IZVEDBENI SKLEP KOMISIJE (EU) 2021/1773

z dne 28. junija 2021

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

(notificirano pod dokumentarno številko C(2021) 4801)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

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

ob upoštevanju naslednjega:

1. **UVOD**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1 Ustavni okvir

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

(8) Čeprav Združeno kraljestvo nima kodificirane ustave v običajnem pomenu uveljavljene ustanovne listine, so se sčasoma razvijala ustavna načela, zlasti na podlagi sodne prakse in družbenih norm. Priznana je bila ustavnopravna vrednost določenih listin in predpisov, kot so Magna Carta, Bill of Rights iz leta 1689 in zakon o človekovih pravicah iz leta 1998 (Human Rights Act 1998). Kot del ustave so se z običim pravom (common law), navedenimi listinami in predpisi in mednarodnimi pogodbami, zlasti Evropsko konvencijo o človekovih pravicah (EKČP), ki jo je Združeno kraljestvo ratificiralo leta 1951, razvile temeljne pravice posameznikov. Združeno kraljestvo je leta 1987 ratificiralo tudi Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov ([10]).

(9) Z zakonom o človekovih pravicah iz leta 1998 so bile pravice iz EKČP vključene v pravo Združenega kraljestva. S tem zakonom so vsem posameznikom podeljene temeljne pravice in svoboščine iz členov 2 do 12 in 14 EKČP ter členov 1 do 3 Protokola št. 1 k EKČP in člena 1 Protokola št. 13 k EKČP v povezavi s členi 16 do 18 EKČP. To zajema pravico do spoštovanja zasebnega in družinskega življenja, ki vključuje tudi pravico do varstva podatkov, in pravico do poštenega sojenja ([11]). Natančneje, v skladu s členom 8 EKČP se lahko javna oblast vmešava v izvrševanje pravice do zasebnosti le, če je to določeno z zakonom, kadar je nujno v demokratični družbi zaradi nacionalne varnosti, javne varnosti ali ekonomske blaginje države, zato da se prepreči nered ali kaznivo dejanje, da se zavaruje zdravje ali morala ali da se zavarujejo pravice in svoboščine drugih ljudi.

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

([9]) Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (UK Explanatory Framework for Adequacy Discussion, Section F: Law Enforcement), ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Načela navedene konvencije so bila prvotno prenesena v pravo Združenega kraljestva z zakonom o varstvu podatkov iz leta 1984, ki je bil nadomeščen z zakonom o varstvu podatkov iz leta 1998 in nato z zakonom o varstvu podatkov iz leta 2018 (v povezavi z UK GDPR). Združeno kraljestvo je leta 2018 podpisalo tudi Protokol o spremembi Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov in trenutno dela na ratifikaciji Konvencije.

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

(10) V skladu z zakonom o človekovih pravicah iz leta 1998 mora biti vsak ukrep javnih organov združljiv s pravico, ki jo zagotavlja EKČP ([12]). Poleg tega je treba primarno in sekundarno zakonodajo razumeti in izvajati tako, da sta združljivi z navedenimi pravicami ([13]). Če posameznik meni, da so javni organi kršili njegove pravice, vključno s pravico do zasebnosti in varstva podatkov, lahko pri sodiščih Združenega kraljestva uveljavlja pravna sredstva na podlagi zakona o človekovih pravicah iz leta 1998, ko izčrpa vsa nacionalna pravna sredstva, pa lahko zaradi kršitve pravic, zagotovljenih na podlagi EKČP, uveljavlja pravna sredstva pri Evropskem sodišču za človekove pravice.

2.2 **Okvir Združenega kraljestva za varstvo podatkov**

(11) Združeno kraljestvo je 31. januarja 2020 izstopilo iz Unije. Na podlagi Sporazuma o izstopu Združenega kraljestva Velika Britanija in Severna Irska iz Evropske unije in Evropske skupnosti za atomsko energijo ([14]) se je v Združenem kraljestvu v prehodnem obdobju do 31. decembra 2020 še naprej uporabljalo pravo Unije. Pred izstopom in v prehodnem obdobju je bil zakonodajni okvir o varstvu osebnih podatkov v Združenem kraljestvu, ki ureja obdelavo osebnih podatkov s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, sestavljen iz pomembnih delov zakona o varstvu podatkov iz leta 2018 (Data Protection Act 2018), s katerim je bila v nacionalno zakonodajo prenesena Direktiva (EU) 2016/680.

(12) Vlada Združenega kraljestva je za pripravo na izstop iz EU sprejela zakon iz leta 2018 o izstopu iz Evropske unije (European Union (Withdrawal) Act 2018) (v nadaljnjem besedilu: zakon o izstopu iz EU) ([15]), ki je zakonodajo Unije, ki se neposredno uporablja, vključil v zakonodajo Združenega kraljestva in določil, da se t. i. domača zakonodaja, ki izhaja iz EU, še naprej uporablja do konca prehodnega obdobja. Del 3 zakona o varstvu podatkov iz leta 2018 ([16]), s katerim se Direktiva (EU) 2016/680 prenaša v nacionalno zakonodajo, pomeni domačo zakonodajo, ki izhaja iz EU, v skladu z zakonom o izstopu iz EU. Sodišča Združenega kraljestva morajo v skladu z zakonom o izstopu iz EU nespremenjeno domačo zakonodajo, ki izhaja iz EU, razlagati v skladu z ustrezno sodno prakso Sodišča Evropske unije (v nadaljnjem besedilu: Sodišče) in splošnimi načeli prava Unije, kot so učinkovala tik pred koncem prehodnega obdobja (tako imenovana ohranjena sodna praksa EU oziroma ohranjena splošna načela prava EU) ([17]).

(13) Ministri Združenega kraljestva lahko na podlagi zakona o izstopu iz EU sprejemajo sekundarno zakonodajo v obliki aktov z zakonsko močjo, da se v ohranjeno pravo EU uvedejo potrebne spremembe, ki so posledica izstopa Združenega kraljestva iz Unije. To pooblastilo je bilo izvršeno s predpisi o varstvu podatkov, zasebnosti in elektronski komunikaciji (spremembe itd.) (izstop iz EU) iz leta 2019 (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ali DPPEC Regulations) (v nadaljnjem besedilu: predpisi DPPEC) ([18]). S temi predpisi se zakonodaja Združenega kraljestva o varstvu podatkov, vključno z zakonom o varstvu podatkov iz leta 2018, spreminja tako, da ustreza domačemu kontekstu ([19]).

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

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

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

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

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

([17]) Člen 6 zakona iz leta 2018 o izstopu iz EU.

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

([19]) S predpisi o izstopu se uvajajo številne spremembe v del 3 zakona o varstvu podatkov iz leta 2018. Mnogo teh sprememb je tehničnih, kot je črtanje sklicevanj na „državo članico“ ali „direktivo o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj“ (glej na primer člen 48(8) ali člen 73(5)(a) zakona o varstvu podatkov iz leta 2018) in nadomestitev s pojmom „domače pravo“, tako da bo del 3 po koncu prehodnega obdobja deloval učinkovito kot domače pravo. V nekaterih delih so bile potrebne druge vrste sprememb, na primer glede tega, „kdo“ sprejema „sklepe o ustreznosti“ za zakonodajni okvir Združenega kraljestva o varstvu podatkov (glej člen 74A zakona o varstvu podatkov iz leta 2018), in sicer pristojni minister, ne Evropska komisija.

(14) Zato bodo pravni standardi za obdelavo osebnih podatkov s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, v Združenem kraljestvu po prehodnem obdobju v skladu s sporazumom o izstopu še naprej določeni v pomembnih delih zakona o varstvu podatkov iz leta 2018, vendar kakor je bil spremenjen s predpisi DPPEC, zlasti v delu 3 navedenega zakona. Splošna uredba o varstvu podatkov, kakor se uporablja v Združenem kraljestvu (UK GDPR), se za tovrstno obdelavo ne uporablja.

(15) Del 3 zakona o varstvu podatkov iz leta 2018 določa pravila za obdelavo osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, vključno z načeli o varstvu podatkov, pravnimi podlagami za obdelavo (zakonitost), pravicami posameznikov, na katere se nanašajo osebni podatki, obveznostmi pristojnih organov kot upravljavcev in omejitvami nadaljnjih prenosov podatkov. Obenem so veljavna pravila za nadzor, izvrševanje in sodno varstvo, ki se uporabljajo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, določena v delih 5 in 6 zakona o varstvu podatkov iz leta 2018.

(16) Poleg tega je treba glede na pomembno vlogo policije na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj upoštevati pravila, ki urejajo policijsko delo. Policijsko delo se izvaja decentralizirano, zato se za policijsko delo (a) v Angliji in Walesu, (b) na Škotskem in (c) na Severnem Irskem uporabljajo različni zakonodajni akti, ki pa so po svoji vsebini pogosto podobni ([20]). Poleg tega različne vrste smernic vsebujejo dodatna pojasnila o načinu uporabe pristojnosti policije. Obstajajo tri glavne oblike smernic za policijsko delo: 1) zakonsko predpisane smernice, izdane v skladu z zakonodajo, kot so etični kodeks (Code of Ethics) ([21]) in kodeks ravnanja pri upravljanju policijskih informacij (Code of Practice on the Management of Police Information) ([22]), izdan v skladu z zakonom o policiji iz leta 1996 ([23]), ali kodeksi PACE ([24]), izdani v skladu z zakonom o policijskih dokazih in dokazih v kazenskih postopkih ([25]), 2) smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij (Authorised Professional Practice on the Management of Police Information) ([26]), ki jih je objavil strokovni organ uslužbencev policije (College of Policing), ter 3) operativne smernice (ki jih je objavila policija). Svet nacionalnih načelnikov policije (National Police Chiefs Council) (usklajevalni organ za vse policijske službe Združenega kraljestva) objavlja operativne smernice, ki so jih podprle vse policijske službe in se zato uporabljajo na nacionalni ravni ([27]). Namen teh smernic je zagotoviti skladnost med službami glede načina upravljanja informacij ([28]).

(17) Kodeks ravnanja pri upravljanja policijskih informacij je pristojni minister objavil leta 2005, pri čemer je uporabil pooblastila iz člena 39A zakona o policiji iz leta 1996 ([29]). Vsak kodeks ravnanja, izdan na podlagi zakona o policiji, mora odobriti pristojni minister, preden je predložen parlamentu, pa se je treba o njem posvetovati z nacionalno agencijo za boj proti kriminalu (National Crime Agency). Člen 39A(7) zakona o policiji določa, da mora policija ustrezno upoštevati kodekse, izdane na podlagi zakona, zaradi česar se pričakuje, da policija ravna skladno

([20]) Za podrobnejše pojasnilo o policiji in njenih pooblastilih v Združenem kraljestvu glej: obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj (glej opombo 9).

([21]) Kodeks ravnanja o načelih in standardih strokovnega ravnanja v policijskem poklicu v Angliji in Walesu (The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales) je na voljo na povezavi: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; etični kodeks policijskih organov Severne Irske (the Police Service Northern Ireland Code of Ethic) je na voljo na povezavi: https://www.nipolicingboard.org.uk/psni-code-ethics; etični kodeks o policijskem delu na Škotskem (the Code of Ethic for policing in Scotland) je na voljo na povezavi: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Kodeks ravnanja pri upravljanju policijskih informacij (Code of Practice on the Management of Police Information) je na voljo na povezavi: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Zakon o policiji iz leta 1996 (Police Act 1996) je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Kodeksi ravnanja v zvezi z zakonom o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984 (Police and Criminal Evidence Act 1984 (PACE) codes of practice) so na voljo na povezavi: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Zakon o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984 (Police and Criminal Evidence Act 1984) je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij so na voljo na povezavi: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Priročnik o varstvu podatkov za strokovnjake na področju varstva policijskih podatkov (Data Protection Manual for Police Data Protection Professionals) je na voljo na povezavi: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Kodeks ravnanja pri upravljanju policijskih informacij (glej opombo 22) se na primer uporablja za hrambo informacij pri operativnem policijskem delu (glej uvodno izjavo (47) tega sklepa).

([29]) Iz informacij organov Združenega kraljestva izhaja, da je strokovni organ uslužbencev policije med razpravami o ustreznosti pripravljal kodeks ravnanja pri upravljanju informacij in evidenc (Information and Records Management Code of Practice), ki bi nadomestil kodeks ravnanja pri upravljanju policijskih informacij. Osnutek kodeksa, ki je bil 25. januarja 2021 objavljen za javno posvetovanje, je na voljo na naslednji povezavi: https://www.college.police.uk/article/information-records-management-consultation.

z njimi ([30]). Poleg tega morajo biti nezavezujoče smernice (kot so smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij) vedno skladne s kodeksom ravnanja pri upravljanju policijskih informacij, ki je nadrejeni akt ([31]). Čeprav se lahko v določenih operativnih razmerah zgodi, da morajo policisti odstopati od teh smernic, morajo vsekakor še vedno izpolnjevati zahteve iz dela 3 zakona o varstvu podatkov iz leta 2018 ([32]).

(18) Dodatne smernice v zvezi z zakonodajo Združenega kraljestva o varstvu podatkov za obdelavo na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zagotavlja informacijski pooblaščenec ([33]) (za dodatne podrobnosti o uradu informacijskega pooblaščenca glej uvodne izjave od (93) do (109)). Čeprav navedene smernice niso pravno zavezujoče, bi bila sodišča v sodnem postopku zavezana upoštevati vsako kršitev teh smernic, saj imajo razlagalno vrednost in prikazujejo, kako informacijski pooblaščenec v praksi razlaga in izvaja zakonodajo o varstvu podatkov ([34]).

(19) Nazadnje, organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj Združenega kraljestva morajo, kot je navedeno v uvodnih izjavah od (8) do (10), zagotoviti skladnost z EKČP in Konvencijo Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

(20) Pravni okvir, ki ureja obdelavo osebnih podatkov s strani organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj Združenega kraljestva, je torej po strukturi in glavnih elementih zelo podoben okviru, ki se uporablja v EU. V to je zajeto dejstvo, da okvir ne temelji le na obveznostih iz domačega prava, ki jih je oblikovalo pravo EU, temveč tudi na obveznostih, kot so določene v mednarodnem pravu, zlasti s pristopom Združenega kraljestva k EKČP in Konvenciji Sveta Evrope o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov ter njegovim priznavanjem pristojnosti Evropskega sodišča za človekove pravice. Te obveznosti, ki izhajajo iz pravno zavezujočih mednarodnih instrumentov, ki se nanašajo zlasti na varstvo osebnih podatkov, so torej še posebno pomemben element pravnega okvira, ki se ocenjuje v tem sklepu.

2.3 **Stvarno področje uporabe in ozemeljska veljavnost**

(21) Stvarno področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 sovpada s področjem uporabe Direktive (EU) 2016/680, kot je določeno v členu 2(2) Direktive. Del 3 se uporablja za obdelavo osebnih podatkov, ki jo pristojni organ v celoti ali delno izvaja z avtomatiziranimi sredstvi, in za obdelavo osebnih podatkov, ki so že ali bodo del zbirke in ki je pristojni organ ne izvaja z avtomatiziranimi sredstvi.

(22) Da bi upravljavec spadal na področje uporabe dela 3, mora biti pristojni organ, obdelava pa mora biti izvedena za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Ureditev varstva podatkov, ki se ocenjuje v tem sklepu, se torej uporablja za vse dejavnosti teh pristojnih organov na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj.

(23) Pojem „pristojni organ“ je opredeljen v členu 30 zakona o varstvu podatkov kot oseba iz dodatka 7 k zakonu o varstvu podatkov iz leta 2018 ter vsaka druga oseba, kolikor ima ta oseba zakonske pristojnosti za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Pristojni organi iz dodatka 7 ne zajemajo le policije, temveč tudi vse ministrske in vladne oddelke Združenega kraljestva ter druge organe s preiskovalnimi nalogami (npr. vodja oddelkov davčne in carinske uprave Združenega kraljestva (Commissioner for Her Majesty's Revenue and Customs), valižanska davčna uprava (Welsh Revenue Authority), organ, pristojen za konkurenco in

([30]) V zadevi R proti the Commission of Police of the Metropolis [2014] EWCA Civ 585 je bil potrjen pravni status kodeksa ravnanja pri upravljanju policijskih informacij, prizivni sodnik Laws pa je izjavil, da mora komisar londonske policijske uprave (Metropolitan Police) upoštevati navedeni kodeks in smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij v skladu s členom 39A zakona o policiji iz leta 1996.

([31]) Inšpekcijske nadzore policije v zvezi s skladnostjo s kodeksom ravnanja pri upravljanju policijskih informacij izvaja inšpektorat policije in gasilsko-reševalne službe Združenega kraljestva (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services – HMICFRS).

([32]) Glej v zvezi s tem stališče strokovnega organa uslužbencev policije o skladnosti s smernicami o dovoljeni strokovni praksi pri upravljanju policijskih informacij glede vseh vidikov policijskega dela, ki pojasnjuje, da je „smernice o dovoljeni strokovni praksi pri upravljanju policijskih informacij odobril strokovni organ za policijsko delo (strokovni organ uslužbencev policije) kot uradni vir poklicne prakse za policijsko delo. Pričakuje se, da policijski uradniki in uslužbenci pri izvajanju pooblastil upoštevajo navedene smernice. Vendar se lahko pojavijo okoliščine, v katerih mora policija zaradi upravičenega operativnega razloga odstopati od navedenih smernic, če je tako ravnanje jasno utemeljeno. Policija bi morala biti odgovorna za lokalna in nacionalna tveganja, povezana z delovanjem zunaj nacionalno dogovorjenih smernic; če je posledica tega incident ali preiskava (kot na primer prek neodvisnega urada za ravnanje policije (Independent Office of Police Conduct)), pa je policija odgovorna za vsako tveganje“, stališče je na voljo na povezavi https://www.app.college.police.uk/faq-page/.

([33]) Smernice o obdelavi podatkov v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (Guide to Law Enforcement Processing) so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Glej sodbo v zadevi Bridges proti Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), v kateri je sodišče High Court kljub navedbi, da smernice informacijskega pooblaščenca niso zakonsko določene, navedlo: „[p]ri presoji, ali je upravljavec podatkov upošteval obveznosti po členu člen 64 [glede izvedbe ocene učinka v zvezi z varstvom podatkov, ki se nanaša na obdelavo, pri kateri obstaja visoko tveganje], bo sodišče upoštevalo smernice, ki jih je objavil informacijski pooblaščenec glede ocene učinka v zvezi z varstvom podatkov.“

trge (Competition and Markets Authority), zemljiška knjiga Združenega kraljestva (Her Majesty's Land Register) ali nacionalna agencija za boj proti kriminalu), organe, pristojne za pregon, druge organe kazenskega pravosodja in druge nosilce pooblastil ali organizacije, ki izvajajo dejavnosti preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([35]). Del 3 zakona o varstvu podatkov iz leta 2018 se uporablja tudi za sodišča, kadar izvajajo sodne funkcije, razen za del, povezan s pravicami posameznika, na katerega se nanašajo osebni podatki, in nadzorom, ki ga izvaja urad informacijskega pooblaščenca ([36]). Seznam pristojnih organov, naveden v dodatku 7, ni dokončen in ga lahko posodobi pristojni minister s predpisi, s katerimi se upoštevajo spremembe v organizaciji javnih funkcij ([37]).

