkov v EU, in pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov, predložena odgovornim zastopnikom skupine APEC za pravila o varovanju zasebnosti pri čezmejnem prenosu podatkov z dne 6. marca 2014.

2.2.6 *Avtomatizirano sprejemanje odločitev*

(52) Čeprav je več elementov pravil o avtomatiziranem sprejemanju odločitev, ocenjenih v uvodni izjavi 54 Izvedbenega sklepa (EU) 2021/1772, ohranjenih, so bili z zakonom o podatkih (uporaba in dostop) spremenjeni nekateri vidiki teh pravil.

(53) Prvič, novouvedeni člen 22B UK GDPR določa splošno prepoved obdelave posebnih vrst osebnih podatkov (opredeljenih v členu 9(1) UK GDPR) za odločitve, ki temeljijo zgolj na avtomatizirani obdelavi in imajo pravne ali podobno pomembne učinke za posameznika, na katerega se nanašajo osebni podatki. Vendar določa tri izjeme od te prepovedi, in sicer če je posameznik, na katerega se nanašajo osebni podatki, izrecno privolil v tako obdelavo ali če je odločitev nujna za sklenitev ali izvajanje pogodbe med upravljavcem in posameznikom, na katerega se nanašajo osebni podatki, ali če obdelavo predpisuje ali dovoljuje zakon. Pri zadnjih dveh izjemah mora biti avtomatizirana obdelava potrebna iz razlogov bistvenega javnega interesa ([76]). Splošna prepoved se ne uporablja za pomembne odločitve, ki temeljijo na avtomatizirani obdelavi vrst podatkov, ki niso posebne vrste podatkov.

(54) Poleg tega novi člen 22A UK GDPR pojasnjuje opredelitev odločitve, ki „temelji zgolj na avtomatizirani obdelavi“, tako da določa, da v postopku sprejemanja take odločitve ni smiselnega človekovega posredovanja. Pomembno je, da morajo upravljavci oceniti, v kolikšni meri k odločitvi prispeva oblikovanje profilov, da bi ugotovili, ali je bilo človekovo posredovanje smiselno. Člen 22A UK GDPR prav tako pojasnjuje, da je „pomembna odločitev“ odločitev, ki ima pravne učinke ali podobno pomemben vpliv na posameznika, na katerega se nanašajo osebni podatki ([77]).

(55) Drugič, novouvedeni člen 22C UK GDPR določa, da morajo upravljavci poskrbeti za zagotovitev ustreznih zaščitnih ukrepov za vsako pomembno odločitev, ki v celoti ali delno temelji na osebnih podatkih in izključno na avtomatizirani obdelavi (vključno z obdelavo osebnih podatkov, ki niso posebne vrste podatkov). S temi zaščitnimi ukrepi je treba posamezniku, na katerega se nanašajo osebni podatki, med drugim zagotoviti informacije o postopku odločanja, in mu omogočiti, da lahko odločitev izpodbija in poda stališča, ter zagotoviti, da si lahko zagotovi človekovo posredovanje v postopku sprejemanja odločitev ([78]).

(56) Novouvedeni člen 22D UK GDPR pristojnega ministra nazadnje pooblašča, da sprejme sekundarno zakonodajo, v kateri se opredeli, kaj je oziroma kaj ni smiselno človekovo posredovanje in katere odločitve se štejejo oziroma se ne štejejo za odločitve, ki imajo podobne pomembne učinke na posameznike, na katere se nanašajo osebni podatki. Pooblašča ga tudi, da sprejme sekundarno zakonodajo, s katero se (i) dodajo novi zaščitni ukrepi, (ii) naložijo zahteve, ki dopolnjujejo obstoječe zaščitne ukrepe, in (iii) opredelijo ukrepi, ki ne upoštevajo zaščitnih ukrepov ([79]). Pomembno je, da se mora pristojni minister pred sprejetjem predpisov v skladu s členom 22D UK GDPR posvetovati z uradom informacijskega pooblaščenca ([80]), pri čemer predpisi ne smejo spreminjati člena 22C UK GDPR ([81]), glede njih pa se izvede postopek pozitivne potrditve ([82]), kar pomeni, da jih morata potrditi oba domova parlamenta Združenega kraljestva, preden se lahko sprejmejo.

(57) Čeprav je bil z zakonom o podatkih (uporaba in dostop) na ta način spremenjen okvir za avtomatizirano sprejemanje odločitev, je treba opozoriti, da v pravnem okviru Združenega kraljestva za avtomatizirano sprejemanje odločitev še naprej veljajo ključni zaščitni ukrepi, v skladu s katerimi se pravica do človeškega posredovanja zahteva v vseh primerih pomembnih odločitev, ki temeljijo zgolj na avtomatizirani obdelavi, tj. na obdelavi občutljivih in neobčutljivih osebnih podatkov ([83]). Kot je Komisija ugotovila v prejšnjih sklepih

([76]) Člen 22B UK GDPR, kot je bil uveden s členom 80(1) zakona o podatkih (uporaba in dostop).
([77]) Člen 22A UK GDPR, kot je bil uveden s členom 80(1) zakona o podatkih (uporaba in dostop).
([78]) Člen 22C UK GDPR, kot je bil uveden s členom 80(1) zakona o podatkih (uporaba in dostop).
([79]) Člen 22D UK GDPR, kot je bil uveden s členom 80(1) zakona o podatkih (uporaba in dostop). Glede vseh predpisov, sprejetih na podlagi teh pooblastil, se izvede postopek pozitivne potrditve, s katerim se zagotavlja parlamentarni nadzor. S predpisi se ne morejo spremeniti zahteve iz člena 22C.
([80]) Člen 182(2) zakona o varstvu podatkov iz leta 2018.
([81]) Člen 22D(4) UK GDPR.
([82]) Člen 22D(5) UK GDPR.
([83]) Člen 22C(2) UK GDPR, kot je bil uveden s členom 80(1) zakona o podatkih (uporaba in dostop).

o ustreznosti ([84]), posebna pravila o avtomatiziranem sprejemanju odločitev iz UK GDPR poleg tega verjetno ne bodo vplivala na raven varstva osebnih podatkov, ki se prenašajo iz Unije v Združeno kraljestvo. Glede osebnih podatkov, zbranih v Uniji, velja, da vse odločitve, ki temeljijo na samodejni obdelavi, po navadi sprejme upravljavec v Uniji (ki ima neposredno razmerje z zadevnim posameznikom, na katerega se nanašajo osebni podatki), zato se zanje uporabljajo pravila iz Uredbe (EU) 2016/679.

### 2.3 **Nadzor in izvrševanje**

#### 2.3.1 *Neodvisen nadzor*

(58) V Združenem kraljestvu nadzor in uveljavljanje skladnosti z okvirom varstva podatkov še naprej izvaja neodvisni nadzorni organ za varstvo podatkov, kot je analizirano v uvodnih izjavah 85 do 91 Izvedbenega sklepa (EU) 2021/1772. Z zakonom o podatkih (uporaba in dostop) je prenovljena struktura upravljanja tega organa z ustanovitvijo pravne osebe, tj. informacijske komisije, ki bo nadomestila urad informacijskega pooblaščenca, ki je bil oblikovan kot „corporation sole“ (ločen enoosebni pravni subjekt).

(59) Z izvedbo ukrepov upravljanja, določenih v zakonu o podatkih (uporaba in dostop), bo ukinjen urad informacijskega pooblaščenca, funkcije, osebje in premoženje pa bodo z urada informacijskega pooblaščenca preneseni na nov organ, tj. informacijsko komisijo. Informacijsko komisijo sestavljajo izvršni in neizvršni člani ([85]). Navedeni zakon določa tudi, da informacijski pooblaščenec prevzame funkcijo predsednika informacijske komisije, ki je eden od neizvršnih članov ([86]). Nadalje določa, da se, kolikor je to ustrezno zaradi prenosa funkcij, sklici na informacijskega pooblaščenca v vseh predpisih ali drugih dokumentih (ne glede to, kdaj so sprejeti ali izdani) štejejo za sklice na informacijsko komisijo. Komisija lahko za opravljanje svojih funkcij ustanovi odbore, pri čemer lahko funkcije prenese na člana, zaposlenega ali odbor komisije ([87]), ter lahko uredi svoj poslovnik in poslovnike odborov, vključno glede sklepčnosti in odločanja z večino glasov. Ti poslovniki morajo biti javno objavljeni ([88]).

(60) Pomembno je, da za neodvisnost informacijske komisije veljajo enaki zaščitni ukrepi, tudi glede pravil o imenovanju in razrešitvi njenega predsednika, kot so bili ocenjeni v uvodnih izjavah 87 do 90 Izvedbenega sklepa (EU) 2021/1772 ([89]). Podobni zaščitni ukrepi veljajo tudi za druge neizvršne člane informacijske komisije. Natančneje, predsednika informacijske komisije imenuje kralj na priporočilo pristojnega ministra. Izbran je na podlagi dosežkov ter na podlagi poštenega in odprtega postopka izbire ([90]). Druge neizvršne člane imenuje pristojni minister po posvetovanju s predsednikom. Kandidate je mogoče priporočiti za imenovanje ali imenovati le, če so izbrani na podlagi dosežkov po poštenem in odprtem postopku izbire ter če je pristojni minister prepričan, da niso v nasprotju interesov ([91]). Izvršni člani so zaposleni v informacijski komisiji pod pogoji, ki jih določijo neizvršni člani ([92]). Izvršnega direktorja imenujejo predsednik in drugi neizvršni člani po posvetovanju s pristojnim ministrom. Tudi izvršni člani so lahko imenovani le, če so izbrani na podlagi dosežkov po poštenem in odprtem postopku izbire ([93]).