(24) Zadevna obdelava mora biti tudi za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, pri čemer je ta namen opredeljen kot preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem ([38]). Kadar se obdelava, ki jo izvajajo pristojni organi, ne izvaja za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ni urejena z delom 3 zakona o varstvu podatkov iz leta 2018. Tako je na primer, ko organ, pristojen za konkurenco in trge, preiskuje primere, ki niso inkriminirani (npr. združitve med podjetji). V tem primeru se uporablja UK GDPR skupaj z delom 2 zakona o varstvu podatkov iz leta 2018, saj pristojni organi obdelavo osebnih podatkov izvajajo za namene, ki niso preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Da bi se določilo, katera ureditev varstva podatkov (del 3 ali del 2 zakona o varstvu podatkov iz leta 2018) se uporablja pri posamezni obdelavi osebnih podatkov, mora pristojni organ, tj. upravljavec, proučiti, ali je glavni namen take obdelave eden od namenov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj v skladu z navedenim zakonom.

(25) V členu 207(2) zakona je glede ozemeljske veljavnosti dela 3 zakona o varstvu podatkov iz leta 2018 določeno, da se navedeni zakon uporablja za obdelavo osebnih podatkov v kontekstu dejavnosti osebe, ki ima ustanovitev na ozemlju Združenega kraljestva. To vključuje javne organe ozemelj Anglije, Walesa, Škotske in Severne Irske, ki spadajo na ozemeljsko področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 ([39]).

2.3.1 *Opredelitev pojmov osebni podatki in obdelava*

(26) Ključna pojma osebni podatki in obdelava sta opredeljena v delu 3 zakona o varstvu podatkov iz leta 2018 in se uporabljata v celotnem zakonu. Opredelitve natančno sledijo ustreznim opredelitvam iz člena 3 Direktive (EU) 2016/680. V skladu z zakonom o varstvu podatkov iz leta 2018 pojem osebni podatki zajema vse informacije, ki se nanašajo na določenega ali določljivega živega posameznika ([40]). V skladu s členom 3(3) zakona o varstvu podatkov iz leta 2018 je določljiv posameznik tisti, ki ga je mogoče neposredno ali posredno določiti na podlagi informacij, vključno z navedbo imena ali identifikatorja ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, genetsko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika. Pojem „obdelava" je opredeljen kot dejanje ali niz dejanj, ki se izvaja v zvezi z informacijami ali nizi informacij, kot so (a) zbiranje, beleženje, urejanje, strukturiranje ali shranjevanje, (b) prilagajanje ali spreminjanje, (c) priklic, vpogled ali uporaba, (d) razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, (e) prilagajanje ali kombiniranje ali (f) omejevanje, izbris ali uničenje. Poleg tega je v zakonu pojem „obdelava občutljivih podatkov" opredeljen kot (a) obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, vero ali filozofsko prepričanje ali članstvo v sindikatu; (b) obdelava genskih podatkov ali biometričnih podatkov za namene edinstvene identifikacije posameznika; (c) obdelava podatkov o zdravstvenem stanju ter (d) obdelava podatkov v zvezi s spolnim življenjem ali spolno usmerjenostjo posameznika" ([41]). V členu 205 zakona o varstvu podatkov iz leta 2018 so v zvezi s tem opredeljeni pojmi „biometrični podatki" ([42]), „podatki o zdravstvenem stanju" ([43]) in „genski podatki" ([44]).

([35]) V dodatku 7 k zakonu o varstvu podatkov iz leta 2018 so med drugim navedeni direktor javnega tožilstva, direktor javnega tožilstva za Severno Irsko ali informacijski pooblaščenec.

([36]) Člen 43(3) zakona o varstvu podatkov iz leta 2018.

([37]) Člen 30(3) zakona o varstvu podatkov iz leta 2018. Obveščevalne službe (tajna obveščevalna služba, varnostna služba in britanska obveščevalna služba GCHQ (Government Communications Headquarters)) niso pristojni organi (glej člen 30(2) zakona o varstvu podatkov iz leta 2018) in del 3 zakona o varstvu podatkov iz leta 2018 se ne uporablja za nobeno od njihovih dejavnosti. Njihove dejavnosti spadajo na področje uporabe dela 4 zakona o varstvu podatkov iz leta 2018.

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

([39]) To pomeni, da se zakon o varstvu podatkov iz leta 2018 in torej ta sklep ne uporabljata za kronska odvisna ozemlja Združenega kraljestva in druga čezmorska ozemlja Združenega kraljestva, kot so na primer Falklandski otoki in ozemlje Gibraltarja.

([40]) Osebni podatki o pokojniku ne spadajo na področje uporabe zakona o varstvu podatkov iz leta 2018.

([41]) Člen 35(8) zakona o varstvu podatkov iz leta 2018.

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

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

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

(27) V členu 32 zakona o varstvu podatkov iz leta 2018 sta pojasnjeni opredelitvi pojmov „upravljavec“ in „obdelovalec“ v kontekstu obdelave osebnih podatkov za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ki natančno sledita ustreznim opredelitvam iz Direktive (EU) 2016/680. Upravljavec pomeni pristojni organ, ki določa namene in sredstva obdelave osebnih podatkov. Kadar obdelavo določa pravo, je upravljavec tisti pristojni organ, ki mu to pravo nalaga tako obveznost. Obdelovalec je opredeljen kot oseba, ki obdeluje osebne podatke v imenu upravljavca (ki ni oseba, zaposlena pri upravljavcu).

2.4 **Zaščitni ukrepi, pravice in obveznosti**

2.4.1 *Zakonitost in poštenost obdelave*

(28) V skladu s členom 35 zakona o varstvu podatkov iz leta 2018 mora biti obdelava osebnih podatkov zakonita in poštena, in to na podoben način, kot je določen v členu 4(l)(a) Direktive (EU) 2016/680. V skladu s členom 35(2) zakona o varstvu podatkov iz leta 2018 je obdelava osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zakonita le, če temelji na pravu in je posameznik, na katerega se nanašajo osebni podatki, privolil v njihovo obdelavo za navedeni namen, ali pa je obdelava potrebna za opravljanje naloge, ki jo v ta namen izvaja pristojni organ.

2.4.1.1 Obdelava, ki temelji na pravu

(29) Za zakonitost obdelave, ki spada v del 3 zakona o varstvu podatkov iz leta 2018, mora taka obdelava podobno kot v členu 8 Direktive (EU) 2016/680 „temeljiti na pravu“. „Zakonita“ obdelava pomeni, da jo dovoljujejo predpisi, obče pravo ali posebne kraljeve pravice ([45]).

(30) Pooblastila pristojnih organov so na splošno urejena s predpisi, kar pomeni, da so njihove naloge in pristojnosti jasno določene v zakonodaji, ki jo sprejme Parlament ([46]). Policija in drugi pristojni organi iz dodatka 7 k zakonu o varstvu podatkov iz leta 2018 se lahko v nekaterih primerih pri obdelavi podatkov sklicujejo na obče pravo ([47]). Obče pravo se je oblikovalo s precedensi, določenimi v odločbah sodišč. Obče pravo je pomembno v smislu pooblastil, ki jih ima na voljo policija, ki iz tega pravnega vira pridobiva svoje temeljne dolžnosti, tj. varovanje javnosti z odkrivanjem in preprečevanjem kaznivih dejanj ([48]). Vendar policija pri izvajanju takih dolžnosti uporablja obče pravo in zakonodajna

([45]) Pojasnjevalne opombe k zakonu o varstvu podatkov iz leta 2018, odstavek 181, ki so na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Pooblastila nacionalne agencije za boj proti kriminalu (National Crime Agency) na primer izhajajo iz zakona o kaznivih dejanjih in sodiščih iz leta 2013 (Crime and Courts Act 2013), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2013/22/contents. Podobno so pooblastila agencije za prehranske standarde (Food Standards Agency) določena z zakonom o prehranskih standardih iz leta 1999 (Food Standards Act 1999), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1999/28/contents. Drugi primeri zajemajo zakon o pregonu storilcev kaznivih dejanj iz leta 1985 (Prosecution of Offenders Act 1985), s katerim je bilo ustanovljeno državno tožilstvo (Crown Prosecution Service) (glej: https://www.legislation.gov.uk/ukpga/1985/23/contents); zakon o vodjih oddelkov davčne in carinske uprave iz leta 2005 (Commissioners for Revenue and Customs Act 2005), s katerim je bila ustanovljena davčna in carinska uprava Združenega kraljestva (glej https://www.legislation.gov.uk/ukpga/2005/11/contents); zakon o kazenskem postopku (Škotska) iz leta 1995 (Criminal Procedure (Scotland) Act 1995), s katerim je bila ustanovljena škotska komisija za ponovno proučitev kazenskih zadev (Scottish Criminal Cases Review Commission) (glej https://www.legislation.gov.uk/ukpga/1995/46/contents); zakon o pravosodju (Severna Irska) iz leta 2002 (Justice (Northern Ireland) Act 2002), s katerim je bilo ustanovljeno državno tožilstvo na Severnem Irskem (Public Prosecution Service in Northern Ireland) (glej https://www.legislation.gov.uk/ukpga/2002/26/contents), ter zakon o kazenskem pravosodju iz leta 1987 (Criminal Justice Act 1987), s katerim je bil ustanovljen in je dobil pooblastila urad za resne prevare (Serious Fraud Office) (glej https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Glede na podatke organov Združenega kraljestva na primer pristojnosti za preiskovanje smrti in pregon kaznivih dejanj škotskega glavnega državnega tožilca (Lord Advocate), ki je vodja sistema kazenskega pregona na Škotskem in deluje v okviru škotskega državnega tožilstva (Crown Office and Procurator Fiscal Service), pristojnega za zadeve pregona na Škotskem, izhajajo iz občega prava, medtem ko so nekatere od njegovih nalog določene v predpisih. Nadalje, pristojnosti monarha ter posledično različnih vladnih oddelkov in ministrov prav tako izhajajo iz kombinacije zakonodaje, občega prava in posebnih kraljevih pravic (to so pristojnosti na podlagi občega prava, podeljene monarhu, ki pa jih izvajajo ministri).

([48]) Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, stran 8 (glej opombo 9).

pooblastila ([49]). Kadar ima policija zakonska pooblastila, ta nadomeščajo vsa pooblastila, ki izhajajo iz občega prava ([50]).

(31) Sodišča so priznala, da so v obseg pooblastil in obveznosti policijskega uradnika na podlagi občega prava vključeni „vsi koraki, ki se mu zdijo potrebni za zagotavljanje miru, preprečevanje kaznivih dejanj ali varovanje lastnine pred škodo, povzročeno s kaznivim dejanjem“ ([51]). Pooblastila na podlagi občega prava niso neomejena. Imajo številne omejitve, vključno s tistimi, ki sta jih uvedla sodišče ([52]) in zakonodaja, zlasti zakon o človekovih pravicah iz leta 1998 in zakon o enakosti iz leta 2010 (Equality Act 2010) ([53]). Za pristojne organe, ki obdelujejo podatke v skladu z delom 3 zakona o varstvu podatkov iz leta 2018, je v to zajeto tudi, da se pooblastila na podlagi občega prava izvajajo skladno z zahtevami iz navedenega zakona ([54]). Pri odločitvi o izvedbi kakršne koli obdelave podatkov je treba proučiti zahteve iz veljavnih smernic, kot je kodeks ravnanja glede upravljanja policijskih informacij, in smernic specifično za eno od držav Združenega kraljestva ([55]). Številne smernice, ki jih izdajo vlada in policijski organi, zagotavljajo, da policijski uradniki izvajajo pooblastila v omejitvah, ki jih določa obče pravo ali ustrezni predpis ([56]).

(32) Posebne kraljeve pravice, ki so še en sestavni del prava, se nanašajo na določene pristojnosti, podeljene kroni, ki jih lahko izvaja izvršilna veja oblasti in ne temeljijo na predpisu, temveč izhajajo iz suverenosti monarha ([57]). V okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj je pomembnih zelo malo primerov posebnih pristojnosti. Vključujejo na primer okvir medsebojne pravne pomoči, ki pristojnemu ministru omogoča, da si za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj izmenjuje podatke s tretjimi državami, pristojnost za

([49]) Ključni zakonodajni akti, ki urejajo glavna policijska pooblastila (aretacije, preiskave, dovoljenja za neprekinjeno pridržanje, odvzem prstnih odtisov, odvzem brisov sluznice in drugega biološkega materiala, prestrezanje tiralic, dostop do komunikacijskih podatkov), so: (i), za Anglijo in Wales – zakon o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984 (Police and Criminal Evidence Act 1984 (PACE)), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1984/60/contents (kot je bil spremenjen z zakonom o varstvu svoboščin iz leta 2012 (Protection of Freedoms Act 2012), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2012/9/contents), in zakonom o preiskovalnih pooblastilih iz leta 2016 (Investigatory Powers Act 2016), ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2016/25/contents), (ii) za Škotsko – zakon o kazenskem pravosodju (Škotska) iz leta 2016 (Criminal Justice (Scotland) Act 2016), ki je na voljo na povezavi: https://www.legislation.gov.uk/asp/2016/1/contents in zakon o kazenskem postopku (Škotska) iz leta 1995 (Criminal Procedure (Scotland) Act 1995, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/1995/46/contents), ter (iii) za Severno Irsko – zakon o policijskih dokazih in dokazih v kazenskih postopkih (Severna Irska) iz leta 1989 (Police and Criminal Evidence (Northern Ireland) Order 1989), ki je na voljo na povezavi: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Organi Združenega kraljestva so pojasnili, da je v Združenem kraljestvu že dolgo vzpostavljena prevlada zakonskega prava, ki sega do sodbe Entick proti Carrington [1765] EWHC KB J98, s katero se je priznalo, da je izvajanje pooblastil izvršilne veje oblasti omejeno, ter uvedlo načelo, da so pooblastila na podlagi občega prava in posebna pooblastila monarha in vlade podrejena pravu države.

([51]) Glej sodbo Rice proti Connolly [1966] 2 QB 414.

([52]) Glej sodbo R(Catt) proti Association of Chief police Officers [2015] AC 1065, v kateri je sodnik Lord Sumption v zvezi s policijskimi pooblastili za pridobitev informacij od posameznika (ki je storil kaznivo dejanje) in njihovo hrambo odločil, da ima policija na podlagi občega prava pooblastilo za pridobivanje in hrambo informacij za namene policijskega dela, tj. na splošno za vzdrževanje javnega reda in preprečevanje in odkrivanje kaznivih dejanj. Ta pooblastila ne dovoljujejo, da bi se informacije pridobivale z vsiljivimi metodami, kot je vstop na zasebno posest, ali dejanji (ki niso aretacija v skladu s pooblastili na podlagi občega prava), ki bi pomenila napad. Sodnik je menil, da so bila v tej zadevi pooblastila na podlagi občega prava dovolj široka, da je bilo dovoljeno pridobivanje in shranjevanje take vrste javnih informacij, ki so se obravnavale v teh pritožbah.

([53]) Zakon o enakosti iz leta 2010 je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Za primer zadeve, v kateri so policijska pooblastila na podlagi občega prava ocenjena v skladu z zakonom o varstvu podatkov iz leta 1998, glej odločbo sodišča High Court v zadevi Bridges proti the Chief Constable of South Wales Police (glej opombo 33). Glej tudi sodbi v zadevi Vidal-Hall proti Google Inc [2015] EWCA Civ 311 in v zadevi Richard proti BBC [2018] EWHC 1837 (Ch).

([55]) Glej na primer smernice severnoirske policije o navodilih za storitev upravljanja evidenc, ki so na voljo na povezavi: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Spodnji dom parlamenta Združenega kraljestva je objavil informativni dokument, v katerem so določena glavna pooblastila na podlagi občega prava in zakonska pooblastila policije v Angliji in Walesu (glej https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). V skladu s tem dokumentom so na primer pooblastila za zagotavljanje „državnega miru“ ter „uporaba telesne sile“ pooblastila, izvedena na podlagi občega prava, „pooblastila za pridržanje in pregled“ pa so vedno izvedena iz predpisa. Poleg tega škotska vlada na svojem spletnem mestu zagotavlja informacije o policijskih pooblastilih za aretacijo ter pridržanje in pregled (glej https://www.gov.scot/policies/police/police-powers/).

([57]) V skladu z informacijami, ki so jih zagotovili organi Združenega kraljestva, med posebne pristojnosti, ki jih izvaja vlada, spadajo sestavljanje in ratifikacija mednarodnih pogodb, opravljanje diplomatske dejavnosti, uporaba oboroženih sil v Združenem kraljestvu za vzdrževanje miru v podporo policiji.

izmenjavo informacij na ta način pa ni vedno določena v predpisih ([58]). Posebne kraljeve pravice zavezujejo načela občega prava ([59]) in so podrejene zakonskim aktom, zato zanje veljajo omejitve iz zakona o človekovih pravicah iz leta 1998 in zakona o varstvu podatkov iz leta 2018 ([60]).

(33) V ureditvi Združenega kraljestva se podobno kot v členu 8 Direktive (EU) 2016/680 zahteva, da morajo pristojni organi za upoštevanje načela zakonitosti zagotoviti, da mora biti obdelava, kadar temelji na pravu, tudi potrebna za opravljanje naloge, ki se izvaja za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Urad informacijskega pooblaščenca v smernicah v zvezi s tem pojasnjuje, da „mora biti usmerjen in sorazmeren način za dosego namena. Pravna podlaga se ne bo uporabljala, če se lahko namen razumno doseže z drugimi manj vsiljivimi sredstvi. Ne zadostuje trditev, da je obdelava potrebna, ker ste se odločili za določen način opravljanja poslovne dejavnosti. Vprašanje je, ali je obdelava za navedeni namen potrebna“ ([61]).

2.4.1.2 Obdelava na podlagi privolitve posameznika, na katerega se nanašajo osebni podatki

(34) V členu 35(2) zakona o varstvu podatkov iz leta 2018 je določena možnost obdelave osebnih podatkov na podlagi privolitve posameznika, kot je navedeno v uvodni izjavi (28).

(35) Vendar se zdi, da privolitev ni pravna podlaga, ki bi bila ustrezna za dejanja obdelave, ki spadajo na področje uporabe tega sklepa. Dejanja obdelave, ki jih zajema ta sklep, se bodo vedno nanašala na podatke, ki so jih pristojni organ države članice v skladu z Direktivo (EU) 2016/680 prenesli pristojnemu organu Združenega kraljestva. Zato običajno ne bodo zajemala neposrednega stika (zbiranje) med javnim organom in posamezniki, na katere se nanašajo osebni podatki, ki lahko temelji na privolitvi v skladu s členom 35(2)(a) zakona o varstvu podatkov iz leta 2018.

(36) Čeprav se sklicevanje na privolitev pri oceni, izvedeni v skladu s tem sklepom, ne šteje za pomembno, je treba zaradi popolnosti opozoriti, da obdelava v okviru preprečevanja, odkrivanja in preiskovanja kaznivih dejanj nikoli ne temelji izključno na privolitvi, saj mora pristojni organ vedno imeti osnovno pristojnost, s katero je njegova obdelava podatkov upravičena ([62]). Podobno kot je to dovoljeno v skladu z Direktivo (EU) 2016/680 ([63]), to bolj konkretno pomeni, da se privolitev uporablja kot dodatni pogoj, da se omogočijo določena omejena in specifična dejanja obdelave, ki jih sicer ne bi bilo mogoče izvesti, na primer zbiranje in obdelava vzorcev DNK posameznika, ki ni osumljenec. Obdelava se v tem primeru ne bi izvajala, če privolitev ni bila dana ali je preklicana ([64]).