(61) Predsednika lahko s funkcije razreši le kralj na podlagi nagovora obeh domov parlamenta in le, če je pristojni minister domu predložil poročilo, iz katerega izhaja, da je po njegovem mnenju predsednik kriv hujše kršitve dolžnega ravnanja uradnih oseb, je v nasprotju interesov, ni izpolnil posebnih zahtev po informacijah glede

([84]) Glej na primer uvodno izjavo 94 Izvedbenega sklepa (EU) 2019/419 ter uvodno izjavo 81 Izvedbenega sklepa Komisije (EU) 2022/254 z dne 17. decembra 2021 v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Republiki Koreji na podlagi zakona o varstvu osebnih podatkov (UL L 44, 24.2.2022, str. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) Točka 3(1) dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([86]) Členi 117, 118, 119 in 120 zakona o podatkih (uporaba in dostop) skupaj z dodatkom 14 k temu zakonu.
([87]) Točki 13 in 14 dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([88]) Točka 16 dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([89]) Člen 52 UK GDPR in dodatek 12A k zakonu o varstvu podatkov iz leta 2018, kot je bil uveden s členom 114A predloga zakona o podatkih (uporaba in dostop).
([90]) Točka 5(1) in točka 3(2) dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([91]) Točka 3(2) ter točki 5 in 6 dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([92]) Točka 11 dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([93]) Točka 5(2) dodatka 12A k zakonu o varstvu podatkov iz leta 2018.

morebitnega nasprotja interesov ali ni sposoben, primeren ali pripravljen opravljati svoje funkcije ([94]). Neizvršne člane lahko minister razreši s funkcije le, če je prepričan, da so izpolnjeni posebni pogoji, določeni v zakonodaji. Ti vključujejo nasprotje interesov, hujšo kršitev dolžnega ravnanja uradnih oseb ali nesposobnost, nepripravljenost ali neprimernost za opravljanje svojih funkcij. Kar zadeva dodatne zaščitne ukrepe, mora pristojni minister svojo odločitev o razrešitvi javno objaviti, člana pa obvestiti o razlogih zanjo ([95]).

(62) Glavna vloga informacijske komisije bo še naprej spremljanje in izvajanje okvira varstva podatkov v Združenem kraljestvu, „da se zaščitijo temeljne pravice in svoboščine“ posameznikov ([96]). Kar zadeva nalogo informacijske komisije, da zagotovi ustrezno raven varstva osebnih podatkov, zakon o podatkih (uporaba in dostop) od komisije izrecno zahteva, da upošteva interese posameznikov, na katere se nanašajo osebni podatki, upravljavcev in drugih ter zadeve splošnega javnega interesa in da vzbuja zaupanje javnosti v obdelavo osebnih podatkov ([97]). Ti cilji so prav tako navedeni v uvodni izjavi 7 Uredbe (EU) 2016/679.

(63) Poleg tega zakon o podatkih (uporaba in dostopa) določa, da mora informacijska komisija pri opravljanju nalog v skladu z zakonodajo o varstvu podatkov upoštevati spodbujanje inovacij in konkurence, pomen preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj, potrebo po varovanju javne in nacionalne varnosti ter posebne potrebe, povezane z zaščito otrok ([98]). Zakonodaja EU o varstvu podatkov prav tako priznava potrebo po uskladitvi varstva osebnih podatkov z več drugimi temeljnimi pravicami in cilji, kot so gospodarski in socialni napredek, varnost in pravica ter svoboda gospodarske pobude ([99]).

2.3.2 *Izvrševanje, vključno s sankcijami*

(64) Pooblastila in naloge informacijske komisije še naprej ustrezajo pooblastilom in nalogam nadzornih organov držav članic za varstvo podatkov v skladu z ustreznimi členi Uredbe (EU) 2016/679 ([100]), kot je ocenjeno v uvodnih izjavah 91 do 95 Izvedbenega sklepa (EU) 2021/1772.

(65) Z zakonom o podatkih (uporaba in dostop) so bila uvedena določena pojasnila glede izvajanja nekaterih od teh pooblastil.

(66) Zakon o podatkih (uporaba in dostop) po eni strani pojasnjuje, da lahko informacijska komisija pri uporabi pooblastila za informativno obvestilo zahteva posebne „dokumente“ in „informacije“ ([101]). Po drugi strani pa uvaja dve novi preiskovalni pooblastili za informacijsko komisijo: novo pooblastilo, da zahteva poročilo ([102]), in novo pooblastilo, da v primeru domnevne kršitve UK GDPR ali zakona o varstvu podatkov iz leta 2018 upravljavcem izda „obvestila o razgovoru“ ([103]).

([94]) Točka 7(6) in (7) dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([95]) Točka 9(6), (7), (8) in (9) dodatka 12A k zakonu o varstvu podatkov iz leta 2018.
([96]) Člen 51 UK GDPR.
([97]) Člen 91 zakona o podatkih (uporaba in dostop), s katerim je bil uveden člen 120A zakona o varstvu podatkov iz leta 2018.
([98]) Člen 91 zakona o podatkih (uporaba in dostop), s katerim je bil uveden člen 120B zakona o varstvu podatkov iz leta 2018. Z zakonom o podatkih (uporaba in dostop) je dalje v zakon o varstvu podatkov iz leta 2018 uveden nov člen 120C, s katerim se od informacijske komisije zahteva, da pripravi in objavi strategijo, ki med drugim izraža, kako bo obravnavala navedena vprašanja in kako bo pri izvajanju regulativnih funkcij upoštevala spodbujanje gospodarske rasti.
([99]) Glej zlasti uvodni izjavi 2 in 4 ter člen 23 Uredbe (EU) 2016/679.
([100]) Člena 57 in 58 UK GDPR.
([101]) Člen 97 zakona o podatkih (uporaba in dostop), ki spreminja člen 142 zakona o varstvu podatkov iz leta 2018. Vidiki vpliva tehnologije in vloge varstva podatkov pri ustvarjanju zaupanja v digitalno gospodarstvo so del dejavnosti regulativnih organov za varstvo podatkov v Združenem kraljestvu in EU. Glej na primer letno poročilo Evropskega odbora za varstvo podatkov za leto 2024, stran 12, v katerem je navedeno: „EOVP je dinamičen in sodelovalen organ, ki ima ključno vlogo pri zagotavljanju dosledne uporabe zakonodaje o varstvu podatkov po vsej Evropi. Kot namestnik predsednice menim, da je varuh pravic posameznikov do zasebnosti, ki spretno usklajuje potrebe po inovacijah in gospodarski rasti.“
([102]) Člen 98 zakona o podatkih (uporaba in dostop), ki spreminja člen 146 zakona o varstvu podatkov iz leta 2018.
([103]) Člen 100 zakona o podatkih (uporaba in dostop), s katerim je bil uveden člen 148A zakona o varstvu podatkov iz leta 2018.

(67) Informacijska komisija je pri izvajanju teh pooblastil od začetka veljavnosti Izvedbenega sklepa (EU) 2021/1772 obravnavala približno 40 000 pritožb posameznikov, na katere se nanašajo osebni podatki, na leto, kar je podobno številu pritožb, obravnavanih, ko je bilo Združeno kraljestvo še del Unije in je uporabljalo Uredbo (EU) 2016/679 ([104]). Urad informacijskega pooblaščenca je opravil tudi preiskave po uradni dolžnosti, ki so zajemale širok nabor sektorskih vprašanj in vprašanj skladnosti, vključno s pravicami posameznikov, na katere se nanašajo osebni podatki ([105]).

(68) Kar zadeva izvršilne ukrepe, je pooblaščenec od začetka veljavnosti Izvedbenega sklepa (EU) 2021/1772 izdal 120 opominov, 32 obvestil o predložitvi informacij, 3 obvestila o preverjanju, 12 obvestil o izvršitvi, 2 opozorili in 12 glob ([106]). To vključuje več pomembnih denarnih kazni, izrečenih na podlagi UK GDPR in zakona o varstvu podatkov iz leta 2018. Informacijski pooblaščenec je na primer aprila 2023 platformi družbenih medijev naložil globo v višini 12,7 milijona GBP zaradi zlorabe podatkov otrok ([107]). Marca 2025 je bila podjetju za programsko opremo naložena globa v višini 3,07 milijona GBP zaradi varnostnih pomanjkljivosti, ki so ogrozile osebne podatke več kot 70 000 ljudi ([108]). Informacijski pooblaščenec je pred kratkim, junija 2025, podjetju za genetsko testiranje naložil globo v višini 2,31 milijona GBP, ker po obsežnem kibernetskem napadu leta 2023 ni izvedlo ustreznih varnostnih ukrepov za zaščito osebnih podatkov uporabnikov iz Združenega kraljestva ([109]).

(69) Urad informacijskega pooblaščenca je od sprejetja Izvedbenega sklepa (EU) 2021/1772 pripravil in objavil tudi znatno število smernic, mnenj in drugih usmerjevalnih dokumentov, v katerih je pojasnjena uporaba pravil o varstvu podatkov na pomembnih področjih, kot so prepoznavanje obrazov, pravičnost v umetni inteligenci, podatki otrok, neposredno trženje, video nadzor, pravica dostopa, preglednost v zdravstvenem in socialnem varstvu itd., za različne ciljne skupine, vključno z malimi in srednjimi podjetji, posebnimi subjekti, kot so šole, vrtci ali majhni javni organi, pa tudi za podjetja na splošno, širšo javnost ali posameznike, na katere se nanašajo osebni podatki ([110]).