([58]) V zvezi s tem glej oceno ureditve Združenega kraljestva za nadaljnje prenose v uvodnih izjavah (74) do (87).

([59]) Glej sodbo v zadevi Bancoult proti Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, v kateri je sodišče ugotovilo, da lahko za posebno pristojnost za izdajanje odločb v svetu veljajo tudi običajni razlogi za sodno presojo.

([60]) Glej sodbo v zadevi Attorney-General proti De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, v kateri je sodišče ugotovilo, da posebnih pristojnosti ni mogoče uporabiti, če jih nadomeščajo zakonska pooblastila; sodbo v zadevi Laker Airways Ltd v Department of Trade [1977] QB 643, v kateri je sodišče ugotovilo, da posebnih pristojnosti ni mogoče uporabiti za onemogočanje zakonskega prava; sodbo v zadevi R. proti Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, v kateri je sodišče ugotovilo, da posebnih pristojnosti ni mogoče uporabiti, kadar so v nasprotju s sprejeto zakonodajo, tudi če ta še ni veljavna; sodbo v zadevi R (Miller) proti Secretary of State for Exiting the European Union [2017] UKSC 5, v kateri je sodišče potrdilo zmožnost zakonskega prava, da prilagodi in ukine posebne pristojnosti. Za splošni pregled razmerja med posebnimi kraljevimi pravicami in predpisi ali pooblastili na podlagi občega prava glej informativni dokument spodnjega doma parlamenta Združenega kraljestva, ki je na voljo na povezavi: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Kaj je bistvo prvega načela?“ (Guide to Law Enforcement Processing, "What is the first principle about?"), ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) To izhaja iz besedila ustrezne določbe zakona o varstvu podatkov iz leta 2018, v skladu s katero je obdelava osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj zakonita le in v obsegu, če „temelji na pravu in je (a) posameznik, na katerega se nanašajo osebni podatki, privolil v njihovo obdelavo v ta namen, (b) ali pa je obdelava potrebna za opravljanje naloge, ki jo v ta namen izvaja pristojni organ“.

([63]) Glej uvodni izjavi 35 in 37 Direktive (EU) 2016/680.

([64]) Organi Združenega kraljestva so pojasnili, da bi bil en primer, v katerem bi bila privolitev ustrezna podlaga za obdelavo, kadar policija v povezavi s pogrešano osebo pridobi vzorec DNK, da ga primerja s truplom, ki je najdeno. V takih primerih ne bi bilo ustrezno, da bi policija posameznika, na katerega se nanašajo osebni podatki, prisilila k predložitvi vzorca; pač pa bi ga prosila za privolitev, ki je dana prostovoljno in se lahko kadar koli prekliče. Če se privolitev prekliče, podatkov ni več mogoče obdelati, razen če se za nadaljnjo obdelavo vzorca določi nova pravna podlaga (npr. posameznik, na katerega se nanašajo osebni podatki, je postal osumljenec). Drug primer bi bil lahko, kadar policija preiskuje kaznivo dejanje, v katerem bi lahko imela žrtev (lahko gre za žrtev ropa, kaznivega dejanja zoper spolno nedotakljivost ali nasilja v družini, sorodnike žrtve, ki ji je bilo vzeto življenje, ali žrtve drugih kaznivih dejanj) korist od napotitve na organizacijo za pomoč žrtvam (Victim Support) (tj. neodvisne dobrodelne organizacije, ki podpira ljudi, ki so jih prizadela kazniva dejanja in travmatični dogodki). V takih primerim bo policija, če ima žrtvino privolitev, organizaciji za pomoč žrtvam le posredovala osebne informacije, kot so ime in kontaktni podatki.

(37) V primerih, v katerih je potrebno privoljenje posameznika, mora biti tako privoljenje nedvoumno in mora zajemati jasno pritrdilno dejanje ([65]). Policija mora imeti obvestilo o varovanju zasebnosti, ki med drugim vključuje potrebne informacije, povezane z veljavno uporabo privolitve. Poleg tega nekateri oddelki policije objavljajo dodatno gradivo o tem, kako zagotavljajo skladnost z zakonodajo o varstvu podatkov, vključno z navedbo, kako in kdaj bodo privolitev uporabili kot pravno podlago ([66]).

2.4.1.3 Obdelava občutljivih podatkov

(38) Glede obdelave posebnih vrst podatkov bi morali veljati posebni zaščitni ukrepi. V zvezi s tem so v delu 3 zakona o varstvu podatkov iz leta 2018, podobno kot je določeno v členu 10 Direktive (EU) 2016/680, določeni strožji zaščitni ukrepi za t. i. obdelavo občutljivih podatkov ([67]).

(39) V skladu s členom 35(3) zakona o varstvu podatkov iz leta 1998 lahko pristojni organi obdelujejo občutljive podatke za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj le v dveh primerih: (1) posameznik, na katerega se nanašajo osebni podatki, je privolil v njihovo obdelavo za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in ko se obdelava izvaja, ima upravljavec sestavljen dokument o ustrezni politiki (Appropriate Policy Document) ([68]) ali (2) obdelava je nujno potrebna za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj in izpolnjuje vsaj enega od pogojev iz dodatka 8 k zakonu o varstvu podatkov iz leta 2018 ter ko se obdelava izvaja, ima upravljavec sestavljen dokument o ustrezni politiki ([69]).

(40) Kar zadeva prvi primer in kot je pojasnjeno v uvodni izjavi 38, se pri tovrstnem prenosu sklicevanje na privolitev ne šteje za ustrezno v skladu s tem sklepom ([70]).

(41) Kadar se pri obdelavi občutljivih podatkov ni mogoče sklicevati na privolitev, se lahko obdelava izvede z uporabo enega od pogojev iz dodatka 8 k zakonu o varstvu podatkov iz leta 2018. Ti pogoji se nanašajo na obdelavo, ki je potrebna za namene, opredeljene z zakonom, izvajanje sodne oblasti, zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugega posameznika, varstvo otrok in ogroženih posameznikov, pravne zahtevke, sodne akte, preprečevanje goljufij, arhiviranje, kadar posameznik, na katerega se nanašajo osebni podatki, sam objavi osebne podatke. Za vse pogoje iz dodatka 8 razen primera, ko posameznik sam objavi osebne podatke, velja preskus nujne potrebnosti. Urad informacijskega pooblaščenca je pojasnil, da „nujna potrebnost v tem

([65]) Ni ločene opredelitve privolitve za namene obdelave osebnih podatkov v skladu z delom 3 zakona o varstvu podatkov iz leta 2018. Urad informacijskega pooblaščenca je zagotovil smernice o pojmu privolitev v skladu z delom 3 zakona o varstvu podatkov iz leta 2018, v katerih je pojasnil, da ima enak pomen in da bi ga bilo treba uskladiti z opredelitvijo iz GDPR, zlasti da „mora biti privolitev prostovoljna, konkretna in informirana ter da mora biti posamezniku zagotovljena dejanska izbira, s katero izrazi strinjanje s podatki, ki se obdelujejo“ (Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „O čem govori prvo načelo?“ (glej opombo 64), za privolitev pa smernice glede varstva podatkov (Guide to Data Protection), ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Glej na primer informacije na spletni strani policije grofije Lincolnshire (https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) ali na spletni strani policije grofije Zahodni Yorkshire (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Člen 35(8) zakona o varstvu podatkov iz leta 2018.

([68]) Člen 35(4) zakona o varstvu podatkov iz leta 2018.

([69]) Člen 35(5) zakona o varstvu podatkov iz leta 2018.

([70]) Zaradi popolnosti je treba navesti, da kadar obdelava temelji na privolitvi, mora biti ta prostovoljna, konkretna in informirana ter mora vsebovati izrecno izbiro glede izražanja strinjanja s podatki, ki se obdelujejo. Kadar obdelava temelji na privolitvi posameznika, na katerega se nanašajo osebni podatki, mora imeti upravljavec poleg tega sestavljen dokument o ustrezni politiki. V členu 42 zakona o varstvu podatkov iz leta 2018 so navedene zahteve, ki jih mora izpolnjevati tak dokument. Jasno je navedeno, da morajo biti v dokumentu vsaj pojasnjeni postopki upravljavca za zagotavljanje skladnosti z načeli o varstvu podatkov ter njegova politika glede hrambe in izbrisa osebnih podatkov. To v skladu s členom 42 zakona o varstvu podatkov iz leta 2018 pomeni, da mora upravljavec sestaviti dokument, v katerem (a) so pojasnjeni postopki upravljavca za zagotavljanje skladnosti z načeli o varstvu podatkov ter (b) je pojasnjena politika upravljavca glede hrambe in izbrisa osebnih podatkov, obdelanih s sklicevanjem na privolitev posameznika, na katerega se nanašajo osebni podatki, ali je določeno, kako dolgo se bodo taki osebni podatki najverjetneje hranili. Dokument o politiki vsebuje zlasti zahtevo, da mora upravljavec vedno vključevati elemente iz točk (a) in (b) ter pri tem spoštovati dolžnost vodenja evidence dejavnosti obdelave. Urad informacijskega pooblaščenca je objavil dokument s predlogo (Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj. Pogoji za obdelavo občutljivih podatkov (Guide to Law Enforcement Processing. „Conditions for sensitive processing“)), ki je na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing), če upravljavec ne izpolni teh zahtev, pa lahko tudi sprejme izvršilni ukrep. Ustrezni dokument o politiki proučijo tudi sodišča pri obravnavi morebitnih kršitev zakona o varstvu podatkov iz leta 2018. Na primer v nedavni sodbi v zadevi R (Bridges) proti Chief Constable of South Wales Police so sodišča pregledala ustrezni dokument o politiki upravljavca in ugotovila, da je bil primeren, a bi se vanj lahko vključile dodatne podrobnosti. Zato je policija južnega Walesa ustrezni dokument o politiki pregledala in ga posodobila z novimi smernicami urada informacijskega pooblaščenca (glej opombo 33). Ustrezni dokument o politiki mora upravljavec v skladu s členom 42(3) zakona o varstvu podatkov iz leta 2018 redno pregledovati. Nazadnje, kot dodatni zaščitni ukrep mora upravljavec v skladu s členom 42(4) zakona o varstvu podatkov iz leta 2018 voditi razširjeno evidenco dejavnosti obdelave, ki zajema dodatne elemente v primerjavi s splošno obveznostjo upravljavca, ki je voditi evidenco dejavnosti obdelave, ki je določena v členu 61 zakona o varstvu podatkov iz leta 2018.

kontekstu pomeni, da se mora obdelava nanašati na nujno družbeno potrebo, ki se je ne da razumno doseči z manj vsiljivimi sredstvi“ ([71]). Poleg tega za nekatere od pogojev veljajo dodatne omejitve. Na primer za sklicevanje na pogoj „namenov, opredeljenih z zakonom“ in „pogoj varstva“ (odstavka 1 in 4 dodatka 8) je treba opraviti dodaten preskus bistvenega javnega interesa. V zvezi s pogoji, ki se nanašajo na varstvo otroka (odstavek 4 dodatka 8), mora biti posameznik, na katerega se nanašajo osebni podatki, določene starosti in se šteti za ogroženega. Poleg tega lahko upravljavec uporabi pogoj iz odstavka 4 dodatka 8 le v primeru posebnih okoliščin ([72]). Podobne omejitve veljajo za pogoja „sodnih aktov“ in „preprečevanja goljufij“ (odstavka 7 oziroma 8 dodatka 8). Oba veljata le za posebne upravljavce. Le sodišče ali drug pravosodni organ lahko uporabi pogoj sodnih aktov in le upravljavci, ki so organizacije za boj proti goljufijam, se lahko sklicujejo na pogoj preprečevanja goljufij.

(42) Nazadnje, kadar se obdelava opira na enega od pogojev iz dodatka 8 oziroma je skladna s členom 42 k zakonu o varstvu podatkov iz leta 2018, mora biti sestavljen dokument o ustrezni politiki, v katerem so pojasnjeni postopki upravljavca za zagotavljanje skladnosti z načeli o varstvu podatkov in njegova politika glede hrambe in izbrisa osebnih podatkov, in uporabljajo se obveznosti razširjene evidence.

2.4.2 *Omejitev namena*

(43) Osebni podatki bi se morali obdelovati za določen namen in se nato uporabljati samo, če to ni nezdružljivo z namenom obdelave. To načelo o varstvu podatkov je zagotovljeno s členom 36 zakona o varstvu podatkov iz leta 2018. Ta določba podobno kot člen 4(1)(b) Direktive (EU) 2016/680 zahteva, da (a) mora biti namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za katerega so osebni podatki zbrani, vsakič določen, izrecen in zakonit ter (b) da se tako zbrani osebni podatki ne smejo obdelovati na način, ki je nezdružljiv z namenom, za katerega so bili zbrani.

(44) Kadar pristojni organi obdelujejo podatke za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, lahko to zajema namene arhiviranja, znanstveno- ali zgodovinskoraziskovalne namene in statistične namene ([73]). V takih primerih je v zakonu o varstvu podatkov iz leta 2018 tudi pojasnjeno, da arhiviranje (ali obdelava za znanstveno- ali zgodovinskoraziskovalne namene in statistične namene) ni dovoljeno, kadar se izvaja v zvezi z odločitvami, sprejetimi glede določenega posameznika, na katerega se nanašajo osebni podatki, ali če je verjetno, da bi mu to povzročilo znatno škodo ali stisko ([74]).

2.4.3 *Točnost in najmanjši obseg podatkov*

(45) Podatki morajo biti točni in, kjer je to potrebno, ažurirani. Podatki morajo biti tudi ustrezni, relevantni in ne smejo presegati namenov, za katere se obdelujejo. Ta načela so podobno, kot je določeno v členu 4(1)(c), (d) in (e) Direktive (EU) 2016/680, zagotovljena s členoma 37 in 38 zakona o varstvu podatkov iz leta 2018. Sprejeti je treba vse razumne korake, da bi se netočni osebni podatki ([75]) čim prej izbrisali ali

([71]) Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, „Pogoji za obdelavo občutljivih podatkov“ (glej opombo 70).

([72]) Obdelava se izvede brez privolitve posameznika, na katerega se nanašajo osebni podatki, kadar: (a) posameznik, na katerega se nanašajo osebni podatki, ne more privoliti v obdelavo, (b) se od upravljavca ne more razumno pričakovati, da bo pridobil privolitev posameznika, na katerega se nanašajo osebni podatki, v obdelavo, in (c) se mora obdelava izvesti brez privolitve posameznika, na katerega se nanašajo osebni podatki, saj bi njegova privolitev posegala v zagotavljanje zaščite iz pododstavka (1)(a).

([73]) Glej člen 41(1) zakona o varstvu podatkov iz leta 2018.

([74]) Glej člen 41(2) zakona o varstvu podatkov iz leta 2018.

([75]) V členu 205 zakona o varstvu podatkov iz leta 2018 je pojem „netočni“ opredeljen kot „nepravilni ali zavajajoči“ osebni podatki. Organi Združenega kraljestva so pojasnili, da je običajno, da so podatki, povezani s kazenskimi preiskavami, pogosto nepopolni, a so lahko ne glede na to točni.

popravili ([76]), pri čemer se upošteva namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za katerega se obdelujejo ([77]), ter da bi se zagotovilo, da se osebni podatki, ki so netočni, nepopolni ali neposodobljeni, ne posredujejo ali dajo na voljo za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ([78]).

(46) V ureditvi varstva podatkov Združenega kraljestva je nadalje podobno kot v členu 7 Direktive (EU) 2016/680 določeno, da se osebni podatki, ki temeljijo na dejstvih, v največji možni meri razločijo od osebnih podatkov, ki temeljijo na osebnih ocenah ([79]). Kjer je to ustrezno in če je mogoče, je treba uvesti jasno razlikovanje med osebnimi podatki, ki se nanašajo na različne kategorije posameznikov, na katere se nanašajo osebni podatki, kot so osumljenci, osebe, obsojene za kaznivo dejanje, žrtve kaznivega dejanja in priče ([80]).

2.4.4 *Omejitev hrambe*

(47) V skladu s členom 5 Direktive (EU) 2016/680 se osebni podatki načeloma ne bi smeli hraniti dlje, kot je potrebno za namene, za katere se obdelujejo. V skladu s členom 39 zakona o varstvu podatkov iz leta 2018 in podobno kot v členu 5 navedene direktive je obdelane osebne podatke za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj prepovedano hraniti dlje, kot je potrebno za namen, za katerega se obdelujejo. V pravni ureditvi v Združenem kraljestvu je zahteva, da morajo biti določeni ustrezni časovni roki za reden pregled potrebe po nadaljnji hrambi osebnih podatkov za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Dodatna pravila o praksah, povezanih s hrambo osebnih podatkov, in uporabljenih časovnih rokih so bila določena v ustrezni zakonodaji in smernicah, ki urejajo pristojnosti in delovanje policije. V Angliji in Walesu je na primer s kodeksom ravnanja pri upravljanju policijskih informacij, ki ga je izdal strokovni organ uslužbencev policije, in smernicami o dovoljeni strokovni praksi pri upravljanju policijskih informacij zagotovljen okvir za dosledni postopek hrambe, pregleda in odstranjevanja na osnovi tveganja za upravljanje informacij pri operativnem policijskem delu ([81]). Ta okvir določa jasna pričakovanja v vseh službah policije, glede načina oblikovanja, izmenjave, uporabe in upravljanja informacij v posameznih policijskih enotah in drugih agencijah in med njimi ([82]). Pričakuje se, da policija ravna v skladu s kodeksom ravnanja, skladnost pa preverja inšpektorat policije in gasilsko-reševalne službe Združenega kraljestva ([83]).

(48) Severnoirska policija (Police Service of Northern Ireland) ni zakonsko obvezana upoštevati kodeksa ravnanja glede upravljanja policijskih informacij. Vendar je okvir kodeksa, sprejetega leta 2011, dopolnjen s priročnikom za severnoirsko policijo ([84]), ki določa politike in postopke o načinu uporabe navedenega kodeksa na Severnem Irskem.

([76]) Člen 38(1)(b) zakona o varstvu podatkov iz leta 2018.

([77]) V obrazložitvenem okviru Združenega kraljestva za razpravo o ustreznosti je navedeno: „to zagotavlja, da so priznane pravice posameznikov, na katere se nanašajo osebni podatki, in operativne potrebe organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj. Zgornja točka je bila med pripravo osnutka zakona o varstvu podatkov pozorno proučena, saj lahko obstajajo specifični in omejeni operativni razlogi, zakaj podatkov ni mogoče popraviti. To se najverjetneje zgodi v primeru, če se morajo zadevni netočni osebni podatki ohraniti v prvotni obliki za dokazne namene," (glej obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek F: Preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, stran 21 (glej opombo 9)).

([78]) Člen 38(4) zakona o varstvu podatkov iz leta 2018. Poleg tega je treba v skladu s členom 38(5) zakona o varstvu podatkov iz leta 2018 preveriti kakovost osebnih podatkov, še preden se jih posreduje ali da na voljo, vsako posredovanje osebnih podatkov pa se opremi s potrebnimi informacijami, ki prejemniku omogočijo, da oceni stopnjo točnosti, popolnosti in zanesljivosti podatkov, in mora vključevati stopnjo posodobljenosti, vendar če se po pošiljanju osebnih podatkov izkaže, da so bili poslani nepravilni podatki ali da posredovanje ni bilo zakonito, je treba prejemnika o tem takoj uradno obvestiti.