## 3. POMEMBNE SPREMEMBE V ZVEZI Z DOSTOPOM DO OSEBNIH PODATKOV, KI JIH IZ EVROPSKE UNIJE PRENESEJO JAVNI ORGANI V ZDRUŽENEM KRALJESTVU, IN NJIHOVO UPORABO

### 3.1 Splošni pravni okvir

(70) Združeno kraljestvo je še naprej član Sveta Evrope, spoštuje Evropsko konvencijo o človekovih pravicah (EKČP) in priznava pristojnost Evropskega sodišča za človekove pravice. Zato zanj še naprej veljajo obveznosti, določene v mednarodnem pravu, kot so opisane v uvodnih izjavah 116 do 119 Izvedbenega sklepa (EU) 2021/1772, ki njegov sistem vladnega dostopa do osebnih podatkov oblikujejo na podlagi načel, zaščitnih ukrepov in pravic posameznikov, enakih načelom, zaščitnim ukrepom in pravicam posameznikov, ki veljajo za 27 držav članic kot pogodbenic EKČP in ki se v veliki meri kažejo v ustrezni sodni praksi Sodišča Evropske unije.

(71) Posebni zaščitni ukrepi in pravice za varstvo podatkov so še naprej zagotovljeni z zakonom o varstvu podatkov iz leta 2018, če podatke obdelujejo javni organi Združenega kraljestva, vključno z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter organi nacionalne varnosti, kot je analizirano v uvodnih izjavah 121 do 132 Izvedbenega sklepa (EU) 2021/1772. Z zakonom o podatkih (uporaba in dostop) so bile uvedene le omejene in ciljne spremembe tistih delov zakona o varstvu podatkov iz leta 2018, ki določajo pravila za obdelavo osebnih podatkov v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (del 3 zakona o varstvu podatkov iz leta 2018) in nacionalne varnosti (del 4 zakona o varstvu podatkov iz leta 2018).

([104]) Letna poročila informacijskega pooblaščenca za obdobja 2021–2022, 2022–2023 in 2023–2024. Glej tudi Izvedbeni sklep (EU) 2021/1772, uvodna izjava 96.

([105]) Letno poročilo informacijskega pooblaščenca za obdobje 2023–2024, stran 41.

([106]) Letna poročila informacijskega pooblaščenca za obdobja 2021–2022, 2022–2023 in 2023–2024.

([107]) Več informacij o teh in drugih izvršilnih ukrepih je na voljo na spletišču urada informacijskega pooblaščenca na naslednji povezavi: https://ico.org.uk/action-weve-taken/enforcement/.

([108]) Več informacij je na voljo na naslednji povezavi: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

([109]) Več informacij je na voljo na naslednji povezavi: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

([110]) Na voljo na povezavi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) Kar zadeva 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, del 3 zakona o varstvu podatkov iz leta 2018 še naprej določa načela, pravice in obveznosti, podobne načelom, pravicam in obveznostim iz Direktive (EU) 2016/680 ([111]).

(73) Komisija je zlasti na isti datum sprejela ta sklep in sklep 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 za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, zagotavlja raven varstva, ki je v osnovi enakovredna tisti, ki jo zagotavlja Direktiva (EU) 2016/680.

(74) Z zakonom o podatkih (uporaba in dostop) so bile spremenjene in združene obstoječe izjeme iz dela 3 zakona o varstvu podatkov iz leta 2018, ki so na voljo pristojnim organom za namene nacionalne varnosti. Izjema zaradi nacionalne varnosti pristojnim organom omogoča, da ne uporabijo nekaterih določb iz dela 3 zakona o varstvu podatkov iz leta 2018, če je izvzetje od zadevne določbe potrebno za zaščito nacionalne varnosti ([112]). Ta izjema odraža izjeme zaradi nacionalne varnosti, določene za obdelavo osebnih podatkov na podlagi UK GDPR (člen 26 zakona o varstvu podatkov iz leta 2018) in v delu 4 zakona o varstvu podatkov iz leta 2018 (člen 110 zakona o varstvu podatkov iz leta 2018).

(75) Za izjemo zaradi nacionalne varnosti veljajo enake omejitve in zaščitni ukrepi kakor za izjeme na podlagi UK GDPR in dela 4 zakona o varstvu podatkov iz leta 2018, kot je analizirano v uvodnih izjavah 64 do 67 in 126 Izvedbenega sklepa (EU) 2021/1772. Ta izjema se lahko uporabi le, če in kolikor je to potrebno za zaščito nacionalne varnosti. Ker ne gre za splošno izjemo, jo mora upravljavec obravnavati in se nanjo sklicevati za vsak primer posebej ([113]). Dalje, izjemo je treba vedno uporabljati v skladu s standardi človekovih pravic (ki temeljijo na zakonu o človekovih pravicah iz leta 1998 in Evropski konvenciji o človekovih pravicah), po katerih bi moral biti v demokratični družbi vsak poseg v pravice do zasebnosti potreben in sorazmeren ([114]). To je potrjeno tudi v smernicah urada informacijskega pooblaščenca o uporabi izjem zaradi nacionalne varnosti ([115]).

(76) Dalje, na podlagi sprememb, uvedenih z zakonom o podatkih (uporaba in dostop) ([116]), je lahko posebna dejavnost obdelave, ki jo izvajajo organi, pristojni za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, urejena tudi z določbami dela 4 zakona o varstvu podatkov iz leta 2018, ki se običajno uporablja le za obdelavo podatkov, ki jo izvajajo organi za nacionalno varnost.

([111]) S členom 69 zakona o podatkih (uporaba in dostop) so v zakon o varstvu podatkov iz leta 2018 kot nova člena 33(1A) in 40A dodani opredelitev privolitve in pogoji za sklicevanje na privolitev, kakor so določeni v členu 4(11) in členu 7 UK GDPR (ki odražata ustrezne določbe iz Uredbe (EU) 2016/679), s čimer so pojasnjeni pojem privolitve in pogoji za sklicevanje na privolitev, kadar jo pristojni organi uporabljajo kot pravno podlago za obdelavo osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Poleg tega člen 71(7) in (8) zakona o podatkih (uporaba in dostop) nekoliko pojasnjuje besedilo člena 36(1) zakona o varstvu podatkov iz leta 2018. Nazadnje, kadar je ustrezno, se spremembe UK GDPR z zakonom o podatkih (uporaba in dostop), kot so opisane v oddelku 2, odražajo tudi v delu 3 zakona o varstvu podatkov iz leta 2018; glej na primer člen 74(2) do (5) o obdelavi občutljivih podatkov, člen 76(4) do (6) glede rokov za odgovor na zahteve posameznika, na katerega se nanašajo osebni podatki, člen 78(2) in (3) glede iskanj v odgovor na zahteve posameznikov, na katere se nanašajo osebni podatki, ter člen 80(3) do (5) o avtomatiziranem sprejemanju odločitev.

([112]) Člen 78A(1) zakona o varstvu podatkov iz leta 2018, kot je bil uveden s členom 88 zakona o podatkih (uporaba in dostop). Izjema v skladu s členom 78A(2) do (4) zakona o varstvu podatkov iz leta 2018 omogoča, da se ne uporabijo načela varstva podatkov (razen načela zakonitosti ter pogojev in zaščitnih ukrepov za obdelavo občutljivih podatkov), pravice posameznikov, obveznosti upravljavcev in obdelovalcev podatkov glede kršitev varnosti podatkov, nekateri deli pravil o mednarodnih prenosih podatkov ter nekatera pooblastila informacijskega pooblaščenca za vstop zaradi izvajanja inšpekcijskih pregledov in sprejemanja izvršilnih ukrepov.

([113]) Glej sodbo Baker/Secretary of State for the Home Department [2001] UKIT NSA2 (v nadaljnjem besedilu: Baker/Secretary of State).

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

([115]) Glej smernice urada informacijskega pooblaščenca o izjemi zaradi nacionalne varnosti in obrambe, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Člena 89 in 90 zakona o podatkih (uporaba in dostop).

(77) Ureditev varstva podatkov za obdelavo na področju nacionalne varnosti je tako v določenih primerih razširjena tudi na obdelavo podatkov, ki jo izvajajo organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, vendar le v posebnih okoliščinah ter ob strogih pogojih in zaščitnih ukrepih, tj. če (i) je pristojni organ v predpisih, ki jih sprejme pristojni minister in za katere je potrebna parlamentarna odobritev, opredeljen kot „upravičen pristojni organ“ ([117]) in (ii) če pristojni minister z obvestilom določi posebno dejavnost obdelave, ki jo izvaja upravičen pristojni organ. Pomembno je, da je taka določitev mogoča le, če pristojni minister meni, da je določitev dejavnosti obdelave potrebna za zaščito nacionalne varnosti, tj. če organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj deluje za namene nacionalne varnosti, dejavnost obdelave pa izvaja upravičen pristojni organ kot skupni upravljavec z vsaj eno obveščevalno službo ([118]). Pristojni minister se mora pred izdajo obvestila o določitvi kot dodatni zaščitni ukrep posvetovati s pooblaščencem ([119]), besedilo obvestila je treba načeloma objaviti ([120]), oseba, na katero se obvestilo o določitvi neposredno nanaša, pa lahko zahteva sodno presojo ([121]). Zato je namen te spremembe predvsem pojasniti, da se, kadar imajo organi Združenega kraljestva pristojnosti tako na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj kakor na področju nacionalne varnosti ter obdelujejo podatke v okviru svojih pristojnosti na področju nacionalne varnosti, lahko uporablja ureditev varstva podatkov za nacionalne varnostne službe.

(78) Del 4 zakona o varstvu podatkov iz leta 2018 ureja obdelavo podatkov, ki jo izvajajo obveščevalne službe Združenega kraljestva. Še naprej določa glavna načela varstva podatkov in pogoje za obdelavo posebnih vrst podatkov, zagotavlja pravice posameznikov, na katere se nanašajo osebni podatki, zahteva vgrajeno varstvo podatkov ter ureja prenose osebnih podatkov, kot je opisano v uvodnih izjavah 125 do 132 Izvedbenega sklepa (EU) 2021/1772.

(79) Spremembe te ureditve, uvedene z zakonom o podatkih (uporaba in dostop), so omejene. Z zakonom o podatkih (uporaba in dostop) je v zvezi s pravico dostopa posameznikov, na katere se nanašajo osebni podatki, iz člena 94 zakona o varstvu podatkov iz leta 2018 uveden nov odstavek 2A, v katerem je pojasnjeno, da je posameznik, na katerega se nanašajo osebni podatki, do ustreznih informacij upravičen le, če jih lahko upravljavec zagotovi na podlagi razumnega in sorazmernega iskanja ([122]). Kot je pojasnjeno v uvodni izjavi 35, ta sprememba opredeljuje pravico dostopa na podlagi uveljavljenih pravnih standardov, pri katerih se upoštevajo tudi interesi posameznika, na katerega se nanašajo osebni podatki. Čeprav je na področju avtomatiziranega sprejemanja odločitev upravljavcem še naprej prepovedano sprejemati odločitve, ki znatno vplivajo na posameznika, na katerega se nanašajo osebni podatki, in temeljijo izključno na avtomatizirani obdelavi osebnih podatkov v zvezi z njim, razen če se taka odločitev zahteva ali je dovoljena z zakonom, če je posameznik, na katerega se nanašajo osebni podatki, privolil v odločitev, sprejeto na tej podlagi, ali če je odločitev sprejeta v okviru pogodbe ([123]), je z zakonom o podatkih (uporaba in dostop) v del 4 zakona o varstvu podatkov iz leta 2018 ([124]) uvedena enaka opredelitev pojma „odločitve, ki v celoti temeljijo na avtomatizirani obdelavi“, kot je vključena v člen 22A UK GDPR in analizirana v uvodni izjavi 53 tega sklepa.

### 3.2 **Pomembne spremembe v zvezi z dostopom javnih organov Združenega kraljestva za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj do podatkov ter njihovo uporabo s strani teh organov**

(80) Pravo Združenega kraljestva še naprej določa pomembne omejitve glede dostopa do osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in njihove uporabe ter na tem področju zagotavlja nadzorne mehanizme in mehanizme pravnih sredstev, kot je analizirano v uvodnih izjavah 134 do 174 Izvedbenega sklepa (EU) 2021/1772.

([117]) Člen 82(A1), (2A) in (4) zakona o varstvu podatkov iz leta 2018, kot je bil uveden s členom 89(2) zakona o podatkih (uporaba in dostop).

([118]) Člen 82A(1) in (2), kot je bil uveden s členom 89(3) zakona o podatkih (uporaba in dostop). Pristojni minister se mora pred izdajo obvestila o določitvi kot dodatni zaščitni ukrep posvetovati s pooblaščencem, glej novi člen 82A(8) zakona o varstvu podatkov iz leta 2018; besedilo obvestila je treba načeloma objaviti, glej novi člen 82D(1), pri čemer se upoštevajo izjeme iz novega člena 82D(3) zakona o varstvu podatkov iz leta 2018; oseba, na katero se obvestilo o določitvi neposredno nanaša, pa lahko zahteva sodno presojo, glej novi člen 82E zakona o varstvu podatkov iz leta 2018.

([119]) Člen 82A(8) zakona o varstvu podatkov iz leta 2018.

([120]) Člen 82D(1), pri čemer se upoštevajo izjeme iz novega člena 82D(3) zakona o varstvu podatkov iz leta 2018.

([121]) Člen 82E zakona o varstvu podatkov iz leta 2018.

([122]) Člen 78(4) zakona o podatkih (uporaba in dostop).

([123]) Člen 96 zakona o varstvu podatkov iz leta 2018.

([124]) V skladu z novim členom 96(4) zakona o varstvu podatkov iz leta 2018 odločitev temelji na povsem avtomatizirani obdelavi, če v postopek odločanja ni vključena možnost, da bi človek odločitev sprejel, zavrnil ali nanjo vplival. Glej člen 80(4), točka (c), zakona o podatkih (uporaba in dostop).

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

(81) Zbiranje osebnih podatkov od poslovnih subjektov v Združenem kraljestvu za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je v pravnem redu Združenega kraljestva še naprej dovoljeno na podlagi odredb o preiskavi in odredb o predložitvi dokazov, pri čemer se upoštevajo pogoji in zaščitni ukrepi iz uvodnih izjav 135 do 138 Izvedbenega sklepa (EU) 2021/1772.

(82) Poleg tega so bila z zakonom o nacionalni varnosti iz leta 2023 ([125]), katerega cilj je obravnavati grožnje nacionalni varnosti zaradi vohunjenja, sabotaže in oseb, ki delujejo v imenu tujih sil, za policijo Združenega kraljestva uvedena nova pooblastila za vstop, preiskavo in zaseg, vključno z možnostjo pridobitve osebnih podatkov, kadar obstajajo utemeljeni razlogi za sum, da bo pridobljeno gradivo, ki bo verjetno dokaz, da je bilo ali bo storjeno eno od hujših kaznivih dejanj ali dejavnosti tuje sile, ki pomenijo grožnjo, iz zakona o nacionalni varnosti iz leta 2023 ([126]). Za ta pooblastila veljajo podobni pogoji in zaščitni ukrepi, kot so bili analizirani v Izvedbenem sklepu (EU) 2021/1772 za pooblastila, ki so obstajala takrat. Zlasti mora biti njihova uporaba dovoljena z odredbo, odredbo o predložitvi dokazov ali obrazložitveno odredbo, ki jo izda neodvisen sodni organ, načeloma na zahtevo policista/preiskovalnega uradnika ([127]). Posebna zaščita obstaja za zaupno gradivo, kot so novinarsko gradivo in informacije, za katere velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko ([128]). Podobno mora izdajo odredb o razkritju ([129]), odredb o podatkih o strankah ([130]) in odredb o spremljanju računov ([131]), ki so bile prav tako uvedene z zakonom o nacionalni varnosti iz leta 2023, odobriti sodnik na zahtevo ustreznega uradnika, zanjo pa veljajo posebni pogoji in zaščitni ukrepi, vključno s tem, da se odredba zahteva v zvezi z določeno osebo za namene preiskave dejavnosti, ki pomeni grožnjo tuje sile, da bo odredba povečala učinkovitost preiskave in da se ne uporablja za pridobitev informacij, za katere velja varovanje zaupnosti sporazumevanja med odvetnikom in stranko ali ki so kako drugače izključene, kot so novinarsko gradivo in nekateri zdravstveni zapisi ([132]).

(83) Kot je pojasnjeno v uvodnih izjavah 139 do 141 Izvedbenega sklepa (EU) 2021/1772, lahko v pravnem okviru Združenega kraljestva določeni organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, na primer National Crime Agency ali metropolitanska policija (Metropolitan Police Service), uporabijo tudi ciljna preiskovalna pooblastila na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 (Investigatory Powers Act 2016) ([133]) za namene preprečevanja ali odkrivanja hudih kaznivih dejanj. Preiskovalna pooblastila, ki jih lahko uporabljajo 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) in ciljno poseganje v opremo (del 5 zakona o preiskovalnih pooblastilih iz leta 2016). Kadar pristojni minister izda obvestila o hrambi podatkov v skladu z delom 4 zakona o preiskovalnih pooblastilih iz leta 2016, lahko organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj pridobijo dostop do hranjenih komunikacijskih podatkov na podlagi pooblastil za pridobivanje komunikacijskih podatkov v skladu z delom 3 zakona o preiskovalnih pooblastilih iz leta 2016.

([125]) Na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Dodatek 2 k zakonu o nacionalni varnosti iz leta 2023. Ustrezna kazniva dejanja po zakonu o nacionalni varnosti iz leta 2023 so na primer pridobitev ali izdaja zaščitenih podatkov (člen 1), pridobitev ali izdaja poslovnih skrivnosti (člen 3), pomoč tuji obveščevalni službi (člen 4), sabotaža (člen 12) ali izvajanje določenih prepovedanih ravnanj za tujo silo z namenom povzročitve motnje (člen 13).

([127]) Glej točke 2(1), 3(1), 4(1) in 10(1) dodatka 2 k zakonu o nacionalni varnosti iz leta 2023.

([128]) Glej točke 2(4)(b), 3(4)(b) in (c), 4(4)(b) in (c) ter 10(1) dodatka 2 k zakonu o nacionalni varnosti iz leta 2023.

([129]) Uradnik lahko z odredbami o razkritju v skladu z dodatkom 3 k zakonu o nacionalni varnosti iz leta 2023 izda obvestilo, s katerim od osebe zahteva, naj zagotovi informacije, predloži dokumente in/ali odgovori na vprašanja, pomembna za preiskavo, da bi se opredelilo premoženje, povezano z dejavnostjo tuje sile, ki pomeni grožnjo, vključno s pretokom ali uporabo tega premoženja.

([130]) Uradnik lahko z odredbami o podatkih o strankah v skladu z dodatkom 4 k zakonu o nacionalni varnosti iz leta 2023 od finančne institucije zahteva predložitev vseh podatkov o stranki, ki se nanašajo na določeno osebo.

([131]) Od finančne institucije se lahko z odredbami o spremljanju računov v skladu z dodatkom 5 zahteva, da uradniku zagotovi informacije, določene v odredbi, za obdobje in na način, določena v odredbi, pri čemer obdobje ne sme biti daljše od 90 dni.

([132]) Dodatek 3, točka 2(1), dodatek 4, točka 1 in dodatek 5, točka 1, k zakonu o nacionalni varnosti iz leta 2023.

([133]) 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.