([79]) Člen 38(2) zakona o varstvu podatkov iz leta 2018.

([80]) Člen 38(3) zakona o varstvu podatkov iz leta 2018.

([81]) S tem okvirom se zagotavlja skladna hramba pridobljenih osebnih podatkov. Obdobje pregleda je odvisno od kaznivih dejanj, ki so razdeljena v štiri skupine: (1) določene zadeve, povezane z zaščito javnosti; (2) druga nasilna in huda kazniva dejanja zoper spolno nedotakljivost, (3) vsa druga kazniva dejanja in (4) razno. Več podrobnosti je na voljo v smernicah o dovoljeni strokovni praksi glede upravljanja policijskih informacij (glej opombo 26).

([82]) Druge organizacije se lahko glede na informacije organov Združenega kraljestva svobodno odločajo, ali bodo upoštevale načela kodeksa ravnanja glede upravljanja policijskih informacij, na primer davčna in carinska uprava Združenega kraljestva in nacionalna agencija za boj proti kriminalu prostovoljno sprejemata številna načela navedenega kodeksa zaradi doslednosti na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Na splošno večina organizacij zaposlenim zagotavlja posebne politike in smernice za vse zaposlene o načinu obravnavanja osebnih podatkov v okviru njihove vloge, ki so prilagojene posebni organizaciji. To običajno vključuje tudi obvezno usposabljanje.

([83]) Kodeks ravnanja pri upravljanju policijskih informacij je bil izdan z uporabo pooblastil iz zakona o policiji iz leta 1996, ki strokovnemu organu uslužbencev policije omogoča, da izdaja kodekse ravnanja v zvezi z učinkovitim delovanjem policijskega dela. Vsak kodeks ravnanja, izdan na podlagi tega zakona, mora odobriti pristojni minister, preden je predložen parlamentu, pa se je o njem treba posvetovati z nacionalno agencijo za boj proti kriminalu. Člen 39A(7) zakona o policiji iz leta 1996 določa, da mora policija ustrezno upoštevati kodekse, izdane na podlagi navedenega zakona.

([84]) Poglavja 1–6 priročnika za severnoirsko policijo h kodeksu ravnanja glede upravljanja policijskih informacij.

(49) Policija na Škotskem se sklicuje na standardni postopek delovanja za shranjevanje evidenc (Record Retention Standard Operating Procedure) ([85]), ki podpira politiko upravljanja evidenc škotske policije ([86]). V tem postopku delovanja so določena posebna pravila za hrambo evidenc s strani škotske policije.

(50) Poleg splošne zahteve po pregledu evidenc, ki se uporablja za celotno Združeno kraljestvo, so nadaljnje podrobnosti določene v lokalnih predpisih. Za nekaj primerov v zvezi z Anglijo in Walesom je v zakonu o policijskih dokazih in dokazih v kazenskih postopkih, kakor je bil spremenjen z zakonom o varstvu svoboščin iz leta 2012, navedena določba o hrambi prstnih odtisov in profilov DNA ter posebna ureditev za posameznike, ki niso obsojeni ([87]). Z navedenim zakonom o varstvu svoboščin je bil tudi vzpostavljen položaj pooblaščenca za hrambo in uporabo biometričnih podatkov (Commissioner for the Retention and Use of Biometric Material) (v nadaljnjem besedilu: pooblaščenec za biometrične podatke) ([88]). Posebna pravila o fotografijah, posnetih ob odvzemu prostosti, so določena v pregledu fotografij, posnetih ob odvzemu prostosti, iz leta 2017 ([89]). Glede Škotske so v zakonu o kazenskem postopku (Škotska) iz leta 1995 določena pravila za odvzem in hrambo prstnih odtisov in bioloških vzorcev ([90]). Tudi tu je z zakonodajo kot v Angliji in Walesu urejena hramba biometričnih podatkov v različnih primerih ([91]).

2.4.5 *Varnost podatkov*

(51) Osebni podatki se morajo obdelovati tako, da se zagotavlja njihovo varovanje, kar zajema tudi zaščito pred nepooblaščeno ali nezakonito obdelavo in pred nenamerno izgubo, uničenjem ali poškodovanjem. Zato morajo javni organi sprejeti ustrezne tehnične ali organizacijske ukrepe za varovanje osebnih podatkov pred morebitnimi grožnjami. Navedeni ukrepi se morajo presojati glede na najsodobnejšo tehnologijo in zadevne stroške.

(52) Ta načela se izražajo v členu 40 zakona o varstvu podatkov iz leta 2018, v skladu s katerim se morajo podobno kot v členu 4(1)(f) Direktive (EU) 2016/680 osebni podatki, ki se obdelujejo za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obdelati na način, ki zagotavlja ustrezno varnost osebnih podatkov, pri čemer se uporabijo ustrezni tehnični ali organizacijski ukrepi. To zajema ustrezno varstvo podatkov, tudi pred

([85]) Standardni postopek delovanja za shranjevanje evidenc je na voljo na povezavi: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Več podrobnosti o upravljanju evidenc je na voljo v informacijah, povezanih z nacionalnim registrom Škotske (National Records of Scotland) na povezavi: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Obdobja hrambe se razlikujejo glede na to, ali je posameznik obsojen ali ne (členi 63I–63KI zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Medtem ko se lahko na primer prstni odtisi in profil DNK odrasle osebe, obsojene za kaznivo dejanje, ki se vpiše v kazensko evidenco, hranijo za nedoločen čas (člen 63I(2) zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984), je hramba časovno omejena, če je obsojena oseba mlajša od 18 let, je kaznivo dejanje „manjše“ kaznivo dejanje, ki se vpiše v kazensko evidenco, in oseba še ni bila obsojena (člen 63K zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Hramba v primeru osebe, ki ji je bila odvzeta prostost ali je bila obtožena, ni pa bila obsojena, je omejena na tri leta (člen 63F zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Podaljšanje tega obdobja hrambe mora odobriti pravosodni organ (člen 63F(7) zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). V primeru osebe, ki ji je bila odvzeta prostost ali je bila obtožena, ni pa bila obsojena za prekršek, podatkov ni mogoče hraniti (člena 63D in 63H zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984).

([88]) S členom 20 zakona o varstvu svoboščin iz leta 2012 se vzpostavlja položaj pooblaščenca za biometrične podatke. Med nalogami tega pooblaščenca je odločanje, ali lahko policija evidenco profilov DNK in prstne odtise, odvzete posameznikom, ki jim je bila odvzeta prostost, niso pa bili obsojeni za kaznivo dejanje, ki ga je mogoče kvalificirati, hrani ali ne (člen 63G zakona o policijskih dokazih in dokazih v kazenskih postopkih iz leta 1984). Splošna odgovornost pooblaščenca za biometrične podatke je tudi, da redno preverja hrambo in uporabo DNK in prstnih odtisov ter hrambo na podlagi nacionalne varnosti (člen 20(2) zakona o varstvu svoboščin iz leta 2012). Pooblaščenec za biometrične podatke je imenovan na podlagi kodeksa za imenovanje na javne funkcije (kodeks je na voljo na naslednji povezavi: Kodeks upravljanja za imenovanja na javne funkcije – GOV.UK (www.gov.uk)) in pogoji njegovega imenovanja jasno določajo, da ga lahko razreši minister za notranje zadeve le na podlagi ozko opredeljenega sklopa okoliščin; te okoliščine vključujejo neizpolnjevanje njegovih dolžnosti za obdobje treh mesecev, obsodbo zaradi storitve kaznivega dejanja ali nespoštovanje njegovega mandata.

([89]) Pregled uporabe in hrambe fotografij, posnetih ob policijskem pridržanju (Review of the Use and Retention of Custody Images) je na voljo na povezavi: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Člen 18 in naslednji zakona o kazenskem postopku (Škotska) iz leta 1995.

([91]) Obdobja hrambe se razlikujejo glede na to, ali je bila oseba obsojena (člen 18(3) zakona o kazenskem postopku (Škotska) iz leta 1995) in ali je mladoletna ali ne. V tem zadnjem primeru je obdobje hrambe tri leta od obsodbe v sodni obravnavi, v kateri je udeležen otrok (člen 18E(8) zakona o kazenskem postopku (Škotska) iz leta 1995). Podatki oseb, ki jim je bila odvzeta prostost, niso pa bile obsojene, se ne smejo hraniti (člen 18(3) zakona o kazenskem postopku (Škotska) iz leta 1995), razen v posebnih primerih in odvisno od teže kaznivega dejanja (člen 18A zakona o kazenskem postopku (Škotska) iz leta 1995). Zakon o škotskem pooblaščencu za biometrične podatke iz leta 2020 (Scottish Biometrics Commissioner Act 2020) (glej https://www.legislation.gov.uk/asp/2020/8/contents) vzpostavlja položaj škotskega komisarja za biometrične podatke, ki mora pripravljati in revidirati kodekse ravnanja o odvzemu, hrambi, uporabi in uničenju biometričnih podatkov (ki jih odobri škotski parlament) za namene kazenskega pravosodja in policijske namene (člen 7 zakona o škotskem komisarju za biometrične podatke iz leta 2020).

nepooblaščeno ali nezakonito obdelavo ter nenamerno izgubo, uničenjem ali poškodovanjem ([92]). V členu 66 zakona o varstvu podatkov iz leta 2018 je določeno še, da morata vsak upravljavec in vsak obdelovalec izvesti ustrezne tehnične in organizacijske ukrepe, da se zagotovi ustrezna raven varnosti glede na tveganja, ki izhajajo iz obdelave osebnih podatkov. Upravljavec mora v skladu s pojasnjevalnimi opombami oceniti tveganja in na podlagi te ocene uvesti ustrezne varnostne ukrepe, kot je na primer šifriranje ali varnostno dovoljenje ustrezne stopnje za osebje, ki obdeluje podatke ([93]). Pri oceni je treba na primer tudi upoštevati naravo obdelanih podatkov in druge pomembne dejavnike ali okoliščine, ki bi lahko vplivali na varnost obdelave.

(53) Ureditev, ki ureja skladnost z načeli varstva podatkov, je zelo podobna ureditvi, vzpostavljeni s členi 29 do 31 Direktive (EU) 2016/680. V členu 67(1) zakona o varstvu podatkov iz leta 2018 je zlasti v primeru kršitve varnosti osebnih podatkov, povezane z osebnimi podatki, za katere je odgovoren upravljavec, določeno, da mora upravljavec brez nepotrebnega odlašanja in, kadar je to izvedljivo, v 72 urah po seznanitvi s kršitvijo tako kršitev priglasiti informacijskemu pooblaščencu ([94]). Obveznost priglasitve se ne uporablja, kadar ni verjetno, da bi bile s kršitvijo varnosti osebnih podatkov ogrožene pravice in svoboščine posameznikov ([95]). Upravljavec mora dejstva, ki se nanašajo na vsako kršitev varnosti osebnih podatkov, njene učinke in sprejete popravne ukrepe, dokumentirati tako, da lahko informacijski pooblaščenec preveri skladnost z zakonom o varstvu podatkov ([96]). Če se obdelovalec seznani s kršitvijo varnosti, mora to nemudoma priglasiti upravljavcu ([97]).

(54) Če bi kršitev varnosti osebnih podatkov verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov, mora upravljavec v skladu s členom 68(1) zakona o varstvu podatkov iz leta 2018 posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja obvestiti o kršitvi ([98]). Obvestilo mora vsebovati enake informacije kot priglasitev informacijskemu pooblaščencu iz uvodne izjave (53). Ta obveznost ne velja, če je upravljavec izvedel ustrezne tehnične in organizacijske zaščitne ukrepe, ki so se uporabili za osebne podatke, na katere je vplivala kršitev. Prav tako ne velja, če je upravljavec sprejel poznejše ukrepe za zagotovitev, da ni več verjetnosti, da bi se veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, uresničilo. Upravljavcu ni treba obvestiti posameznika, na katerega se nanašajo osebni podatki, v primeru, ki bi vključeval nesorazmeren napor ([99]). V tem primeru je treba posamezniku, na katerega se nanašajo osebni podatki, informacije dati na voljo na drug, enakomerno učinkovit način, na primer prek javnih komunikacijskih sredstev ([100]). Če upravljavec posameznika, na katerega se nanašajo osebni podatki, ni obvestil o kršitvi, lahko informacijski pooblaščenec, ki mu je bila kršitev priglašena v skladu s členom 67 zakona o varstvu podatkov, po proučitvi verjetnosti, da bi kršitev povzročila veliko tveganje, od upravljavca zahteva, da takega posameznika uradno obvesti o kršitvi ([101]).

([92]) Upravljavec mora v skladu s pojasnjevalnimi opombami k zakonu o varstvu podatkov iz leta 2018 (glej opombo 45) zlasti: oblikovati in organizirati njihovo varnost, da bo ustrezala naravi shranjenih osebnih podatkov in škode, ki lahko nastane zaradi kršitve varnosti; jasno navesti, kdo v njihovi organizaciji je pristojen za zagotavljanje varnosti informacij; poskrbeti za pravilno fizično in tehnično varovanje, podprto z zanesljivimi politikami in postopki, ter zanesljive in dobro usposobljene zaposlene, ter biti pripravljen, da se hitro in učinkovito odzove na vsako kršitev varovanja tajnosti.

([93]) Odstavek 221 pojasnjevalnih opomb k zakonu o varstvu podatkov iz leta 2018 (glej opombo 45).

([94]) V členu 67(4) zakona o varstvu podatkov iz leta 2018 je določeno, da je treba v priglasitev vključiti opis vrste kršitve varnosti osebnih podatkov (po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih evidenc osebnih podatkov), ime in kontaktne podatke kontaktne osebe, opis verjetnih posledic kršitve varnosti osebnih podatkov in opis ukrepov, ki jih upravljavec sprejme ali katerih sprejetje predlaga za obravnavanje kršitve varnosti osebnih podatkov (vključno z, če je to primerno, ukrepi za ublažitev morebitnih škodljivih učinkov kršitve).

([95]) Člen 67(2) zakona o varstvu podatkov iz leta 2018.

([96]) Člen 67(6) zakona o varstvu podatkov iz leta 2018.

([97]) Člen 67(9) zakona o varstvu podatkov iz leta 2018.

([98]) Upravljavec lahko v skladu s členom 68(7) zakona o varstvu podatkov iz leta 2018 v celoti ali delno omeji zagotavljanje informacij posamezniku, na katerega se nanašajo osebni podatki, če in dokler je taka omejitev, ki mora spoštovati temeljne pravice in zakonite interese posameznika, na katerega se nanašajo osebni podatki, nujen in sorazmeren ukrep za (a) preprečitev oviranja uradne ali zakonite preiskave, poizvedbe ali postopka, (b) preprečitev vplivanja na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, (c) zaščito javne varnosti, (d) zaščito nacionalne varnosti, (e) zaščito pravic in svoboščin drugih.

([99]) Člen 68(3) zakona o varstvu podatkov iz leta 2018.

([100]) Člen 68(5) zakona o varstvu podatkov iz leta 2018.

([101]) Člen 68(6) zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 68(8) zakona o varstvu podatkov iz leta 2018).

2.4.6 *Preglednost*

(55) Posamezniki, na katere se nanašajo osebni podatki, morajo biti obveščeni o glavnih značilnostih obdelave njihovih osebnih podatkov. To načelo o varstvu podatkov se kaže v členu 44 zakona o varstvu podatkov iz leta 2018, v katerem je podobno kot v členu 13 Direktive (EU) 2016/680) določeno, da je splošna dolžnost upravljavca, da posameznikom, na katere se nanašajo osebni podatki, zagotavlja informacije o obdelavi njihovih osebnih podatkov (z zagotovitvijo splošnega dostopa javnosti do informacij ali kako drugače) ([102]). Informacije, ki se dajo na voljo, zajemajo (a) identiteto in kontaktne podatke upravljavca, (b) kontaktne podatke pooblaščene osebe za varstvo podatkov, kadar ta obstaja, (c) namene obdelave osebnih podatkov, (d) o pravici posameznikov, na katere se nanašajo osebni podatki, da od upravljavca zahtevajo dostop do osebnih podatkov, popravek in izbris osebnih podatkov ali omejitev njihove obdelave, ter (e) o pravici do vložitve pritožbe pri informacijskem pooblaščencu in njegove kontaktne podatke ([103]).

(56) Upravljavec mora v posebnih primerih, da omogoči uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, v skladu za zakonom o varstvu podatkov iz leta 2018 (na primer ko so bili osebni podatki, ki se obdelujejo, zbrani brez vednosti posameznika, na katerega se nanašajo osebni podatki), takemu posamezniku tudi zagotoviti informacije o (a) pravni podlagi za obdelavo, (b) obdobju hrambe osebnih podatkov ali, če to ni mogoče, merilih, ki se uporabijo za določitev tega obdobja, in (c) če je ustrezno, o kategorijah uporabnikov osebnih podatkov (vključno z uporabniki v tretjih državah ali mednarodnih organizacijah), ter (d) nadaljnje informacije, ki so potrebne, da se omogoči uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, v skladu z delom 3 zakona o varstvu podatkov iz leta 2018 ([104]).

2.4.7 *Pravice posameznikov*

(57) Posameznikom, na katere se nanašajo osebni podatki, mora biti podeljenih več izvršljivih pravic. Posameznikom so v poglavju 3 dela 3 zakona o varstvu podatkov iz leta 2018 podeljene pravice do dostopa, popravka in izbrisa in omejitve ([105]), ki so primerljive s pravicami iz poglavja 3 Direktive (EU) 2016/680.

(58) Pravica do dostopa je določena v členu 45 zakona o varstvu podatkov iz leta 2018. Prvič, posameznik je upravičen, da od upravljavca pridobi potrditev, ali se njegovi osebni podatki obdelujejo ali ne ([106]). Drugič, če se osebni podatki obdelujejo, ima posameznik, na katerega se nanašajo osebni podatki, pravico do dostopa do teh podatkov in prejema teh informacij o obdelavi: (a) o namenih in pravnih podlagah za obdelavo, (b) o kategorijah zadevnih podatkov, (c) o prejemniku, ki so mu bili podatki razkriti, (d) o obdobju hrambe osebnih podatkov, (e) o obstoju pravice posameznika, na katerega se nanašajo osebni podatki, do popravka in izbrisa osebnih podatkov, (f) o pravici do vložitve pritožbe in (g) o informacijah o izvoru zadevnih osebnih podatkov ([107]).

(59) Posameznik, na katerega se nanašajo osebni podatki, ima v skladu s členom 46 zakona o varstvu podatkov iz leta 2018 pravico zahtevati, da upravljavec popravi netočne osebne podatke v zvezi z njim. Upravljavec mora podatke brez nepotrebnega odlašanja popraviti (ali kadar so podatki netočni, ker niso popolni, dopolniti). Če je treba osebne podatke ohraniti za namene dokazovanja, mora upravljavec (namesto njihovega popravka) omejiti njihovo obdelavo ([108]).