(84) Od sprejetja Izvedbenega sklepa (EU) 2021/1772 zakon o preiskovalnih pooblastilih iz leta 2016 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), še naprej zagotavlja pravno podlago ter določa veljavne omejitve in zaščitne ukrepe glede uporabe takih pooblastil, kot so opisani v Izvedbenem sklepu (EU) 2021/1772. Pomembno je, da morajo v skladu s pravnim okvirom organi za izvajanje teh pooblastil še naprej pridobiti odredbo ([134]), ki jo izda pristojni organ ([135]) in odobri neodvisni pravosodni pooblaščenec (Judicial Commissioner) ([136]) (tako imenovani postopek z dvojnim varovalom). Za pridobitev take odredbe je treba še naprej opraviti preskus potrebnosti in sorazmernosti ([137]).

(85) Od sprejetja Izvedbenega sklepa (EU) 2021/1772 so bile z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 (Investigatory Powers (Amendment) Act 2024), ki je aprila 2024 prejel kraljevo privolitev, hkrati spremenjene nekatere posebne določbe zakona o preiskovalnih pooblastilih iz leta 2016 ([138]). Če se te spremembe in druge pomembne spremembe nanašajo na pogoje, omejitve in zaščitne ukrepe v zvezi z uporabo navedenih posebnih preiskovalnih pooblastil, ki jih imajo javni organi v Združenem kraljestvu za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, kot so ocenjena v uvodnih izjavah 177 do 215 Izvedbenega sklepa (EU) 2021/1772, so analizirane v naslednjih odstavkih. V zvezi z elementi okvira Združenega kraljestva, ki z navedenim zakonom niso bili spremenjeni ali na katere druge pomembne spremembe niso vplivale, še naprej velja analiza iz Izvedbenega sklepa (EU) 2021/1772.

(86) V zvezi s ciljnim pridobivanjem in hrambo komunikacijskih podatkov ([139]) ostajajo v veljavi pogoji in zaščitni ukrepi, ki urejajo ta pooblastila, kot so bili ocenjeni v Izvedbenem sklepu (EU) 2021/1772. Z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 so bili obstoječi zaščitni ukrepi pojasnjeni tako, da je bil v člen 11 zakona o preiskovalnih pooblastilih iz leta 2016 (s katerim se vzpostavlja kaznivo dejanje nezakonitega pridobivanja komunikacijskih podatkov od telekomunikacijskega operaterja) vključen seznam primerov, ki se razumejo kot zajeti v „zakonito pooblastilo“ iz te določbe ([140]). Poleg tega je bila z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 dodatno pojasnjena opredelitev komunikacijskih podatkov v členu 261 zakona o preiskovalnih pooblastilih iz leta 2016, in sicer z izrecno navedbo, da se podatki o naročnikih štejejo za komunikacijske podatke ([141]).

([134]) 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.

([135]) 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.

([136]) Pravosodni pooblaščenci pomagajo pooblaščencu za nadzor nad izvajanjem preiskovalnih pooblastil (Investigatory Powers Commissioner), neodvisnemu organu, ki izvaja nadzorne funkcije nad uporabo preiskovalnih pooblastil s strani obveščevalnih agencij.

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

([138]) Na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) 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. Komunikacijski podatki lahko zajemajo čas in trajanje komunikacije, številko ali elektronski naslov pošiljatelja in prejemnika, včasih pa tudi lokacijo naprav, uporabljenih za telekomunikacijo, glej člen 261(5) zakona o preiskovalnih pooblastilih iz leta 2016. 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.

([140]) Na primer, kadar zadevna oseba komunikacijske podatke pridobi pri izvajanju zakonskih pooblastil zadevnega javnega organa ali kadar se ti pridobijo na podlagi sodne odločbe ali druge sodne odobritve. Člen 11(3A) zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 12(3) zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([141]) Člen 261(5A) in (5B), kot je bil uveden členom 13(3) zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

(87) Za izdajanje obvestil, s katerimi se zahteva hramba komunikacijskih podatkov ([142]), še naprej veljajo omejitve in zaščitni ukrepi, kot so bili opisani v uvodnih izjavah 208 in 209 Izvedbenega sklepa (EU) 2021/1772, zlasti zahteve glede potrebnosti in sorazmernosti ter pridobitve odobritve neodvisnega pravosodnega pooblaščenca. Čeprav je bila z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 uvedena možnost podaljšanja takih obvestil, pa za vsako podaljšanje veljajo enaki pogoji potrebnosti in sorazmernosti ter odobritve pravosodnega pooblaščenca ([143]).

(88) Kar zadeva komunikacijske podatke, je bila z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 spremenjena tudi opredelitev telekomunikacijskega operaterja, tj. morebitnih naslovnikov obvestila o hrambi. Ta opredelitev zdaj vključuje vsako osebo, ki „nadzoruje ali zagotavlja telekomunikacijski sistem, ki (i) ni (v celoti ali delno) v Združenem kraljestvu ali se nadzoruje iz Združenega kraljestva in (ii) ga druga oseba uporablja za ponujanje ali zagotavljanje telekomunikacijskih storitev osebam v Združenem kraljestvu“ ([144]). Pomembno je, da je kljub spremenjeni opredelitvi še naprej vedno potrebna tesna povezava s trgom Združenega kraljestva. S spremembo je tako pojasnjeno, da so velika podjetja z zapletenimi podjetniškimi strukturami v celoti zajeta z zakonom o preiskovalnih pooblastilih iz leta 2016, ne da bi bila opredelitev razširjena na ponudnike telekomunikacijskih storitev, ki niso namenjene osebam v Združenem kraljestvu . To potrjujejo tudi pojasnjevalne opombe k zakonu o preiskovalnih pooblastilih (sprememba) iz leta 2024, v katerih je navedeno, da se s to spremembo na področje uporabe ustreznih pooblastil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 ([145]) ne vključujejo dodatna podjetja, pač pa ima pravzaprav pojasnjevalno nalogo.

(89) Z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 so bile nazadnje uvedene nekatere ciljne spremembe postopka za izdajo odredb, tudi v zvezi s ciljnim prestrezanjem in ciljnim poseganjem v opremo, tj. pooblastili, ki jih lahko uporabljajo tudi določeni organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v Združenem kraljestvu za namene preprečevanja ali odkrivanja hudih kaznivih dejanj. Spremembe se nanašajo le na poseben primer, ko se ta pooblastila uporabljajo za pridobivanje sporočil osebe, ki je član zadevnega zakonodajnega organa, oziroma zasebnih informacij o taki osebi ([146]). Čeprav lahko odredbe v zvezi s ciljnim prestrezanjem in poseganjem v opremo običajno izda pristojni minister in odobri pravosodni pooblaščenec (glej uvodne izjave 186 do 196 in 210 do 215 Izvedbenega sklepa (EU) 2021/1772), pa je v skladu s členoma 26 in 111 zakona o preiskovalnih pooblastilih potrebna dodatna odobritev predsednika vlade, kadar se odredba nanaša na poslanca ali drugega člana zadevnega zakonodajnega organa (t. i. postopek s trojnim varovalom). Zakon o preiskovalnih pooblastilih (sprememba) iz leta 2024 zdaj predsedniku vlade omogoča, da imenuje pet pristojnih ministrov, ki bodo pooblaščeni za izvajanje pooblastil predsednika vlade za odobritev teh odredb, če je odobritev nujna in je predsednik vlade ne more dati, ker tega ni zmožen iz zdravstvenih razlogov ali ker nima dostopa do varne komunikacije. Pomembno je, da še naprej veljajo omejitve in zaščitni ukrepi v zvezi z izdajo teh odredb, kot so opisani v navedenih uvodnih izjavah Izvedbenega sklepa (EU) 2021/1772.

### 3.2.2 *Nadaljnja uporaba zbranih informacij*

(90) 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), še naprej veljajo pogoji, analizirani v uvodnih izjavah 142 do 156 Izvedbenega sklepa (EU) 2021/1772.

([142]) Namen izdaje takih obvestil o hrambi podatkov v skladu s členi 87 do 89 zakona o preiskovalnih pooblastilih iz leta 2016 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. 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.

([143]) Člen 94A zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 20(4) zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([144]) Člen 261(10), točka (c), zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 19 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([145]) Pojasnjevalne opombe k zakonu o preiskovalnih pooblastilih (sprememba) iz leta 2024, točka 359, na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Glej člena 26 in 111 zakona o preiskovalnih pooblastilih iz leta 2016.

(91) Kar zadeva poseben položaj nadaljnjih prenosov iz Združenega kraljestva v Združene države Amerike, je sporazum 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 (v nadaljnjem besedilu: sporazum med Združenim kraljestvom in ZDA) ([147]), ki je bil sklenjen oktobra 2019, začel veljati in se izvaja od oktobra 2022. V skladu s sporazumom med Združenim kraljestvom in ZDA bi lahko za podatke, prenesene iz EU k ponudnikom storitev v Združenem kraljestvu, veljale odredbe o predložitvi dokazov, ki jih izdajo pristojni organi ZDA za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter ki bi se uporabljale v Združenem kraljestvu.

(92) Pomembno je, da se še naprej uporabljajo pogoji in zaščitni ukrepi, na podlagi katerih se lahko take odredbe izdajo in izvršijo, kot je ocenjeno v uvodni izjavi 154 Izvedbenega sklepa (EU) 2021/1772. Podatki, pridobljeni na podlagi Sporazuma, so zlasti zaščiteni enako kot na podlagi posebnih zaščitnih ukrepov, zagotovljenih s tako imenovanim krovnim sporazumom med EU in ZDA ([148]), ki so vsi vključeni v sporazum med Združenim kraljestvom in ZDA s sklicem na smiselno podlago ([149]).

(93) Združeno kraljestvo je od sprejetja Izvedbenega sklepa (EU) 2021/1772 navedlo, da je pojasnilo, tudi s sodelovanjem z ustreznimi partnerji v okviru izvajanja sporazuma med Združenim kraljestvom in ZDA, kako so posebni zaščitni ukrepi iz krovnega sporazuma, ki so bili zasnovani za sodelovanje med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, prilagojeni in uporabljeni za posebne prenose, zajete z navedenim sporazumom. Zlasti je pojasnilo, da se določbe krovnega sporazuma, ki predvidevajo vlogo ustreznega pristojnega organa (ki ne obstaja v primeru neposrednega sodelovanja med ponudnikom storitev iz Združenega kraljestva in organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v ZDA), smiselno razlagajo tako, da se nanašajo na imenovani organ (kot je opredeljen v sporazumu med Združenim kraljestvom in ZDA) ([150]) ustrezne pogodbenice.

(94) Združeno kraljestvo je na primer glede uradnega obvestila o incidentu na področju informacijske varnosti v skladu s členom 10 krovnega sporazuma med EU in ZDA, v skladu s katerim je treba poslati obvestilo pristojnemu organu, ki podatke prenese, pojasnilo, da se ta določba uporablja smiselno, kar pomeni, da je treba obvestilo poslati imenovanemu organu tiste pogodbenice, iz katere so bili podatki preneseni.

(95) Združeno kraljestvo je v zvezi z dovoljenjem pristojnega organa, ki podatke prenese, pred vsakim nadaljnjim prenosom osebnih podatkov v skladu s členom 7 krovnega sporazuma pojasnilo, da bo to določbo uporabljalo smiselno, kar pomeni, da bo moral imenovani organ pogodbenice, iz katere so bili podatki preneseni, odobriti vsak nadaljnji prenos.

(96) Glede obveznosti iz člena 8 krovnega sporazuma o ohranjanju kakovosti in celovitosti podatkov bi bil na podlagi smiselne razlage določbe v primeru kakršnih koli težav v zvezi s kakovostjo in celovitostjo podatkov imenovani organ pogodbenice, ki podatke prejme, odgovoren za vzpostavitev stika s ponudnikom, ki je podatke prenesel.

([147]) Sporazum 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), 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.

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

([149]) Člen 9(1) sporazuma.

([150]) V skladu s členom 1(8) sporazuma med Združenim kraljestvom in ZDA „imenovani organ“ pomeni vladni organ, ki ga za Združeno kraljestvo določi minister za notranje zadeve, za Združene države pa generalni državni tožilec in pravni svetovalec vlade (Attorney General).

(97) Združeno kraljestvo je glede sodnega varstva poudarilo, da bodo prenosi na podlagi sporazuma med Združenim kraljestvom in ZDA vedno vključevali imenovani organ vsake pogodbenice. Kadar so ZDA pogodbenica, ki prejeme podatke od ponudnikov storitev v Združenem kraljestvu, bo ministrstvo za pravosodje (Department of Justice) ZDA delovalo kot imenovani organ. V skladu z razlago Združenega kraljestva bo zato v vsako zahtevo, izdano na podlagi sporazuma med Združenim kraljestvom in ZDA, vključeno ministrstvo za pravosodje kot zvezni organ, imenovan v skladu z zakonom ZDA o sodnem varstvu (US Judicial Redress Act), tako da se lahko zoper to ministrstvo uveljavlja sodno varstvo v skladu s členom 19 krovnega sporazuma. Poleg tega je Združeno kraljestvo službam Komisije potrdilo, da zakon o sodnem varstvu ni edini mehanizem za uveljavljanje sodnega varstva. Glede na okoliščine in ozadje posamezne zadeve drugi veljavni zakoni ZDA zagotavljajo drugačne načine, na katere se lahko uveljavlja sodno varstvo.

### 3.2.3 *Nadzor in pravna sredstva*

(98) Glede na pooblastila, ki jih pristojni organi uporabljajo pri obdelavi osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (na podlagi zakona o varstvu podatkov iz leta 2018 ali zakona o preiskovalnih pooblastilih iz leta 2016), različni organi še naprej zagotavljajo nadzor nad uporabo teh pooblastil, kot je ocenjeno v uvodnih izjavah 158 do 174 Izvedbenega sklepa (EU) 2021/1772, mehanizmi pravnih sredstev pa so še naprej na voljo na podlagi dela 3 zakona o varstvu podatkov iz leta 2018, zakona o preiskovalnih pooblastilih iz leta 2016 in zakona o človekovih pravicah iz leta 1998, kot je analizirano v uvodnih izjavah 250 do 269 Izvedbenega sklepa (EU) 2021/1772.

(99) Kar zadeva nadzor nad delom 3 zakona o varstvu podatkov iz leta 2018, so naloge in pooblastila informacijske komisije analizirani v uvodnih izjavah 158 do 160 in 162 Izvedbenega sklepa (EU) 2021/1772, pri čemer se upoštevajo spremembe, uvedene z zakonom o podatkih (uporaba in dostop), opisane v oddelkih 2.3.1 in 2.3.2 tega sklepa.

(100) Informacijski pooblaščenec je pri izvajanju teh pooblastil od sprejetja Izvedbenega sklepa (EU) 2021/1772 obravnaval številne pritožbe ([151]), izvedel več preiskav in sprejel izvršilne ukrepe glede obdelave podatkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Med letoma 2021 in 2025 je izvedel preiskave in izrekel opomine številnim policijskim organom zaradi različnih kršitev njihovih obveznosti glede varstva podatkov, na primer pri odzivanju na zahteve za dostop do podatkov, uvajanju varnostnih ukrepov za podatke video nadzora, obravnavi občutljivih kazenskih evidenc, združevanju podatkov različnih posameznikov ali razkrivanju osebnih podatkov tretjim osebam ([152]). Izdal je tudi smernice, mnenja in usmerjevalne dokumente, na primer o pravici dostopa ali načinih obravnavanja očitno neutemeljene ali pretirane zahteve v skladu z delom 3 zakona o varstvu podatkov iz leta 2018 ([153]).

(101) Neodvisen in sodni nadzor uporabe preiskovalnih pooblastil na podlagi zakona o preiskovalnih pooblastilih iz leta 2016 še naprej zagotavlja pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil, ki mu pomagajo drugi pravosodni pooblaščenci, skupaj imenovani pravosodni pooblaščenci ([154]). Na tem področju so bile z zakonom o preiskovalnih pooblastilih (spremembe) iz leta 2024 uvedene le omejene in ciljne spremembe, ki ne vplivajo na neodvisnost, naloge in pooblastila pravosodnih pooblaščencev, temveč se z njimi krepi delovanje obstoječe ureditve nadzora v praksi, zlasti z uvedbo namestnikov pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, na katere lahko navedeni pooblaščenec prenese posebna pooblastila, kadar sam ne more opravljati svojih nalog ali ni na voljo zanje. Ti namestniki pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil, ki jih ta tudi imenuje, morajo biti pravosodni pooblaščenci ([155]).

([151]) Informacijska komisija je na primer v obdobju 2023–2024 prejela 1 890 pritožb na podlagi splošne uredbe o varstvu podatkov in/ali zakona o varstvu podatkov iz leta 2018 v zvezi z organizacijami v podsektorjih „policijski organ“, „policijske sile“ in „policijski komisarji“. Glej tudi letno poročilo in računovodske izkaze informacijskega pooblaščenca za obdobje 2023–24 (Information Commissioner's Annual Report and Financial Statements 2023/24), na voljo na povezavi: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Dodatne informacije so na voljo na povezavi: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Na voljo na povezavah: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ in https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Glej uvodno izjavo 250 Izvedbenega sklepa (EU) 2021/1772.

([155]) Člen 227 zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 7 zakona o preiskovalnih pooblastilih (sprememba).

### 3.3 **Pomembne spremembe v zvezi z dostopom javnih organov Združenega kraljestva do podatkov za namene nacionalne varnosti ter njihovo uporabo s strani teh organov**

(102) Zakon o preiskovalnih pooblastilih iz leta 2016 še naprej zagotavlja pravni okvir za uporabo preiskovalnih pooblastil, ki se izvajajo v okviru nacionalne varnosti. Poleg sprememb v zvezi s ciljnimi preiskovalnimi pooblastili, na katera se lahko pod posebnimi pogoji sklicujejo tudi nekateri organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, kot je opisano v uvodnih izjavah 77 do 85 tega sklepa, so bile z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 uvedene tudi spremembe enega od pooblastil iz zakona o preiskovalnih pooblastilih iz leta 2016, ki se lahko izvajajo v večjem obsegu.

(103) Z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 je bila v novem delu 7A zakona o preiskovalnih pooblastilih iz leta 2016 natančneje uvedena posebna ureditev za hrambo in pregled podnabora osebnih podatkov v večjem obsegu ([156]), in sicer za tiste nabore podatkov, glede katerih posamezniki, na katere se osebni podatki nanašajo, ne bi mogli upravičeno pričakovati ali bi lahko upravičeno pričakovali le malo zasebnosti v zvezi s podatki ([157]). Ali je nabor osebnih podatkov v večjem obsegu del tega posebnega podnabora podatkov, določi vodja obveščevalne službe na podlagi vseh okoliščin, zlasti (i) narave podatkov, (ii) obsega, v katerem so posamezniki podatke dali v javnost ali privolili v njihovo objavo, (iii) če so bili podatki objavljeni, obsega, v katerem so bili objavljeni pod uredniškim nadzorom ali od osebe, ki deluje v skladu s strokovnimi standardi, (iv) če so bili podatki objavljeni ali so kako drugače v javni domeni, obsega, v katerem so podatki splošno znani, in (v) obsega, v katerem so bili podatki že uporabljeni v javni domeni ([158]).