([102]) V smernicah za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj je naveden ta primer: „Na spletnem mestu imate splošno obvestilo o zasebnosti, ki zajema osnovne informacije o organizaciji, namenu obdelave osebnih podatkov, pravicah posameznika, na katerega se nanašajo osebni podatki, in njegovi pravici do pritožbe pri informacijskem pooblaščencu. Prejeli ste obveščevalne podatke, da je bil posameznik prisoten, ko je bilo storjeno kaznivo dejanje. Temu posamezniku morate med prvim zaslišanjem zagotoviti splošne informacije in dodatne podporne informacije, da bi lahko uveljavljal svoje pravice. Pošteno obdelavo informacij, ki jo zagotavljate, lahko omejite le, če bo negativno vplivala na začeto preiskavo“ (smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Katere informacije moramo zagotoviti posamezniku?“, na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) V smernicah za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj je navedeno, da morajo biti zagotovljene informacije o obdelavi osebnih podatkov v jedrnati, razumljivi in lahko dostopni obliki, morajo biti napisane v jasnem in preprostem jeziku, prilagojenem potrebam ciljnih uporabnikov, kot so otroci, in morajo biti na voljo brezplačno (smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Kako moramo zagotavljati te informacije?“, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Člen 44(2) zakona o varstvu podatkov iz leta 2018.

([105]) Za podrobno analizo pravic posameznika glej smernice glede pravic posameznika v zvezi z obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Člen 45(1) zakona o varstvu podatkov iz leta 2018.

([107]) Člen 45(2) zakona o varstvu podatkov iz leta 2018.

([108]) Člen 46(4) zakona o varstvu podatkov iz leta 2018.

(60) Člen 47 zakona o varstvu podatkov iz leta 2018 posameznikom zagotavlja pravico do izbrisa in omejitve obdelave. Upravljavec mora ([109]) brez nepotrebnega odlašanja izbrisati osebne podatke, če bi njihova obdelava kršila katero koli načelo o varstvu podatkov, pravno podlago za obdelavo ali zaščitne ukrepe, povezane z arhiviranjem in občutljivo obdelavo podatkov. Upravljavec mora podatke izbrisati tudi, če je to obvezno po zakonu. Če je treba osebne podatke ohraniti za namene dokazovanja, mora upravljavec (namesto njihovega izbrisa) omejiti njihovo obdelavo ([110]). Upravljavec mora omejiti obdelavo osebnih podatkov, če posameznik, na katerega se nanašajo osebni podatki, izpodbija njihovo točnost in ni mogoče preveriti, ali so podatki točni ali ne ([111]).

(61) Kadar posameznik, na katerega se nanašajo osebni podatki, zahteva popravek ali izbris osebnih podatkov ali omejitev njihove uporabe, ga mora upravljavec pisno obvestiti, ali je odobril zahtevo, v primeru zavrnitve pa o razlogih za zavrnitev in razpoložljivih pravnih sredstvih (pravici posameznika, na katerega se nanašajo osebni podatki, do vložitve zahtevka pri informacijskem pooblaščencu za preiskavo glede zakonitosti uporabe omejitve, pravico do vložitve pritožbe pri informacijskem pooblaščencu in pravico do vložitve vloge pri sodišču za izdajo odločbe o izpolnitvi obveznosti) ([112]).

(62) Če upravljavec popravi osebne podatke, ki jih je prejel od drugega pristojnega organa, mora to priglasiti drugemu organu ([113]). Če upravljavec popravi ali izbriše osebne podatke, ki jih je razkril, ali omeji njihovo uporabo, mora o tem uradno obvestiti prejemnike, ti pa morajo podobno popraviti ali izbrisati osebne podatke ali omejiti njihovo uporabo (če ohranijo odgovornost za to) ([114]).

(63) Poleg tega ima posameznik, na katerega se nanašajo osebni podatki, pravico, da ga upravljavec brez nepotrebnega odlašanja obvesti o kršitvi varnosti osebnih podatkov, če bi ta kršitev verjetno povzročila veliko tveganje za pravice in svoboščine posameznika ([115]).

(64) Upravljavec mora v zvezi v vsemi navedenimi pravicami posameznika, na katerega se nanašajo osebni podatki, in podobno kot v določbah člena 12 Direktive (EU) 2016/680 zagotoviti, da se posamezniku, na katerega se nanašajo osebni podatki, vse informacije posredujejo v jedrnati, razumljivi in lahko dostopni obliki ([116]) ter po možnosti v jasnem in preprostem jeziku ([117]). Upravljavec mora zahtevi posameznika, na katerega se nanašajo osebni podatki, ugoditi brez nepotrebnega odlašanja in načeloma vsekakor v enem mesecu od njenega prejetja ([118]). Če upravljavec upravičeno dvomi o identiteti posameznika, lahko zahteva zagotovitev dodatnih informacij in odloži obravnavo zahteve, dokler ni ugotovljena identiteta. Upravljavec lahko zahteva razumno pristojbino ali zavrne ukrepanje, kadar meni, da je zahteva očitno neutemeljena ([119]). Urad informacijskega pooblaščenca je zagotovil smernice za primere, ko se zahteva šteje za očitno neutemeljeno ali pretirano ali ko se lahko zahteva pristojbina ([120]).

(65) Poleg tega lahko pristojni minister v skladu s členom 53(4) zakona o varstvu podatkov iz leta 2018 najvišji znesek pristojbine določi s predpisi.

([109]) Posameznik, na katerega se nanašajo osebni podatki, lahko od upravljavca zahteva, da izbriše osebne podatke ali omeji njihovo obdelavo (vendar mora upravljavec obveznosti, da izbriše podatke ali omeji njihovo obdelavo, izvajati ne glede na to, ali je podan tak zahtevek ali ne).

([110]) Člena 46(4) in 47(2) zakona o varstvu podatkov iz leta 2018.

([111]) Člen 47(3) zakona o varstvu podatkov iz leta 2018.

([112]) Člen 48(1) zakona o varstvu podatkov iz leta 2018.

([113]) Člen 48(7) zakona o varstvu podatkov iz leta 2018.

([114]) Člen 48(9) zakona o varstvu podatkov iz leta 2018.

([115]) Člen 68 zakona o varstvu podatkov iz leta 2018.

([116]) Člen 52(1) zakona o varstvu podatkov iz leta 2018.

([117]) Člen 52(3) zakona o varstvu podatkov iz leta 2018.

([118]) V členu 54 zakona o varstvu podatkov iz leta 2018 je opredeljen pomen pojma „veljavni rok“, ki pomeni obdobje enega meseca ali daljše obdobje, kot je lahko določeno v predpisih, ki se začne ob ustreznem času (ko upravljavec prejme zadevno zahtevo, ko upravljavec prejme (morebitne) informacije, zahtevane v zvezi z zahtevo iz člena 52(4) zakona o varstvu podatkov, ali ko je plačana (morebitna) pristojbina, zaračunana v zvezi z zahtevo iz člena 53 zakona o varstvu podatkov).

([119]) Člen 53(1) zakona o varstvu podatkov iz leta 2018.

([120]) Upravljavec se lahko na podlagi smernic urada informacijskega pooblaščenca odloči, da posamezniku, na katerega se nanašajo osebni podatki, zaračuna pristojbino, če je njegova zahteva očitno neutemeljena ali pretirana, vendar nanjo vseeno odgovori. Pristojbina mora biti razuma in mora upravičiti strošek. Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Očitno neutemeljene in pretirane zahteve“, ki na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

2.4.7.1 Omejitve pravic posameznika, na katerega se nanašajo osebni podatki, in obveznosti glede preglednosti

(66) Pristojni organ lahko v določenih okoliščinah omeji določene pravice posameznika, na katerega se nanašajo osebni podatki, tj. pravico do dostopa ([121]), do obveščenosti ([122]), do seznanitve s kršitvijo varnosti osebnih podatkov ([123]) in do obveščenosti o razlogih za zavrnitev popravka ali izbrisa ([124]). Pristojni organ lahko podobno, kot je določeno v ureditvi iz poglavja III Direktive (EU) 2016/680, omejitev uporablja le, kadar je ob spoštovanju temeljnih pravic in zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, potrebna in sorazmerna za: (a) preprečitev oviranja uradne ali zakonite preiskave, poizvedbe ali postopka, (b) preprečitev vplivanja na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, (c) zaščito javne varnosti, (d) zaščito nacionalne varnosti, (e) zaščito pravic in svoboščin drugih.

(67) Urad informacijskega pooblaščenca je zagotovil smernice o uporabi navedenih omejitev. V skladu s temi smernicami morajo upravljavci izvajati analizo vsakega primera posebej, da uravnotežijo pravice posameznika s škodo, ki bi jo tako razkritje povzročilo. Vsako uporabljeno omejitev morajo zlasti utemeljiti kot potrebno in sorazmerno, omejijo pa lahko le tisto, kar je določeno, če bi škodovalo navedenim namenom ([125]).

(68) Pristojni organi so izdali tudi več drugih smernic s podrobnimi informacijami o vseh vidikih zakonodaje o varstvu podatkov, tudi o uporabi omejitve pravic posameznikov, na katere se nanašajo osebni podatki ([126]). Na primer v zvezi s členom 45(4) je v priročniku o varstvu podatkov sveta nacionalnih načelnikov policije navedeno: „Opozoriti je treba, da se lahko omejitve uporabljajo le, če je to potrebno, in le tako dolgo, kot je potrebno. Zato ni dovoljena vsesplošna uporaba omejitev za vse osebne podatke vložnika ali stalna uporaba omejitev. Pri tej drugi točki pogosto velja, da je treba osebne podatke, zbrane brez vednosti posameznika, na katerega se nanašajo osebni podatki, ki je osumljenec v preiskavi, sprva zavarovati pred razkritjem temu posamezniku, da se prepreči vplivanje na preiskovanje med potekom preiskave, da pa pozneje ne bi škodovalo, če bi bili posamezniku med informativnim razgovorom razkriti osebni podatki. Policija mora sprejeti postopke, ki zagotavljajo, da se te omejitve uporabljajo le, kolikor je potrebno, in le za potreben čas trajanja“ ([127]). V teh smernicah so tudi navedeni verjetni primeri uporabe posameznih omejitev ([128]).

(69) Nadalje, v zvezi z možnostjo omejitve uporabe navedenih posebnih pravic zaradi zaščite „nacionalne varnosti“, lahko upravljavec zaprosi za izdajo potrdila, ki ga podpiše vladni minister ali generalni državni tožilec (ali generalni pravobranilec za Škotsko) in ki potrjuje, da je omejitev takih pravic potreben in sorazmeren ukrep za zaščito nacionalne varnosti ([129]). Vlada Združenega kraljestva je izdala smernice za potrdila o omejitvah iz razlogov nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018, v katerih je zlasti poudarjeno, da mora biti vsaka omejitev pravic posameznika, na katerega se nanašajo osebni podatki, zaradi varovanja nacionalne varnosti sorazmerna in potrebna ([130]) (za več podrobnosti o potrdilih glede nacionalne varnosti glej uvodne izjave (131) do (134)).

([121]) Člen 45(4) zakona o varstvu podatkov iz leta 2018.
([122]) Člen 44(4) zakona o varstvu podatkov iz leta 2018.
([123]) Člen 68(7) zakona o varstvu podatkov iz leta 2018.
([124]) Člen 48(3) zakona o varstvu podatkov iz leta 2018.
([125]) Glej na primer smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj o pravici do dostopa, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Glej na primer priročnik o varstvu podatkov za strokovnjake na področju varstva policijskih podatkov, ki ga je izdal svet nacionalnih načelnikov policije (glej opombo 27), ali smernice urada za resne prevare (Serious Fraud Office), ki so na voljo na povezavi: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Priročnik o varstvu podatkov sveta nacionalnih načelnikov policije, stran 140 (glej opombo 27).
([128]) V priročniku o varstvu podatkov sveta nacionalnih načelnikov policije je določeno, da je verjetno, da bo „preprečitev oviranja uradnih ali zakonitih poizvedb, preiskav ali postopkov“ relevantna za osebne podatke, ki se obdelujejo za sodne preiskave, v postopkih pred družinskim sodiščem, za nekazenske preiskave notranje discipline in preiskave, kot je neodvisna preiskava spolne zlorabe otrok; med tem ko je „zaščita pravic in svoboščin drugih“ pomembna za osebne podatke, ki bi se nanašali tudi na druge posameznike in vložnika (priročnik o varstvu podatkov sveta nacionalnih načelnikov policije, stran 140, glej opombo 27).
([129]) Člen 79 zakona o varstvu podatkov iz leta 2018.
([130]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti (UK Government Guidance on National Security Certificates) so na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Kadar se uporablja omejitev pravic posameznika, na katerega se nanašajo osebni podatki, mora pristojni organ tega posameznika brez nepotrebnega odlašanja obvestiti o omejitvi njegovih pravic, razlogih za omejitev in razpoložljivih možnostih pravnih sredstev, razen če bi zagotovitev te informacije ogrozila razlog za uporabo omejitve ([131]). Upravljavec mora kot dodatni zaščitni ukrep pred zlorabo omejitev evidentirati razloge za omejitev informacij in na zahtevo dati te evidence na voljo informacijskemu pooblaščencu ([132]).

(71) Če upravljavec ne zagotovi dodatnih informacij o preglednosti ali dostopu ali zavrne prošnjo za popravek ali izbris osebnih podatkov ali omejitev njihove obdelave, lahko posameznik od informacijskega pooblaščenca zahteva, da prouči, ali je upravljavec omejitev uporabil zakonito ([133]). Zadevni posameznik se lahko tudi pritoži pri informacijskem pooblaščencu ali vloži zahtevek na sodišču, da upravljavcu odredi, naj izpolni zahtevo ([134]).

2.4.7.2 Avtomatizirano sprejemanje odločitev

(72) Člena 49 in 50 zakona o varstvu podatkov iz leta 2018 zajemata pravice, povezane z avtomatiziranim sprejemanjem odločitev, oziroma zaščitne ukrepe, ki se uporabljajo ([135]). Podobno kot je določeno v členu 11 Direktive (EU) 2016/680, lahko upravljavec sprejme pomembno odločitev izključno na podlagi avtomatizirane obdelave osebnih podatkov le, če to predpisuje ali dovoljuje zakon ([136]). Odločitev je pomembna, če bi imela negativen pravni učinek za posameznika, na katerega se nanašajo osebni podatki, ali bi ga zelo prizadela ([137]).

(73) Kadar zakon predpisuje ali dovoljuje, da mora upravljavec sprejeti pomembno odločitev, so v členu 50 zakona o varstvu podatkov iz leta 2018 določeni zaščitni ukrepi, ki se bodo uporabljali pri taki odločitvi (ki je opredeljena kot omejitvena pomembna odločitev). Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, uradno obvestiti o sprejetju take odločitve takoj, ko je to razumno izvedljivo. Posameznik, na katerega se nanašajo osebni podatki, lahko nato od upravljavca zahteva, da v enem mesecu ponovno prouči odločitev ali sprejme novo odločitev, ki ne temelji izključno na podlagi avtomatizirane obdelave. Upravljavec mora zahtevo proučiti in posameznika, na katerega se nanašajo osebni podatki, obvestiti o rezultatu proučitve. Zakon o varstvu podatkov iz leta 2018 daje pristojnemu ministru pristojnost, da sprejema predpise o dodatnih zaščitnih ukrepih ([138]). Tak predpis do zdaj še ni bil izdan.

2.4.8 *Nadaljnji prenosi*

(74) Raven varstva, ki se zagotavlja osebnim podatkom, prenesenim od organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj države članice organu za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v Združenem kraljestvu, se ne sme poslabšati z nadaljnjim prenosom takih podatkov prejemnikom v tretji državi. Taki „nadaljnji prenosi“ podatkov, ki z vidika organa za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v Združenem kraljestvu pomenijo mednarodni prenos iz Združenega kraljestva, bi morali biti dovoljeni le, kadar tudi za nadaljnjega prejemnika zunaj Združenega kraljestva veljajo pravila, ki zagotavljajo podobno raven varstva, kot je zagotovljena v okviru pravnega reda Združenega kraljestva.

([131]) Člen 44(5) in (6), člen 45(5) in (6) ter člen 48(4) zakona o varstvu podatkov iz leta 2018.
([132]) Člen 44(7), člen 45(7) in člen 48(6) zakona o varstvu podatkov iz leta 2018.
([133]) Člen 51 zakona o varstvu podatkov iz leta 2018.
([134]) Člen 167 zakona o varstvu podatkov iz leta 2018.
([135]) V pojasnjevalnih opombah k zakonu o varstvu podatkov iz leta 2018 je glede področja uporabe avtomatizirane obdelave navedeno, da: „se te določbe nanašajo na povsem avtomatizirano sprejemanje odločitev, ne pa na avtomatizirano obdelavo. Avtomatizirana obdelava (vključno z oblikovanjem profilov) poteka, ko je operacija izvedena, ne da bi bilo potrebno človeško posredovanje. To se na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pogosto uporablja, da se veliki nabori podatkov filtrirajo v obvladljive količine, ki jih lahko nato uporabi človeški operater. Pri avtomatiziranem sprejemanju odločitev, ki je oblika avtomatizirane obdelave, mora biti končna odločitev sprejeta brez človeškega posredovanja.“ (Pojasnjevalne opombe k zakonu o varstvu podatkov, odstavek 204, glej opombo 45.)
([136]) Poleg zaščite, ki jo zagotavlja zakon o varstvu podatkov, obstajajo v pravnem okviru Združenega kraljestva druge zakonodajne omejitve, ki se uporabljajo za organe za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in bi preprečevale avtomatizirano obdelavo (vključno z oblikovanjem profilov), ki povzroča nezakonito diskriminacijo. Z zakonom o človekovih pravicah iz leta 1998 so v pravo Združenega kraljestva vključene pravice iz EKČP, vključno s pravico iz člena 14 Konvencije, ki se nanaša na prepoved diskriminacije. Podobno zakon o enakosti iz leta 2010 preprečuje diskriminacijo osebe z zaščitenimi lastnostmi (kar vključuje spol, raso, invalidnost ipd.)
([137]) Člen 49(2) zakona o varstvu podatkov iz leta 2018.
([138]) Člen 50(4) zakona o varstvu podatkov iz leta 2018.

(75) Ureditev Združenega kraljestva o mednarodnih prenosih ureja poglavje 5 dela 3 zakona o varstvu podatkov iz leta 2018 ([139]) in izraža pristop iz Poglavja V Direktive (EU) 2016/680. Za prenos osebnih podatkov v tretjo državo mora pristojni organ izpolnjevati zlasti tri pogoje, in sicer: (a) prenos mora biti potreben za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, (b) prenos mora temeljiti na: (i) predpisu o ustreznosti v zvezi s tretjo državo, (ii) če ne temelji na predpisu o ustreznosti, obstoju ustreznih zaščitnih ukrepov ali (iii), če ne temelji na sklepu o ustreznosti ali obstoju ustreznih zaščitnih ukrepov, na posebnih okoliščinah, ter (c) prejemnik prenosa mora biti: (i) ustrezen organ (ki je enakovreden pristojnemu organu) v tretji državi, (ii) ustrezna mednarodna organizacija, npr. mednarodni organ, ki izvaja naloge, ki ustrezajo kateremu koli namenu preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, ali (iii) oseba, ki ni ustrezen organ, vendar le, kadar je prenos nujno potreben za izvajanje enega od namenov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj; kadar nobena temeljna pravica in svoboščina zadevnega posameznika, na katerega se nanašajo osebni podatki, ne prevlada nad javnim interesom, zaradi katerega je prenos potreben; kadar bi bil prenos osebnih podatkov ustreznemu organu v tretji državi neučinkovit ali neustrezen, in kadar je prejemnik obveščen o namenih, za katere se lahko podatki obdelujejo ([140]).