(104) Pomembno je, da za hrambo in pregled naborov osebnih podatkov v večjem obsegu, ki ne spadajo v to kategorijo, tj. tistih, ki so občutljivejši in se zato glede njih upravičeno pričakuje zasebnost, še naprej velja ureditev, ocenjena v uvodnih izjavah 239 in 240 Izvedbenega sklepa (EU) 2021/1772, zlasti da je potrebna odredba, ki jo najprej odobri minister, nato pa pravosodni pooblaščenec, pri čemer se upoštevajo zahteve glede potrebnosti in sorazmernosti ukrepa, kot je določeno v delu 7 zakona o preiskovalnih pooblastilih iz leta 2016 ([159]).

(105) Del 7A zakona o preiskovalnih pooblastilih iz leta 2016 določa dve vrsti dovoljenj: posamično dovoljenje in odobritev po kategoriji. Hramba ali hramba in pregled vsakega nabora osebnih podatkov v večjem obsegu, ki se hrani na podlagi dela 7A, mora biti dovoljena na podlagi enega od teh dovoljenj. Za obe dovoljenji sta načeloma potrebni ([160]) dovoljenje vodje obveščevalne službe (ali osebe, ki deluje v njegovem imenu) in odobritev neodvisnega pravosodnega pooblaščenca ([161]). Posamično dovoljenje izda vodja obveščevalne službe v skladu s pogoji iz člena 226B(4) zakona o preiskovalnih pooblastilih iz leta 2016 in po predhodni odobritvi pravosodnih pooblaščencev. Pravosodni pooblaščenec mora pregledati ugotovitve osebe, ki je izdala dovoljenje, z vidika tega, ali se člen 226A, tj. zahteva po upravičenem pričakovanju malo ali nič zasebnosti, uporablja za nabor osebnih podatkov v večjem obsegu, opisan v dovoljenju ([162]).

([156]) Odredbe o naboru osebnih podatkov v večjem obsegu, izdane v skladu s členom 200 zakona o preiskovalnih pooblastilih iz leta 2016, obveščevalnim agencijam omogočajo, da hranijo in pregledujejo nabore podatkov, ki vsebujejo osebne podatke, povezane z več posamezniki, pri čemer je narava nabora taka, da večina posameznikov ni in verjetno ne bo postala zanimiva za obveščevalno službo pri opravljanju njenih nalog, ti podatki pa so elektronsko shranjeni pri obveščevalni službi in se hranijo za analizo pri izvajanju njenih zakonskih nalog, glej tudi člen 199 zakona o preiskovalnih pooblastilih iz leta 2016.

([157]) Člen 226A(1) zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([158]) Člen 226A(3) zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([159]) Z zakonom o preiskovalnih pooblastilih (sprememba) iz leta 2024 je bil spremenjen člen 213 zakona o preiskovalnih pooblastilih iz leta 2016 tako, da odredbe za nabor osebnih podatkov v večjem obsegu prenehajo veljati 12 mesecev po izdaji. Prej jih je bilo treba obnoviti vsakih šest mesecev. Glej člen 3 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([160]) Posamično dovoljenje se lahko izda brez predhodne sodne odobritve, le (i) če oseba, ki izda posamično dovoljenje, meni, da zadevni nabor osebnih podatkov v večjem obsegu spada v obstoječo odobritev po kategoriji, ali (ii) v nujnih primerih; glej člen 226B(6) zakona o preiskovalnih pooblastilih iz leta 2016. V slednjem primeru mora odločitev o izdaji nujnega posamičnega dovoljenja v treh delovnih dneh po dnevu izdaje pregledati pravosodni pooblaščenec; glej člen 226BC zakona o preiskovalnih pooblastilih iz leta 2016.

([161]) Člen 226B(1) zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba).

([162]) Člen 226BB(1), točka (a), zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

(106) Z odobritvijo po kategoriji se dovoljuje hramba ali hramba in pregled kategorije naborov osebnih podatkov v večjem obsegu, opisanih v odobritvi.

(107) Odločitev o izdaji odobritve po kategoriji sprejme vodja obveščevalne službe, če meni, da se člen 226A uporablja za kateri koli nabor podatkov v zadevni kategoriji, in če odločitev o izdaji odobritve odobri neodvisni pravosodni pooblaščenec ([163]). Zadnjenavedeni mora preveriti, ali se člen 226A, tj. zahteva po upravičenem pričakovanju malo ali nič zasebnosti, uporablja za vsak nabor podatkov, ki spada v kategorijo naborov podatkov, opisanih v odobritvi ([164]).

(108) Pomembno je, da mora pravosodni pooblaščenec pri odobritvi odločitve o izdaji posamičnega dovoljenja ali odobritve po kategoriji „uporabiti ista načela, kot bi jih sodišče na podlagi zahteve za sodno presojo“ ([165]), in te zadeve obravnavati z zadostno mero skrbnosti, da se zagotovi, da izpolnjuje obveznosti iz člena 2 zakona o preiskovalnih pooblastilih iz leta 2016 (splošne obveznosti glede zasebnosti) ([166]). Poleg tega je izdaja dovoljenj pod strogim naknadnim nadzorom, zlasti s tem, da se letno poroča pristojnemu ministru in parlamentarnemu odboru za obveščevalno in varnostno dejavnost (Intelligence and Security Committee) ([167]) ter da urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil izvaja redne inšpekcijske preglede ([168]).

(109) Kar zadeva pomembne spremembe na področju nadzora, je urad pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil objavil letna poročila za leta 2021, 2022 in 2023, ki vsebujejo podrobne statistične podatke in informacije o tem, kako obveščevalne agencije in organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v Združenem kraljestvu uporabljajo preiskovalna pooblastila ([169]). V poročilih so opisane tudi revizije in preiskave urada ter njegove ugotovitve, ki potrjujejo, da ima pooblaščenec za nadzor nad izvajanjem preiskovalnih pooblastil v okviru ureditve preiskovalnih pooblastil Združenega kraljestva še naprej zelo pomembno nadzorno vlogo. Leta 2023 je na primer pregledal utemeljitve potrebnosti in sorazmernosti uporabe pooblastil za prestrezanje v večjem obsegu s strani vladne obveščevalne službe (Government Communications Headquarters – GCHQ) (kot je ocenjeno v uvodnih izjavah 218 do 225 Izvedbenega sklepa (EU) 2021/1772) ter ugotovil, da je bila velika večina izjav utemeljenih, v nekaterih primerih pa sorazmernost ni bila dobro izražena. O teh ugotovitvah je razpravljal s skupino vladne obveščevalne službe za skladnost, ki se je zavezala, da bo za reševanje tega vprašanja naročila dodatno notranje usposabljanje za povečanje ozaveščenosti ([170]).

(110) Poleg tega je sodišče za preiskovalna pooblastila (Investigatory Powers Tribunal) objavilo javno poročilo o svojih dejavnostih in sodni praksi za obdobje 2021–2023 ([171]). Poročilo kaže, da se je število zadev, ki jih je prejelo navedeno sodišče, od leta 2017 več kot podvojilo, saj jih je bilo leta 2023 prejetih več kot 400 ([172]). Največ pritožb

([163]) Člen 226BA zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba).

([164]) Člen 226BB(1), točka (b), zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba).

([165]) Člen 226BB(2), točka (a), zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([166]) Člen 226BB(2), točka (b), zakona o preiskovalnih pooblastilih iz leta 2016, kot je bil uveden s členom 2 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024. V skladu s splošnimi obveznostmi glede zasebnosti, kot so določene v členu 2 zakona o preiskovalnih pooblastilih iz leta 2016, mora javni organ upoštevati, (a) ali bi bilo mogoče cilj odredbe, odobritve ali obvestila razumno doseči z drugimi, manj vsiljivimi sredstvi; (b) ali se glede pridobivanja informacij na podlagi odredbe, odobritve ali obvestila uporablja višja raven varstva zaradi posebne občutljivosti informacij; (c) javni interes glede celovitosti in varnosti telekomunikacijskih sistemov in poštnih storitev ter (d) vse druge vidike javnega interesa v zvezi z varstvom zasebnosti.

([167]) Člena 226DA in 226DB zakona o preiskovalnih pooblastilih iz leta 2016, kot sta bila uvedena s členom 2 zakona o preiskovalnih pooblastilih (sprememba) iz leta 2024.

([168]) Glej letno poročilo pooblaščenca za nadzor nad izvajanjem preiskovalnih pooblastil za leto 2023, na voljo na povezavi: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, str. 3.

([169]) Vsa letna poročila so na voljo na povezavi: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Glej točke 6.39 do 6.43 letnega poročila za leto 2023, ki je na voljo na povezavi: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) The Investigatory Powers Tribunal Report 2021–2023 (Poročilo sodišča za preiskovalna pooblastila za obdobje 2021–2023), ki je na voljo na povezavi: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) The Investigatory Powers Tribunal Report 2021–2023 (Poročilo sodišča za preiskovalna pooblastila za obdobje 2021–2023), str. 5.

je bilo vloženih zoper organe preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, takoj za njimi pa zoper varnostne in obveščevalne organe ([173]). Pomembno je, da je sodišče za preiskovalna pooblastila v letih 2022 in 2023 izreklo sodbe v zadevah, ki jih je prejelo pred letom 2021, v katerih je ugotovilo, da so javni organi Združenega kraljestva (policija Škotske ([174]), policija širšega Manchestra ([175]), policija Surreyja ([176]) oziroma varnostna služba (MI5) in minister za notranje zadeve ([177])) ravnali nezakonito. Kar zadeva pravna sredstva, je sodišče za preiskovalna pooblastila med drugim odredilo uničenje nezakonito pridobljenega materiala, v enem primeru pa tudi plačilo 12 000 GBP kot pravično zadoščenje za ugotovljene kršitve. Letno poročilo tako potrjuje, da sodišče za preiskovalna pooblastila učinkovito izpolnjuje svojo pomembno vlogo pri zagotavljanju nadzora in pravnih sredstev na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter dostopa do osebnih podatkov za namene nacionalne varnosti.

(111) V poročilu so dalje navedeni tudi pomembni dosežki, kot je sodba Evropskega sodišča za človekove pravice, v kateri je to sodišče odločilo, da lahko posamezniki kjer koli na svetu vložijo zahtevek na sodišče za preiskovalna pooblastila v zvezi z delovanjem režima Združenega kraljestva za prestrezanje v večjem obsegu, če je zadevno ravnanje izvedel javni organ Združenega kraljestva in se je zgodilo v Združenem kraljestvu ([178]).

## 4. **SKLEPNA UGOTOVITEV**

(112) Komisija meni, da UK GDPR in zakon o varstvu podatkov iz leta 2018, kot sta bila spremenjena z zakonom o podatkih (uporaba in dostop), še naprej zagotavljata raven varstva osebnih podatkov, ki se prenašajo iz Evropske unije, ki je v osnovi enakovredna ravni, zagotovljeni z Uredbo (EU) 2016/679.

(113) Poleg tega Komisija meni, da nadzorni mehanizmi in pravna sredstva v pravu Združenega kraljestva v praksi kot celota še naprej 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.

(114) 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, še naprej omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, ter da obstaja učinkovita pravna zaščita zoper take posege.

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

(116) Ta ugotovitev temelji tako na ustrezni nacionalni ureditvi Združenega kraljestva, kot se je razvijala od sprejetja Izvedbenega sklepa (EU) 2021/1772, in na njegovih mednarodnih zavezah, zlasti nadaljnji zavezanosti Združenega kraljestva Evropski konvenciji o človekovih pravicah ter nadaljnjem priznavanju pristojnosti Evropskega sodišča za človekove pravice. Nadaljnja zavezanost takim mednarodnim obveznostim je torej posebno pomemben element ocene, na kateri temelji ta sklep.

([173]) The Investigatory Powers Tribunal Report 2021–2023 (Poročilo sodišča za preiskovalna pooblastila za obdobje 2021–2023), str. 12.
([174]) Sodba Wilson/Police Scotland [2022] UKIPTrib 5.
([175]) Sodba Pendlebury/Greater Manchester Police [2023] UKIPTrib 2.
([176]) Sodba Hill/Metropolitan Police Service & Independent Office for Police Conduct [2022] UKIPTrib 6.
([177]) Sodba Liberty & Privacy International/Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) Sodba Wieder and Guarnieri/Združeno kraljestvo, [2023] ECHR 668 (glej tudi Poročilo sodišča za preiskovalna pooblastila za obdobje 2021–2023, str. 6).

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

(117) 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 jim ne poteče veljavnost, dokler niso umaknjeni, razveljavljeni na podlagi izpodbojne tožbe ali razglašeni za neveljavne na podlagi predloga za sprejetje predhodne odločbe ali sklicevanja na nezakonitost.

(118) Zato je sklep 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 Izvedbenega sklepa (EU) 2021/1772, kot je bil spremenjen s tem sklepom, 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.

(119) V skladu s členom 58(5) Uredbe (EU) 2016/679 in glede na pojasnila Sodišča v sodbi Schrems I ([179]) je treba opozoriti, da če ima nacionalni organ za varstvo podatkov tudi po prejemu pritožbe pomisleke glede skladnosti sklepa Komisije o ustreznosti s temeljnima pravicama posameznika do zasebnosti in do varstva podatkov, mu mora nacionalno pravo zagotavljati pravno sredstvo za predložitev teh očitkov nacionalnemu sodišču, ki bo morda moralo pri Sodišču vložiti predlog za sprejetje predhodne odločbe ([180]).

## 6. SPREMLJANJE

(120) Komisija v skladu s členom 45(4) Uredbe (EU) 2016/679 redno spremlja razvoj dogodkov v Združenem kraljestvu, da lahko presodi, ali še zagotavlja v osnovi enakovredno raven varstva. Tako spremljanje je pomembno zlasti, ker bo Združeno kraljestvo uporabljalo in izvajalo spremenjeno ureditev varstva podatkov. Poleg tega spremenjeni okvir Združenega kraljestva za varstvo podatkov državnemu sekretarju omogoča, da ta okvir podrobneje opredeli s sekundarno zakonodajo. Zato je posebno pozornost treba nameniti takim dodatnim opredelitvam, praktični uporabi spremenjenih pravil Združenega kraljestva o prenosu osebnih podatkov v tretje države, učinkovitosti uveljavljanja pravic posameznikov, vključno z vsemi zadevnimi spremembami v zakonodaji in praksi v zvezi z novouvedenimi izjemami glede takih pravic ali njihovimi omejitvami, delovanju prestrukturiranega urada informacijskega pooblaščenca, vključno v zvezi z obravnavanjem pritožb in uporabo popravljalnih pooblastil, ter skladnosti z omejitvami in zaščitnimi ukrepi v zvezi z vladnim dostopom, zlasti glede na novouvedeni del 7A zakona o preiskovalnih pooblastilih iz leta 2016. Komisija bi morala pri spremljanju med drugim upoštevati razvoj sodne prakse in nadzor, ki ga izvajajo urad informacijskega pooblaščenca in drugi neodvisni organi.

(121) 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 Izvedbenega sklepa (EU) 2021/1772, kot je bil spremenjen s tem sklepom, ter o razvoju praks v zvezi z obdelavo osebnih podatkov, ocenjenih v Izvedbenem sklepu (EU) 2021/1772, kot je bil spremenjen s tem sklepom, in sicer tako glede obdelave osebnih podatkov, ki jo izvajajo upravljavci in obdelovalci v skladu z UK GDPR, kakor glede omejitev in zaščitnih ukrepov, ki se uporabljajo za dostop javnih organov do osebnih podatkov. To bi moralo vključevati razvoj elementov iz uvodne izjave 120.

(122) 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.

([179]) Sodba Schrems I, točka 65.

([180]) Sodba Schrems I, 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.“

(123) Kadar razpoložljive informacije, zlasti informacije, ki izhajajo iz spremljanja Izvedbenega sklepa (EU) 2021/1772, kot je bil spremenjen s tem sklepom, 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 v določenem roku, ki ne sme presegati treh mesecev, sprejmejo ustrezni ukrepi. 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.

(124) Če pristojni organi Združenega kraljestva ob preteku tega določenega roka navedenih ukrepov ne sprejmejo ali drugače zadovoljivo ne 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.

(125) 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.

(126) Komisija bo v ustrezno utemeljenih nujnih 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. **PREGLED, TRAJANJE IN PODALJŠANJE VELJAVNOSTI TEGA SKLEPA**

(127) Komisija bi morala po sprejetju tega sklepa na podlagi člena 45(3) Uredbe (EU) 2016/679 in ob upoštevanju dejstva, da se lahko raven varstva, ki ga zagotavlja pravni okvir Združenega kraljestva, spremeni, redno preverjati, ali so ugotovitve, ki se nanašajo na ustreznost ravni varstva, ki jo zagotavlja Združeno kraljestvo, še vedno dejansko in pravno upravičene, ob upoštevanju elementov iz člena 45(2) Uredbe (EU) 2016/679. Taka ocenjevanja bi se morala izvajati vsaj na štiri leta in bi morala zajemati vse vidike delovanja tega sklepa, vključno z delovanjem ustreznih mehanizmov nadzora in izvrševanja.

(128) Za izvedbo pregleda bi se morala Komisija sestati z ustreznimi predstavniki organov Združenega kraljestva, vključno z informacijsko komisijo. Možnost sodelovanja na takem srečanju bi morali imeti tudi predstavniki članov Evropskega odbora za varstvo podatkov. Komisija bi morala v okviru pregleda od Združenega kraljestva zahtevati predložitev celovitih informacij o vseh vidikih, pomembnih za ugotavljanje ustreznosti. Zahtevati bi morala tudi pojasnila o vseh prejetih informacijah, pomembnih za ta sklep, tudi o informacijah, prejetih od Evropskega odbora za varstvo podatkov, posameznih organov za varstvo podatkov, skupin civilne družbe, iz javnih poročil ali poročil medijev ali iz katerih koli drugih razpoložljivih virov informacij.

(129) Komisija bi morala na podlagi pregleda pripraviti javno poročilo, ki se predloži Evropskemu parlamentu in Svetu.

(130) Komisija mora tudi upoštevati, da se lahko okvir varstva podatkov, ocenjen v tem sklepu in Izvedbenem sklepu (EU) 2021/1772, še naprej razvija.

(131) Zato je primerno določiti, da ta sklep velja šest let od začetka njegove veljavnosti.

(132) 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 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**

(133) Evropski odbor za varstvo podatkov je objavil mnenje ([181]), ki je bilo upoštevano pri pripravi tega sklepa.

(134) Ukrep iz tega sklepa je v skladu z mnenjem odbora, ustanovljenega na podlagi člena 93 Uredbe (EU) 2016/679.

(135) Izvedbeni sklep (EU) 2021/1772 bi bilo zato treba ustrezno spremeniti –

SPREJELA NASLEDNJI SKLEP:

*Člen 1*

Člen 1(2) Izvedbenega sklepa (EU) 2021/1772 se razveljavi.

*Člen 2*

Člen 4 Izvedbenega sklepa (EU) 2021/1772 se nadomesti z naslednjim:

„*Člen 4*

Ta sklep preneha veljati 27. decembra 2031, razen če se njegova veljavnost podaljša po postopku iz člena 93(2) Uredbe (EU) 2016/679.“.

*Člen 3*

Ta sklep je naslovljen na države članice.

V Bruslju, 19. decembra 2025

*Za Komisijo*
Michael MCGRATH
*član Komisije*

([181]) Mnenje 26/2025 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 povezavi: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.