(76) Predpise o ustreznosti v zvezi s tretjo državo, ozemljem ali področjem znotraj tretje države, mednarodno organizacijo ali opisom ([141]) take države, ozemlja, področja ali organizacije izda pristojni minister. Ta mora, kar zadeva standard, ki ga je treba izpolniti, presoditi, ali tako ozemlje/področje/organizacija zagotavlja ustrezno raven varstva osebnih podatkov. V členu 74A(4) zakona o varstvu podatkov iz leta 2018 je določeno, da mora pristojni minister v ta namen proučiti številne elemente, ki izražajo elemente iz člena 36 Direktive (EU) 2016/680 ([142]). Od konca prehodnega obdobja je del 3 zakona o varstvu podatkov iz leta 2018 „domača zakonodaja, ki izhaja iz EU“, ki jo bodo, kot je bilo pojasnjeno, sodišča Združenega kraljestva razlagala v skladu z ustrezno sodno prakso Sodišča, sprejeto pred izstopom Združenega kraljestva iz Unije, in splošnimi načeli prava Unije, kot so učinkovala tik pred koncem prehodnega obdobja. To zajema standard, da je „v osnovi enakovredna“, ki se bo tako uporabljal pri ocenah ustreznosti, ki jih bodo izvedli organi Združenega kraljestva.

(77) Glede postopka se za predpise uporabljajo „splošne“ procesne zahteve iz člena 182 zakona o varstvu podatkov iz leta 2018. V skladu s tem postopkom se mora pristojni minister pred sprejetjem prihodnjih predpisov Združenega

([139]) Ta novi okvir se je začel uporabljati ob koncu prehodnega obdobja, vključno s pristojnostjo pristojnega ministra za sprejemanje predpisov o ustreznosti. Predpisi DPPEC (zlasti odstavki 10 do 12 dodatka 21, ki je bil s predpisi DPPEC vključen v zakon o varstvu podatkov iz leta 2018) določajo, da se med prehodnim obdobjem in po koncu tega obdobja nekateri prenosi osebnih podatkov obravnavajo, kot da temeljijo na predpisih o ustreznosti. Mednje spadajo prenosi v tretje države, za katere ob koncu prehodnega obdobja velja sklep EU o ustreznosti, ter v države članice EU, države Efte in na ozemlje Gibraltarja zaradi njihove uporabe direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj za obdelavo podatkov s področja preprečevanja, odkrivanja in preiskovanja kaznivih dejanj (države Efte uporabljajo Direktivo (EU) 2016/680 zaradi svojih obveznosti na podlagi schengenskega pravnega reda). To pomeni, da se lahko ob koncu prehodnega obdobja prenosi v te države nadaljujejo kot pred izstopom iz EU. Po koncu prehodnega obdobja mora pristojni minister v štirih letih opraviti pregled teh ugotovitev glede ustreznosti.

([140]) Člena 73 in 77 zakona o varstvu podatkov iz leta 2018.

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

([142]) Glej člen 74A(4) zakona o varstvu podatkov iz leta 2018, v katerem je določeno, da mora pri presoji ustreznosti ravni varstva „pristojni minister zlasti upoštevati (a) načelo pravne države, spoštovanje človekovih pravic in temeljnih svoboščin, ustrezno splošno in področno zakonodajo, tudi na področju javne varnosti, obrambe, nacionalne varnosti in kazenskega prava ter dostopa javnih organov do osebnih podatkov, pa tudi izvajanje take zakonodaje, pravila o varstvu podatkov, strokovna pravila ter varnostne ukrepe, vključno s pravili za nadaljnji prenos osebnih podatkov v drugo tretjo državo ali mednarodno organizacijo, ki se spoštujejo v navedeni tretji državi ali mednarodni organizaciji, sodno prakso, pa tudi dejanske in izvršljive pravice ter učinkovito upravno in sodno varstvo posameznikov, na katere se nanašajo osebni podatki, ki se prenašajo; (b) obstoj enega ali več učinkovito delujočih neodvisnih nadzornih organov v tretji državi članici ali pristojnih za mednarodno organizacijo, ki so odgovorni za zagotavljanje in izvrševanje predpisov o varstvu podatkov, kar vključuje tudi ustrezna pooblastila za izvrševanje, za pomoč in svetovanje posameznikom, na katere se nanašajo osebni podatki, pri uresničevanju njihovih pravic ter za sodelovanje z nadzornimi organi držav članic, ter (c) mednarodne zaveze, ki jih je sprejela zadevna tretja država ali mednarodna organizacija, ali druge obveznosti, ki izhajajo iz pravno zavezujočih konvencij ali instrumentov, pa tudi iz sodelovanja države ali mednarodne organizacije v večstranskih ali regionalnih sistemih, zlasti glede varstva osebnih podatkov“.

kraljestva o ustreznosti posvetovati z informacijskim pooblaščencem ([143]). Ko pristojni minister sprejme navedene predpise, se jih predloži parlamentu, ki jih obravnava v postopku tako imenovane negativne potrditve, v katerem lahko oba domova parlamenta proučita predpise in jih v 40 dneh razveljavita ([144]).

(78) V skladu s členom 74 B(1) zakona o varstvu podatkov iz leta 2018 je treba predpise o ustreznosti preverjati na največ štiri leta, pristojni minister pa mora redno spremljati dogajanje v tretjih državah in mednarodnih organizacijah, ki bi lahko vplivalo na odločitve o sprejemanju predpisov o ustreznosti, njihovem spreminjanju ali odpravi. Če pristojni minister izve, da zadevna država ali organizacija ne zagotavlja več ustrezne ravni varstva osebnih podatkov, mora po potrebi spremeniti ali odpraviti navedene predpise ter se z zadevno tretjo državo ali mednarodno organizacijo posvetovati o izboljšanju ravni varstva.

(79) Podobno kot je določeno v členu 37 Direktive (EU) 2016/680, bi bil prenos osebnih podatkov v okviru sektorja preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če takih predpisov o ustreznosti ni, mogoč le, če so vzpostavljeni ustrezni zaščitni ukrepi. Taki zaščitni ukrepi so zagotovljeni (a) z zavezujočim pravnim instrumentom, ki vsebuje ustrezne zaščitne ukrepe za varstvo osebnih podatkov, ali (b) s presojo, ki jo opravi upravljavec, ki po presoji vseh okoliščin prenosa ugotovi, da obstajajo ustrezni zaščitni ukrepi za varstvo podatkov ([145]). Kadar prenosi temeljijo na ustreznih zaščitnih ukrepih, je v zakonu o varstvu podatkov iz leta 2018 prav tako določeno, da mora urad informacijskega pooblaščenca poleg svoje običajne nadzorne vloge od pristojnih organov prejemati posebne informacije o prenosih temu uradu ([146]).

(80) Če prenos ne temelji na sklepu o ustreznosti ali ustreznih zaščitnih ukrepih, se lahko izvede le v določenih, posebnih okoliščinah, imenovanih „posebne okoliščine“ ([147]). Na primer, kadar je prenos potreben: (a) za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge osebe; (b) za zaščito zakonitih interesov posameznika, na katerega se nanašajo osebni podatki; (c) za preprečitev neposredne in resne grožnje javni varnosti v tretji državi; (d) v posameznih primerih za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ali (e) v posameznem primeru iz pravnih razlogov (kot na primer v zvezi s sodnimi postopki ali za zagotavljanje pravnih nasvetov) ([148]). Opozorimo lahko, da se točki (d) in (e) ne uporabljata, če pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, prevladajo nad javnim interesom v prenosu ([149]). Te okoliščine ustrezajo posebnim razmeram in pogojem, ki so v skladu s členom 38 Direktive (EU) 2016/680 opredeljeni kot „odstopanja“.

(81) V takih primerih je treba dokumentirati datum, čas in utemeljitev prenosa, ime prejemnika in druge ustrezne informacije o njem in opis prenesenih osebnih podatkov ter te informacije na zahtevo zagotoviti informacijskemu pooblaščencu ([150]).

(82) Člen 78 zakona o varstvu podatkov iz leta 2018 ureja scenarij „nadaljnjih prenosov“, in sicer ko se osebni podatki, ki so bili preneseni iz Združenega kraljestva v tretjo državo, nato prenesejo v drugo tretjo državo ali mednarodno organizacijo. V skladu s členom 78(1) navedenega zakona mora upravljavec Združenega kraljestva, ki izvede prenos, ta prenos pogojiti z zahtevo, da se podatki ne smejo nadalje prenesti v tretjo državo brez dovoljenja upravljavca, ki izvede prenos. Poleg tega v skladu s členom 78(3) in podobno s tem, kar določa člen 35(1)(e) Direktive (EU) 2016/680, za vsak primer, v katerem je potrebno tako dovoljenje, velja vrsta vsebinskih zahtev.

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

([144]) Med tem 40-dnevnim obdobjem imata lahko oba domova parlamenta Združenega kraljestva možnost, da glasujeta proti predpisom, če tako želita; če je taka odločitev izglasovana, predpisi nimajo več nobenega nadaljnjega pravnega učinka.

([145]) Člen 75 zakona o varstvu podatkov iz leta 2018.

([146]) V skladu s členom 75(3) zakona o varstvu podatkov iz leta 2018, kadar se prenos podatkov opira na ustrezne zaščitne ukrepe: (a) mora biti prenos dokumentiran, (b) mora biti informacijskemu pooblaščencu na zahtevo zagotovljena dokumentacija in (c) mora dokumentacija zajemati zlasti (i) datum in čas prenosa, (ii) ime prejemnika in vse druge ustrezne informacije o njem, (iii) utemeljitev prenosa ter (iv) opis prenesenih osebnih podatkov.

([147]) Smernice za obdelavo podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj „Ali obstajajo posebne zahteve?“, ki so na voljo na povezavi: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

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

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

([150]) Člen 76(3) zakona o varstvu podatkov iz leta 2018.

Konkretneje se mora pristojni organ pri odločanju o tem, ali bo prenos dovolil ali ne, prepričati, da je nadaljnji prenos potreben za namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj ter mora med drugimi dejavniki razmisliti o (a) resnosti okoliščin, zaradi katerih je bilo zahtevano dovoljenje, (b) namenu prvotnega prenosa osebnih podatkov in (c) standardih varstva osebnih podatkov, ki se uporabljajo v tretji državi ali mednarodni organizaciji, v katero bi se prenesli osebni podatki.

(83) Poleg tega se za podatke, ki so bili prvotno preneseni iz Evropske unije in so predmet nadaljnjega prenosa iz Združenega kraljestva, uporabljajo dodatni zaščitni ukrepi.

(84) Prvič, člen 73(1)(b) zakona o varstvu podatkov iz leta 2018 – podobno kot člen 35(1)(c) Direktive (EU) 2016/680 – določa, da kadar je država članica osebne podatke prvotno poslala ali drugače dala na voljo upravljavcu ali drugemu pristojnemu organu, je ta država članica ali katera koli oseba s sedežem v tej državi članici, ki je pristojni organ za namene Direktive (EU) 2016/680, morala dovoliti prenos v skladu s pravom te države članice.

(85) Tako dovoljenje pa po vzoru člena 35(2) Direktive (EU) 2016/680 ni potrebno, če (a) je prenos potreben, da se prepreči neposredna in resna grožnja javni varnosti v državi članici ali tretji državi ali vitalnim interesom države članice, in (b) dovoljenja ni mogoče pridobiti pravočasno. V tem primeru mora biti brez odlašanja obveščen organ v državi članici, ki bi bil pristojen za odločanje o odobritvi prenosa ([151]).

(86) Drugič, enak pristop velja za podatke, ki so bili prvotno preneseni iz Evropske unije v Združeno kraljestvo, nato pa jih je Združeno kraljestvo nadalje preneslo v tretjo državo, ki bi jih nato nadalje prenesla v drugo tretjo državo. V tem primeru pristojni organ Združenega kraljestva na podlagi člena 78(4) ne more dovoliti zadnje omenjenega prenosa v skladu s členom 78(1), razen če je „država članica[, ki je prvotno prenesla zadevne podatke,] ali katera koli druga oseba s sedežem v tej državi članici, ki je pristojni organ za namene direktive o varstvu podatkov pri preprečevanju, odkrivanju in preiskovanju kaznivih dejanj, dovolila prenos v skladu s pravom te države članice“. Ti zaščitni ukrepi so pomembni, ker organom držav članic omogočajo, da v skladu s pravom EU o varstvu podatkov zagotavljajo neprekinjenost zaščite v celotni „verigi prenosov“.

(87) Ta novi okvir glede mednarodnih prenosov podatkov se je začel uporabljati ob koncu prehodnega obdobja ([152]). Vendar odstavki 10 do 12 dodatka 21 (uvedenega s predpisi DPPEC) določajo, da se od konca prehodnega obdobja naprej nekateri prenosi osebnih podatkov obravnavajo, kot da temeljijo na predpisih o ustreznosti. Ti prenosi zajemajo prenos v državo članico, državo Efte, tretjo državo, za katero ob koncu prehodnega obdobja velja sklep EU o ustreznosti, in ozemlje Gibraltarja. Posledično se lahko prenosi v navedene države nadaljujejo kot pred izstopom Združenega kraljestva iz Unije. Po koncu prehodnega obdobja mora pristojni minister v štirih letih opraviti pregled teh ugotovitev glede ustreznosti, tj. do konca decembra 2024. Iz pojasnila organov Združenega kraljestva izhaja, da čeprav mora pristojni minister tak pregled opraviti do konca decembra 2024, pa prehodne določbe ne vključujejo samoderogacijske določbe in zadevne prehodne določbe samodejno ne prenehajo veljati, če pregled ni opravljen do konca decembra 2024.

2.4.9 *Odgovornost*

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

(89) To načelo se kaže v členu 56 zakona o varstvu podatkov iz leta 2018, v katerem so za upravljavca uvedene splošne obveznosti glede odgovornosti, tj. obveznost izvajanja ustreznih tehničnih in organizacijskih ukrepov, da se zagotovi in lahko dokaže, da je obdelava osebnih podatkov skladna z zahtevami iz dela 3 zakona o varstvu podatkov iz leta 2018. Po potrebi je treba pregledati in posodobiti izvedene ukrepe in, kjer je sorazmerno, v zvezi z obdelavo vključiti ustrezne politike varstva podatkov.

([151]) Člen 73(5) zakona o varstvu podatkov iz leta 2018.

([152]) Uporabo tega novega okvira je treba razumeti v smislu člena 782 Sporazuma o trgovini in sodelovanju med Evropsko unijo in Evropsko skupnostjo za atomsko energijo na eni strani ter Združenim Kraljestvom Velika Britanija in Severna Irska na drugi strani (L 444/14 z dne 31.12.2020), ki je na voljo na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:22020A1231(01)&from=SL.

(90) V skladu s poglavjem IV Direktive (EU) 2016/680 členi 55 do 71 zakona o varstvu podatkov iz leta 2018 določajo drugačne mehanizme za zagotovitev odgovornosti ter upravljavcem in obdelovalcem omogočajo, da dokažejo skladnost. Upravljavci morajo zlasti izvesti ukrepe za vgrajeno in privzeto varstvo podatkov, tj. zagotoviti, da se načela o varstvu podatkov učinkovito izvajajo, ter morajo voditi evidenco vseh kategorij dejavnosti obdelave, za katere je odgovoren upravljavec (vključno z informacijami o identiteti upravljavca, kontaktnimi podatki pooblaščene osebe za varstvo podatkov, nameni obdelave, kategorijami prejemnikov razkritih informacij in opisom kategorij posameznikov, na katere se nanašajo osebni podatki, in osebnih podatkov) in informacijskemu pooblaščencu na zahtevo omogočiti dostop do te evidence. Upravljavec in obdelovalec morata tudi voditi dnevnike določenih dejanj obdelave in informacijskemu pooblaščencu omogočiti dostop do njih ([153]). Od upravljavcev se tudi izrecno zahteva, da sodelujejo z informacijskim pooblaščencem pri izvajanju njegovih nalog.

(91) V zakonu o varstvu podatkov iz leta 2018 so prav tako določene dodatne zahteve za obdelavo, ki bi verjetno povzročila veliko tveganje za pravice in svoboščine posameznikov. Med njimi sta obveznost izvedbe ocen učinka v zvezi z varstvom podatkov in posvetovanja z informacijskim pooblaščencem pred obdelavo, če iz take ocene izhaja, da bi obdelava povzročila veliko tveganje za pravice in svoboščine posameznikov (kadar ni ukrepov za ublažitev tveganja).

(92) Upravljavci morajo nadalje imenovati pooblaščeno osebo za varstvo podatkov, razen če je upravljavec sodišče ali drug pravosodni organ, ki izvaja sodno pristojnost ([154]). Upravljavec mora poskrbeti, da je pooblaščena oseba za varstvo podatkov vključena v vsa vprašanja v zvezi z varstvom osebnih podatkov, da ima potrebna sredstva in dostop do osebnih podatkov in dejavnosti obdelave ter da lahko neodvisno izvaja svoje naloge. Naloge pooblaščene osebe za varstvo podatkov, ki zajemajo zagotavljanje informacij in nasvetov, spremljanje skladnosti ter sodelovanje s kontaktno točko in delovanje kot kontaktna točka za informacijskega pooblaščenca, so določene v členu 71 zakona o varstvu podatkov iz leta 2018. Ta pooblaščena oseba mora pri opravljanju nalog upoštevati tveganja, povezana z dejavnostmi obdelave, ter pri tem upoštevati naravo, obseg, okoliščine in namene obdelave.

2.5 **Nadzor in zagotavljanje skladnosti**

2.5.1 *Neodvisen nadzor*

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

(94) V Združenem kraljestvu nadzor in zagotavljanje skladnosti z UK GDPR in zakonom o varstvu podatkov iz leta 2018 izvaja informacijski pooblaščenec ([155]). Informacijski pooblaščenec nadzoruje tudi, kako osebne podatke obdelujejo pristojni organi, kar spada na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018 ([156]). Informacijski pooblaščenec je „Corporation Sole“, tj. ločen enoosebni pravni subjekt. Pri delu mu pomaga urad. Urad informacijskega pooblaščenca je imel 31. marca 2020 768 stalnih članov osebja ([157]). Podporno ministrstvo informacijskega pooblaščenca je ministrstvo za digitalne tehnologije, kulturo, medije in šport ([158]).

([153]) Člen 62 zakona o varstvu podatkov iz leta 2018.
([154]) Člen 69 zakona o varstvu podatkov iz leta 2018.
([155]) Člen 36(2)(b) Direktive (EU) 2016/680.
([156]) Člen 116 zakona o varstvu podatkov iz leta 2018.
([157]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2019–2020 sta na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.
([158]) Odnosi med njima so urejeni s sporazumom o upravljanju. Ključne odgovornosti ministrstva za digitalne tehnologije, kulturo, medije in šport kot podpornega ministrstva so zlasti: zagotavljanje ustreznega financiranja in ustreznih virov uradu informacijskega pooblaščenca; zastopanje interesov urada informacijskega pooblaščenca v parlamentu in drugih vladnih službah; zagotavljanje trdnega nacionalnega okvira varstva podatkov ter zagotavljanje smernic in podpore uradu informacijskega pooblaščenca v zvezi s poslovnimi vprašanji, kot so vprašanja nepremičnin, najemov in nabav (sporazum o upravljanju za obdobje 2018–2021 je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Neodvisnost informacijskega pooblaščenca je izrecno določena v členu 52 UK GDPR, ki v ničemer bistveno ne spreminja člena 52(1) do (3) Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta ([159]). Informacijski pooblaščenec mora pri opravljanju svojih nalog in izvajanju svojih pooblastil v skladu z UK GDPR ravnati popolnoma neodvisno, ne sme biti izpostavljen niti neposrednemu niti posrednemu zunanjemu vplivu ter ne sme nikogar prositi za navodila niti jih od nikogar sprejemati. Poleg tega se mora vzdržati vsakega delovanja, ki je nezdružljivo z njegovimi dolžnostmi, in se v času svojega mandata ne sme ukvarjati z nobenim nezdružljivim delom, bodisi profitnim bodisi neprofitnim.

(96) Pogoji za imenovanje in razrešitev informacijskega pooblaščenca so določeni v dodatku 12 k zakonu o varstvu podatkov iz leta 2018. Informacijskega pooblaščenca imenuje kraljica na podlagi priporočila vlade ter na podlagi poštenega in odprtega postopka izbire. Kandidat mora imeti ustrezne kvalifikacije, izkušnje in znanje. V skladu s kodeksom upravljanja v zvezi z javnimi imenovanji ([160]) seznam ustreznih kandidatov pripravi svetovalni ocenjevalni odbor. Preden minister za digitalne tehnologije, kulturo, medije in šport sprejme končno odločitev, mora zadevni izbrani parlamentarni odbor opraviti preverjanje pred imenovanjem. Mnenje odbora se javno objavi ([161]).

(97) Mandat informacijskega pooblaščenca traja največ sedem let. Informacijskega pooblaščenca lahko s funkcije razreši kraljica, na podlagi nagovora obeh domov parlamenta ([162]). Predloga za razrešitev informacijskega pooblaščenca ni mogoče predložiti nobenemu od domov parlamenta brez poročila, ki ga pristojni minister predloži temu domu, iz katerega izhaja, da je po njegovem mnenju informacijski pooblaščenec kriv hujše kršitve dolžnega ravnanja uradnih oseb in/ali da ne izpolnjuje več pogojev za opravljanje svoje funkcije ([163]).

(98) Financiranje informacijskega pooblaščenca temelji na treh virih: (i) pristojbine za varstvo podatkov, ki jih plačujejo upravljavci in so določene s predpisi pristojnega ministra ([164]), ki znašajo od 85 % do 90 % letnega proračuna urada ([165]), (ii) nepovratna sredstva, ki jih informacijskemu pooblaščencu nameni vlada in s katerimi se financirajo predvsem operativni stroški informacijskega pooblaščenca v zvezi z nalogami, ki se ne nanašajo na varstvo podatkov ([166]), ter (iii) pristojbine, ki se zaračunavajo za opravljanje storitev ([167]). Trenutno se take pristojbine ne zaračunavajo.

(99) Splošne naloge informacijskega pooblaščenca v zvezi z obdelavo osebnih podatkov, ki spada na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018, so določene v dodatku 13 k zakonu o varstvu podatkov iz leta 2018. Mednje spadajo nadzor in izvajanje dela 3 zakona o varstvu podatkov iz leta 2018, večje ozaveščanje javnosti, svetovanje parlamentu, vladi in drugim institucijam o zakonodajnih in upravnih ukrepih, ozaveščanje upravljavcev in obdelovalcev o njihovih obveznostih, zagotavljanje informacij posameznikom, na katere se nanašajo

([159]) Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1).

([160]) Kodeks upravljanja v zvezi z javnimi imenovanji (Governance Code on Public Appointments) je na voljo na povezavi: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

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

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

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

([164]) Člen 137 zakona o varstvu podatkov iz leta 2018.

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

([166]) V sporazumu o upravljanju je pojasnjeno, da „lahko pristojni minister opravi izplačila informacijskemu pooblaščencu iz sredstev, ki jih zagotovi parlament na podlagi odstavka 9 dodatka 12 k zakonu o varstvu podatkov iz leta 2018. Ministrstvo za digitalne tehnologije, kulturo, medije in šport po posvetovanju z informacijskim pooblaščencem temu izplača odobrene zneske (nepovratna sredstva) za kritje upravnih stroškov urada informacijskega pooblaščenca ter opravljanje nalog informacijskega pooblaščenca v zvezi s številnimi posebnimi nalogami, vključno z zagotavljanjem svobode obveščanja“ (sporazum o upravljanju za obdobje 2018–2021, odstavek 1.12, glej opombo 158).

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

osebni podatki, o uveljavljanju njihovih pravic in izvajanje preiskav. Informacijskemu pooblaščencu zaradi vzdrževanja neodvisnosti sodstva ni dovoljeno izvajati nalog v zvezi z obdelavo osebnih podatkov, ki jo izvaja posameznik, kolikor opravlja zadeve iz sodne pristojnosti, ali sodišče, kolikor opravlja zadeve iz sodne pristojnosti. Nadzor nad sodstvom pa je zagotovljen prek posebnih organov, opisanih v nadaljevanju.

2.5.1.1 Izvrševanje, vključno s sankcijami

(100) Informacijski pooblaščenec ima splošna preiskovalna in popravljalna pooblastila, pooblastila v zvezi z dovoljenji in svetovalnimi pristojnostmi, ki se nanašajo na obdelavo osebnih podatkov, za katero se uporablja del 3 zakona o varstvu podatkov iz leta 2018. Ima pooblastila, da upravljavca ali obdelovalca uradno obvesti o domnevni kršitvi dela 3, da upravljavcu ali obdelovalcu izda opozorilo, da bi predvidena dejanja obdelave verjetno kršila določbe dela 3, in da upravljavcu ali obdelovalcu izreče opomin, kadar so bile z dejanji obdelave kršene določbe te dela 3. Poleg tega lahko na lastno pobudo ali na zahtevo izdaja mnenja za parlament, vlado ali druge institucije in organe Združenega kraljestva ter javnost o vseh zadevah, povezanih z varstvom osebnih podatkov ([168]).

(101) Informacijski pooblaščenec je prav tako pristojen, da:

— upravljavcu in obdelovalcu (ter v določenih okoliščinah vsaki drugi osebi) predloži potrebne informacije z izdajo obvestila o predložitvi informacij (v nadaljnjem besedilu: obvestilo o predložitvi informacij) ([169]),

— izvaja preiskave in preglede z izdajo obvestila o preverjanju, na podlagi katerega mora upravljavec ali obdelovalec informacijskemu pooblaščencu morda dovoliti vstop v določene prostore, pregled ali proučitev dokumentov ali opreme, razgovore z osebami, ki obdelujejo osebne podatke v imenu upravljavca (v nadaljnjem besedilu: obvestilo o preverjanju ([170])),

— na drug način pridobi dostop do dokumentov upravljavcev in obdelovalcev ter dostop v njihove prostore, v skladu s členom 154 zakona o varstvu podatkov iz leta 2018 (v nadaljnjem besedilu: pristojnost za vstop in pregled),

— izvaja popravljalna pooblastila, tudi na podlagi opozoril in opominov ali z izdajo odredb v obliki obvestil o izvršitvi, s katerimi od upravljavcev/obdelovalcev zahteva določeno ukrepanje ali prenehanje izvajanja določenih ukrepov (v nadaljnjem besedilu: obvestil o izvršitvi) ([171]), ter

— izreka upravne globe v obliki plačilnega naloga (v nadaljnjem besedilu: obvestilo o plačilnem nalogu) ([172]).

(102) V politiki urada informacijskega pooblaščenca o regulativnih ukrepih (Regulatory Action Policy) so določene okoliščine, v katerih se izda obvestilo o predložitvi informacij, obvestilo o ocenjevanju, obvestilo o izvršitvi oziroma obvestilo o plačilnem nalogu ([173]). Z obvestilom o izvršitvi se lahko naložijo zahteve, za katere informacijski pooblaščenec meni, da so ustrezne za odpravo pomanjkljivosti. Z obvestilom o plačilnem nalogu se zahteva, da mora oseba informacijskemu pooblaščencu plačati znesek, naveden v obvestilu. Tako obvestilo se lahko izda, če niso izpolnjene določene določbe zakona o varstvu podatkov iz leta 2018 ([174]), lahko pa se izda tudi upravljavcu ali obdelovalcu, ki ni spoštoval obvestila o predložitvi informacij, obvestila o ocenjevanju ali obvestila o izvršitvi.

(103) Natančneje, informacijski pooblaščenec mora pri odločanju o tem, ali naj upravljavcu ali obdelovalcu izda obvestilo o plačilnem nalogu in kako visoka naj bo kazen, upoštevati navedbe iz člena 155(3) zakona o varstvu podatkov iz leta 2018, vključno z naravo in težo kršitve, dejstvom, ali je kršitev naklepna ali posledica malomarnosti, ukrepi, ki jih je sprejel upravljavec ali obdelovalec, da bi omilil škodo, ki so jo utrpeli posamezniki, na katere se nanašajo

([168]) Odstavek 2 dodatka 13 k zakonu o varstvu podatkov iz leta 2018.
([169]) Člen 142 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 143 zakona o varstvu podatkov iz leta 2018).
([170]) Člen 146 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 147 zakona o varstvu podatkov iz leta 2018).
([171]) Členi 149 do 151 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 152 zakona o varstvu podatkov iz leta 2018).
([172]) Člen 155 zakona o varstvu podatkov iz leta 2018 (ob upoštevanju omejitev iz člena 156 zakona o varstvu podatkov iz leta 2018).
([173]) Politika o regulativnih ukrepih je na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Urad informacijskega pooblaščenca lahko obvestilo o plačilnem nalogu izda zlasti zaradi kršitve iz člena 149(2), (3), (4) ali (5) zakona o varstvu podatkov iz leta 2018.

osebni podatki, stopnjo odgovornosti upravljavca ali obdelovalca (ob upoštevanju tehničnih in organizacijskih ukrepov, ki jih je sprejel eden ali drugi), vsemi zadevnimi predhodnimi kršitvami upravljavca ali obdelovalca, kategorijami osebnih podatkov, na katere vpliva kršitev, ter dejstvom, ali bi bila kazen učinkovita, sorazmerna in odvračilna.

(104) Najvišji znesek kazni, ki se lahko naloži z obvestilom o plačilnem nalogu, znaša (a) 17 500 000 GBP zaradi neizpolnitve načel o varstvu podatkov (členi 35, 36 in 37, člena 38(1) in 39(1) ter člen 40 zakona o varstvu podatkov iz leta 2018), obveznosti glede preglednosti in pravic posameznikov (členi 44, 45, 46, 47, 48, 49, 52 in 53 zakona o varstvu podatkov iz leta 2018) ter načel o mednarodnih prenosih osebnih podatkov (členi 73, 75, 76, 77 ali 78 zakona o varstvu podatkov iz leta 2018) in (b) 8 700 000 GBP za kršitve po preostalih členih ([175]). V primeru neizpolnitve obvestila o predložitvi informacij, obvestila o ocenjevanju ali obvestila o izvršitvi je najvišji znesek kazni, ki se lahko izreče na podlagi obvestila o plačilnem nalogu 17 500 000 GBP.

(105) Informacijski pooblaščenec je glede na zadnji letni poročili (za obdobji 2018–2019 ([176]) in 2019–2020 ([177])) izvedel številne preiskave v zvezi z obdelavo osebnih podatkov s strani organov preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Oktobra 2019 je na primer izvedel preiskavo in objavil mnenje v zvezi z uporabo tehnologije za prepoznavanje obrazov na javnih mestih na področju preprečevanja, odkrivanja in preiskovanja kaznivih dejanj. Preiskava je bila usmerjena zlasti na uporabo zmogljivosti prepoznavanja obrazov v živo v policiji južnega Walesa in londonski policiji (Metropolitan Police Service). Informacijski pooblaščenec je nadalje preiskoval „Gangs matrix“ (matrika tolp) ([178]) londonske policije in ugotovil vrsto resnih kršitev zakonodaje o varstvu podatkov, ki bi verjetno omajale zaupanje javnosti v matriko in uporabo podatkov.

(106) Novembra 2018 je informacijski pooblaščenec izdal obvestilo o izvršitvi, londonska policija pa je nato sprejela ukrepe, potrebne za povečanje varnosti in odgovornosti ter zagotovitev sorazmerne uporabe podatkov.

(107) Drug primer nedavnega izvršilnega ukrepa je globa v višini 325 000 GBP, ki jo je informacijski pooblaščenec maja 2018 naložil državnemu tožilstvu zaradi izgube nešifriranega DVD-ja s posnetki informativnih razgovorov pri policiji. Poleg tega je informacijski pooblaščenec izvedel preiskave širših tem, na primer v prvi polovici leta 2020 o uporabi pridobivanja podatkov iz mobilnega telefona za policijske namene ter obdelavi podatkov žrtev s strani policije.

(108) Poleg navedenih pooblastil informacijskega pooblaščenca za izvrševanje se določene kršitve zakonodaje o varstvu podatkov štejejo za kazniva dejanja, zato se lahko zanje izrečejo kazenske sankcije (člen 196 zakona o varstvu podatkov iz leta 2018). To se na primer nanaša na pridobitev ali razkritje osebnih podatkov brez privolitve upravljavca in zagotovitev razkritja osebnih podatkov drugi osebi brez privolitve upravljavca ([179]), ponovno identifikacijo informacij v primeru anonimizacije osebnih podatkov, brez privolitve upravljavca, ki je odgovoren za anonimizacijo osebnih podatkov ([180]), namerno oviranje informacijskega pooblaščenca pri izvrševanju njegovih pristojnosti v zvezi s preverjanjem osebnih podatkov v skladu z mednarodnimi obveznostmi ([181]), dajanje neresničnih izjav v odgovor na obvestilo o predložitvi informacij ali uničenje informacij v zvezi z obvestilom o predložitvi informacij ali obvestilom o ocenjevanju ([182]).

(109) Informacijski pooblaščenec ima v skladu s členom 139 zakona o varstvu podatkov iz leta 2018 tudi obveznost, da obema domovoma parlamenta predloži splošno poročilo o izvajanju svojih nalog na podlagi zakona ([183]).

([175]) Člen 157 zakona o varstvu podatkov iz leta 2018.

([176]) Letno poročilo in računovodski izkaz informacijskega pooblaščenca za obdobje 2018-2019 sta na voljo na povezavi: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Letno poročilo informacijskega pooblaščenca za obdobje 2019–2020 (glej opombo 157).

([178]) Zbirka podatkov, v kateri so bili evidentirani obveščevalni podatki v zvezi z domnevnimi člani tolp in žrtvami kaznivih dejanj, povezanih s tolpami.

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

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

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

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

([183]) Leto poročilo mora, kot je določeno v sporazumu o upravljanju: (i) zajemati korporacije, odvisna ali skupna podjetja pod nadzorom urada informacijskega pooblaščenca, (ii) spoštovati priročnik o finančnem poročanju (Financial Reporting Manual) finančnega ministrstva, (iii) vsebovati izjavo vlade s predstavitvijo načinov, na katere je računovodja upravljal in nadzoroval sredstva, ki so bila med letom porabljena za organizacijo, s čimer se pokaže, kako dobro organizacija obvladuje tveganja za dosego svojih ciljev, ter (iv) orisati glavne dejavnosti in učinkovitost v prejšnjem finančnem letu in v obliki povzetka določiti nadaljnje načrte (sporazum o upravljanju za obdobje 2018–2021, odstavek 3.26, glej opombo 158).

2.5.2 *Nadzor nad sodstvom*

(110) Nadzor nad obdelavo osebnih podatkov, ki jo izvajajo sodišča in sodstvo, je dvostranski. Kadar nosilec sodne funkcije ali sodišče ne opravlja zadev iz sodne pristojnosti, izvaja nadzor informacijski pooblaščenec. Kadar pa upravljavec deluje v okviru sodne pristojnosti, urad informacijskega pooblaščenca ne more izvajati nadzorne funkcije ([184]), zato jo izvajajo posebni organi. To izraža pristop iz člena 32 Direktive (EU) 2016/680.

(111) Natančneje, v drugem primeru glede sodišč Anglije in Walesa ter glede prvostopenjskih in višjih sodišč Anglije in Walesa tak nadzor zagotavlja sodni svet za varstvo podatkov (Judicial Data Protection Panel) ([185]). Poleg tega sta vodja sodstva Anglije in Walesa (Lord Chief Justice) in višji predsednik sodišč (Senior President of Tribunals) izdala obvestilo o zasebnosti ([186]), ki določa, kako sodišča v Angliji in Walesu obdelujejo osebne podatke za namene opravljanja sodne funkcije. Podobni obvestili sta izdali tudi sodstvo Severne Irske ([187]) in sodstvo Škotske ([188]).

(112) Poleg tega je na Severnem Irskem vodja sodstva Severne Irske sodnika sodišča High Court imenoval za sodnika, pristojnega za nadzor podatkov (Data Supervisory Judge) ([189]). Izdane so bile tudi smernice za sodstvo Severne Irske o tem, kako ravnati v primeru izgube ali potencialne izgube podatkov ter kako obravnavati vsa vprašanja, ki iz tega izhajajo ([190]).

(113) Na Škotskem je vodja sodstva (Lord President) imenoval sodnika za nadzor podatkov (Data Supervisory Judge) za obravnavo vseh pritožb s področja varstva podatkov. Ta sistem je vzpostavljen na podlagi pravil o pritožbah v sodstvu, podobnih tistim v Angliji in Walesu ([191]).

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

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

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

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

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

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

([189]) Sodnik, pristojen za nadzor podatkov, zagotavlja smernice sodstvu ter obravnava kršitve in/ali pritožbe v zvezi z obdelavo osebnih podatkov, ki jo izvajajo sodišča ali posamezniki, kolikor opravljajo zadeve iz sodne pristojnosti.

([190]) Če se šteje, da gre za resno pritožbo ali težjo kršitev, se zadeva predloži uradniku za obravnavo pritožb v sodstvu (Judicial Complaints Officer) v nadaljnjo obravnavo, v skladu s kodeksom ravnanja v primeru pritožb, ki ga je izdal vodja sodstva Severne Irske. Rezultat take pritožbe je lahko: da se ne sprejme noben nadaljnji ukrep, izdaja nasveta, usposabljanje ali mentorstvo, neuradno opozorilo, uradno opozorilo, zadnje opozorilo, omejitev delovanja ali napotitev pred sodišče, ustanovljeno na podlagi zakona. Kodeks ravnanja v primeru pritožb, ki ga je izdal vodja sodstva Severne Irske, je na voljo na povezavi: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp.._1.pdf.

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

2.5.3 *Pravna sredstva*

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

(116) Prvič, posameznik, na katerega se nanašajo osebni podatki, ima pravico vložiti pritožbo pri informacijskem pooblaščencu, če meni, da je v zvezi z osebnimi podatki, ki se nanašajo nanj, prišlo do kršitve dela 3 zakona o varstvu podatkov iz leta 2018 ([192]). Kot je opisano v uvodnih izjavah (100) in (109), lahko informacijski pooblaščenec preveri, kako upravljavec in obdelovalec zagotavljata skladnost z zakonom o varstvu podatkov iz leta 2018, od njiju zahteva, da v primeru neskladnosti sprejmeta potrebne ukrepe ali se vzdržita določenih ukrepov, ter naloži globe.

(117) Drugič, zakon o varstvu podatkov iz leta 2018 določa pravico do pravnega sredstva zoper odločitev informacijskega pooblaščenca. Če informacijski pooblaščenec pritožbe posameznika, na katerega se nanašajo osebni podatki, ne obravnava ([193]), ima pritožnik dostop do pravnega sredstva, saj lahko od sodišča prve stopnje zahteva ([194]), naj informacijskemu pooblaščencu naloži sprejetje ustreznih ukrepov v odziv na pritožbo ali obveščanje pritožnika o stanju zadeve ([195]). Poleg tega se lahko vsakdo, ki mu informacijski pooblaščenec izda enega od navedenih obvestil (o predložitvi informacij, o ocenjevanju, o izvršitvi ali o plačilnem nalogu), pritoži pri sodišču prve stopnje. Če sodišče ugotovi, da odločba informacijskega pooblaščenca ni v skladu s pravom ali da bi moral ta odločiti drugače, mora sodišče pritožbo dovoliti ali obvestilo oziroma odločbo informacijskega pooblaščenca nadomestiti z drugo ([196]).

(118) Tretjič, posamezniki lahko pravno sredstvo zoper upravljavce in obdelovalce uveljavljajo neposredno pred sodiščem v skladu s členom 167 zakona o varstvu podatkov iz leta 2018. Če sodišče na podlagi vloge posameznika, na katerega se nanašajo osebni podatki, ugotovi, da so bile kršene njegove pravice s področja zakonodaje o varstvu podatkov, lahko upravljavcu, ki je odgovoren za obdelavo takih podatkov, ali obdelovalcu, ki deluje v njegovem imenu, odredi sprejetje ali opustitev določenih ukrepov, navedenih v odločbi. Poleg tega je v skladu s členom 169 zakona o varstvu podatkov iz leta 2018 vsaka oseba, ki utrpi škodo zaradi kršitve zahteve iz zakonodaje o varstvu podatkov (vključno z delom 3 zakona o varstvu podatkov iz leta 2018), ki ni UK GDPR, upravičena do odškodnine za škodo, ki jo je povzročil upravljavec ali obdelovalec, razen če upravljavec ali obdelovalec dokaže, da nikakor ni odgovoren za dogodek, ki je povzročil škodo. Škoda vključuje finančno in nefinančno izgubo, kot je na primer stiska.

(119) Četrtič, vsakdo, ki meni, da so javni organi kršili njegove pravice, vključno s pravico do zasebnosti in do varstva podatkov, lahko uveljavlja pravna sredstva pred sodišči Združenega kraljestva na podlagi zakona o človekovih pravicah iz leta 1998. Upravljavci v skladu z delom 3 zakona o varstvu podatkov iz leta 2018, tj. pristojni organi, so vedno javni organi v smislu zakona o človekovih pravicah iz leta 1998. Posameznik, ki trdi, da je javni organ ravnal (ali predlaga ravnanje) neskladno s pravico iz Konvencije, kar je posledično nezakonito na podlagi člena 6(1) zakona o človekovih pravicah iz leta 1998, lahko pri pristojnem sodišču začne postopek zoper tak organ ali se na zadevne pravice sklicuje v vsakem pravnem postopku, če je (ali bi postal) žrtev nezakonitega dejanja ([197]).

([192]) Člen 165 zakona o varstvu podatkov iz leta 2018.

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

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

([195]) Člen 166 zakona o varstvu podatkov iz leta 2018.

([196]) Člena 161 in 162 zakona o varstvu podatkov iz leta 2018.

([197]) Glej sodbo Brown proti Commissioner of Police of the Metropolis iz leta 2016, v kateri je sodišče tožeči stranki v tožbi zoper policijo odredilo odškodnino v okviru varstva podatkov. Sodišče je razsodilo v korist tožeče stranke, tako da je ugodilo njenim zahtevkom v zvezi s kršitvijo obveznosti iz zakona o varstvu podatkov iz leta 1998, kršitvijo zakona o človekovih pravicah iz leta 1998 (in povezanih pravic iz člena 8 EKČP) ter škodnim dejanjem zlorabe zasebnih informacij (tožena stranka je nazadnje priznala, da je kršila zakon o varstvu podatkov in EKČP, zato se je sodba usmerila na določitev primernega pravnega sredstva). Zaradi teh kršitev je sodišče tožeči stranki dodelilo denarno odškodnino.

(120) Če sodišče ugotovi, da je katero koli dejanje javnega organa nezakonito, lahko odobri odškodnino ali pravno sredstvo ali izda odredbo, za katero je pristojen in kot meni, da je pravično in ustrezno ([198]). Sodišče lahko odloči tudi, da določba primarne zakonodaje ni skladna s pravico, zagotovljeno na podlagi EKČP.

(121) Nazadnje, ko posameznik izčrpa nacionalna pravna sredstva, se lahko obrne na Evropsko sodišče za človekove pravice zaradi kršitev pravic, zagotovljenih na podlagi EKČP.

2.6 **Nadaljnja izmenjava**

(122) Pravo Združenega kraljestva pod določenimi pogoji dovoljuje izmenjavo podatkov med organom za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in drugimi organi Združenega kraljestva za namene, ki se razlikujejo od tistih, za katere so bili podatki prvotno zbrani (tako imenovana nadaljnja izmenjava).

(123) Člen 36(3) zakona o varstvu podatkov iz leta 2018 po vzoru člena 4(2) Direktive (EU) 2016/680 omogoča nadaljnjo obdelavo osebnih podatkov (s strani prvotnega ali drugega upravljavca), ki jih pristojni organ zbere za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, za kateri koli drug namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni drug namen ter če je obdelava potrebna in sorazmerna ([199]). V takem primeru se vsi zaščitni ukrepi, navedeni v delu 3 zakona o varstvu podatkov iz leta 2018 in analizirani zgoraj, uporabljajo za obdelavo, ki jo izvaja organ prejemnik.

(124) V okviru pravnega reda Združenega kraljestva različni zakoni izrecno omogočajo nadaljnjo izmenjavo. Zlasti (i) zakon o digitalnem gospodarstvu iz leta 2017 (Digital Economy Act 2017) omogoča izmenjavo med javnimi organi za več namenov, na primer v primeru goljufije zoper javni sektor, ki vključuje izgubo ali tveganje izgube za javni organ ([200]), ali v primeru dolga javnemu organu ali državi ([201]); (ii) zakon o kriminalu in sodiščih iz leta 2013 (Crime and Courts Act 2013), ki omogoča izmenjavo informacij z nacionalno agencijo za boj proti kriminalu (National Crime Agency) ([202]) za namene boja proti hudim kaznivim dejanjem in organiziranemu kriminalu ter preiskovanja in pregona hudih kaznivih dejanj in organiziranega kriminala; (iii) zakon o hudih kaznivih dejanjih iz leta 2007 (Serious Crime Act 2007), ki javnim organom omogoča, da razkrijejo informacije organizacijam za boj proti goljufijam zaradi preprečevanja goljufij ([203]).

(125) Ti zakoni izrecno določajo, da mora biti izmenjava informacij v skladu z načeli iz zakona o varstvu podatkov iz leta 2018. Poleg tega je poklicni organ uslužbencev policije izdal dokument o odobreni strokovni praksi glede izmenjave informacij ([204]), ki je policiji v pomoč pri izpolnjevanju njenih obveznosti glede varstva podatkov na podlagi UK GDPR, zakona o varstvu podatkov in zakona o človekovih pravicah iz leta 1998. Skladnost izmenjave informacij s pravnim okvirom varstva podatkov, ki se uporablja, je seveda stvar sodne presoje ([205]).

(126) Nadalje, zakon o varstvu podatkov iz leta 2018 podobno kot člen 9 Direktive (EU) 2016/680 določa, da se lahko osebni podatki, zbrani za kateri koli namen preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, obdelujejo za namene, ki ne spadajo na področje preprečevanja, odkrivanja in preiskovanja kaznivih dejanj, če tako obdelavo omogoča zakon ([206]). Ta vrsta izmenjave vključuje dva primera: (1) ko organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj posreduje podatke organu z drugega področja, ki ni obveščevalna agencija (na primer

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

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

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

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

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

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

([204]) Smernice o dovoljeni strokovni praksi glede izmenjave informacij so na voljo na povezavi: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

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

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

finančnemu ali davčnemu organu, organu za varstvo konkurence, socialnemu uradu za mladoletnike itd.), ter (2) ko organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj podatke posreduje obveščevalni agenciji. V prvem primeru obdelava osebnih podatkov spada na področje uporabe UK GDPR ter dela 2 zakona o varstvu podatkov iz leta 2018. Kot je določeno v sklepu, sprejetem v skladu z Uredbo (EU) 2016/679, je z zaščitnimi ukrepi iz UK GDPR in dela 2 zakona o varstvu podatkov iz leta 2018 zagotovljena raven varstva, v osnovi enakovredna tisti, ki se zagotavlja v Uniji ([207]).

(127) V drugem primeru, tj. glede izmenjave podatkov, ki jih organ za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj zbere ter posreduje obveščevalni agenciji za namene nacionalne varnosti, pa je pravna podlaga za izmenjavo člen 19 zakona o boju proti terorizmu iz leta 2008 (Counter Terrorism Act 2008) ([208]). Na podlagi navedenega zakona iz leta 2008 lahko vsaka oseba daje informacije kateri koli obveščevalni službi za namene izvrševanja katere koli naloge take službe, vključno z „nacionalno varnostjo“.

(128) Glede pogojev, na podlagi katerih je mogoča izmenjava podatkov za namene nacionalne varnosti, zakon o obveščevalnih službah (Intelligence Services Act) in zakon o varnostnih službah (Security Services Act) omejujeta zmožnost obveščevalnih služb za pridobivanje podatkov na tisto, kar je potrebno za izvrševanje njihovih zakonskih nalog. Pristojni organi, ki spadajo na področje uporabe dela 3 zakona o varstvu podatkov iz leta 2018, ki želijo posredovati podatke obveščevalnim službam, morajo poleg zakonskih nalog agencij, navedenih v zakonu o obveščevalnih službah in zakonu o varnostnih službah, proučiti več dejavnikov oziroma upoštevati več omejitev ([209]). Člen 20 zakona o boju proti terorizmu iz leta 2008 jasno določa, da mora biti vsaka izmenjava podatkov na podlagi člena 19 tega zakona v skladu z zakonodajo o varstvu podatkov; to pomeni, da se uporabljajo vse omejitve in zahteve iz dela 3 zakona o varstvu podatkov iz leta 2018. Nadalje, organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter obveščevalne službe so javni organi za namen zakona o človekovih pravicah iz leta 1998, ki si morajo zato prizadevati, da bi ravnali skladno s pravicami, zagotovljenimi na podlagi EKČP, vključno iz njenega člena 8. Povedano drugače, te zahteve pomenijo, da je vsakršna izmenjava podatkov med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in obveščevalnimi službami skladna z zakonodajo o varstvu podatkov in z EKČP.

(129) Pri obdelavi osebnih podatkov, prejetih od organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj, ki jo izvajajo obveščevalne službe za namene nacionalne varnosti, veljajo številni pogoji in zaščitni ukrepi ([210]). Del 4 zakona o varstvu podatkov iz leta 2018 se uporablja za vse primere obdelave, ki jih izvajajo obveščevalne službe ali

([207]) Izvedbeni sklep Komisije v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu (C(2021) 4800).

([208]) Člen 19 zakona iz leta 2008 o hudih kaznivih dejanjih, ki je na voljo na povezavi: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) Člen 2(2) zakona o obveščevalnih službah iz leta 1994 (glej spletno mesto: https://www.legislation.gov.uk/ukpga/1994/13/contents) določa, da je „vodja obveščevalne službe odgovoren za učinkovitost navedene službe ter da je njegova dolžnost zagotoviti: (a) ureditev, ki omogoča, da lahko obveščevalna služba prejme le tiste informacije, ki so potrebne za ustrezno izvajanje njenih nalog, ter da lahko razkrije le tiste informacije, ki so potrebne (i) za navedeni namen, (ii) za namene nacionalne varnosti, (iii) za namene preprečevanja ali odkrivanja hudih kaznivih dejanj, ali (iv) za namene katerega koli kazenskega postopka; ter (b) da obveščevalna služba ne sme izvajati nobenih ukrepov v korist katere koli politične stranke v Združenem kraljestvu“; člen 2(2) zakona o varnostnih službah iz leta 1989 (glej spletno mesto: https://www.legislation.gov.uk/ukpga/1989/5/contents) pa določa, da je „generalni direktor odgovoren za učinkovitost službe ter da mora zagotoviti: (a) ureditev, ki zagotavlja, da lahko služba prejme le tiste informacije, ki so potrebne za ustrezno izvajanje njenih nalog, ter da lahko razkrije le tiste informacije, ki so potrebne za navedeni namen ali namen [preprečevanja ali odkrivanja] hudih kaznivih dejanj [ali katerega koli kazenskega postopka]; (b) da služba ne sme izvajati nobenih ukrepov v korist katere koli politične stranke ter (c) ureditev, v dogovoru z generalnim direktorjem nacionalne agencije za boj proti kriminalu, glede usklajevanja dejavnosti službe na podlagi člena 1(4) tega zakona z dejavnostmi policije, nacionalne agencije za boj proti kriminalu in drugimi organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj“.

([210]) Zaščitni ukrepi in omejitve pooblastil obveščevalnih služb so urejeni tudi z zakonom o preiskovalnih pooblastilih iz leta 2016, ki skupaj z zakonom o urejanju preiskovalnih pooblastil iz leta 2000 (Regulation of Investigatory Powers Act 2000) za Anglijo, Wales in Severno Irsko ter zakonom o urejanju preiskovalnih pooblastil (Škotska) iz leta 2000 (Regulation of Investigatory Powers (Scotland) Act 2000) za Škotsko zagotavlja pravno podlago za uporabo takih pooblastil. Vendar ta pooblastila v primeru nadaljnje izmenjave niso pomembna, saj zajemajo neposredno zbiranje osebnih podatkov s strani obveščevalnih agencij. Za oceno pooblastil, ki so na podlagi zakona o preiskovalnih pooblastilih podeljena obveščevalnim agencijam, gej Izvedbeni sklep Komisije v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta o ustreznem varstvu osebnih podatkov v Združenem kraljestvu (C(2021) 4800).

ki se izvajajo v njihovem imenu. Določa zlasti glavna načela o varstvu podatkov (zakonitost, poštenost in preglednost ([211]); omejitev namena ([212]), najmanjši obseg podatkov ([213]), točnost ([214]); omejitev hrambe ([215]) in varnost ([216])), določa tudi pogoje glede obdelave posebnih vrst podatkov ([217]) in pravice posameznikov, na katere se nanašajo osebni podatki ([218]), vsebuje zahtevo o vgrajenem varstvu podatkov ([219]) ter ureja mednarodni prenos osebnih podatkov ([220]).

(130) Hkrati člen 110 zakona o varstvu podatkov iz leta 2018 določa izjemo od posebnih določb v delu 4 zakona o varstvu podatkov iz leta 2018, kadar je taka izjema potrebna za zaščito nacionalne varnosti. Člen 110(2) zakona o varstvu podatkov iz leta 2018 navaja seznam določb, pri katerih je mogoče uporabiti izjemo. Med njimi so načela o varstvu podatkov (razen načela zakonitosti), pravice posameznika, na katerega se nanašajo osebni podatki, obveznost obveščanja informacijskega pooblaščenca o kršitvi varnosti podatkov, inšpekcijska pooblastila informacijskega pooblaščenca v skladu z mednarodnimi obveznostmi, določena pooblastila informacijskega pooblaščenca za izvrševanje, določbe, na podlagi katerih se nekatere kršitve varnosti podatkov štejejo za kaznivo dejanje, in določbe, ki se nanašajo na posebne namene obdelave, na primer za novinarske, akademske ali umetniške namene. To izjemo je mogoče uporabiti le na podlagi analize vsakega primera posebej ([221]). Kot so pojasnili organi Združenega kraljestva in je bilo potrjeno s sodno prakso sodišč Združenega kraljestva, „(a) mora upravljavec upoštevati dejanske posledice za nacionalno varnost ali obrambo, če bi moral zagotoviti skladnost s posamezno določbo za varstvo podatkov, ter to, ali bi lahko razumno zagotovil skladnost z običajnim pravilom brez ogrožanja nacionalne varnosti ali obrambe“ ([222]). Urad informacijskega pooblaščenca nadzoruje, ali je bila izjema ustrezno uporabljena ali ne ([223]).

([211]) V skladu s členom 86(6) zakona o varstvu podatkov iz leta 2018 je treba pri ugotavljanju poštenosti in preglednosti obdelave upoštevati tudi metodo pridobitve podatkov. V tem smislu je zahteva glede poštenosti in preglednosti izpolnjena, če so podatki pridobljeni od osebe, ki je zakonito pooblaščena, da jih lahko zagotovi, ali ki jih na podlagi zakona mora zagotoviti.

([212]) V skladu s členom 87 zakona o varstvu podatkov iz leta 2018 mora biti namen obdelave specifičen, izrecen in zakonit. Podatki se ne smejo obdelovati na način, ki ni skladen z nameni, za katere so bili zbrani. V skladu s členom 87(3) je nadaljnja obdelava osebnih podatkov dovoljena le, če je upravljavec po zakonu pooblaščen za obdelavo podatkov za navedeni namen ter če je obdelava potrebna in sorazmerna z navedenim drugim namenom. Obdelava se šteje za skladno, če se izvaja za namene arhiviranja v javnem interesu, za namene znanstvenih ali zgodovinskih raziskav ali za statistične namene in če zanjo veljajo ustrezni zaščitni ukrepi (člen 87(4) zakona o varstvu podatkov iz leta 2018).

([213]) Osebni podatki morajo biti ustrezni, relevantni in ne čezmerni (člen 88 zakona o varstvu podatkov iz leta 2018).

([214]) Osebni podatki morajo biti točni in posodobljeni (člen 89 zakona o varstvu podatkov iz leta 2018).

([215]) Osebni podatki se ne smejo shranjevati dlje, kot je potrebno (člen 90 zakona o varstvu podatkov iz leta 2018).

([216]) Šesto načelo o varstvu podatkov je, da je treba osebne podatke obdelovati tako, da so upoštevani ustrezni zaščitni ukrepi glede tveganj, ki izhajajo iz obdelave osebnih podatkov. Tveganja med drugim vključujejo nenameren ali nepooblaščen dostop do osebnih podatkov, njihovo uničenje, izgubo, uporabo, spreminjanje ali razkritje (člen 91 zakona o varstvu podatkov iz leta 2018). Člen 107 zahteva tudi, da (1) mora vsak upravljavec vzpostaviti ustrezne zaščitne ukrepe, ki so primerni glede na tveganja, ki izhajajo iz obdelave osebnih podatkov, (2) v primeru avtomatizirane obdelave pa mora vsak upravljavec in vsak obdelovalec na podlagi ocene tveganja vzpostaviti preventivne ukrepe ali ukrepe za zmanjšanje tveganja.

([217]) Člen 86(2)(b) in dodatek 10 k zakonu o varstvu podatkov iz leta 2018.

([218]) V skladu s poglavjem 3 dela 4 zakona o varstvu podatkov iz leta 2018 gre predvsem za te pravice: za pravico do dostopa, pravico do popravka in izbrisa, pravico do ugovora obdelavi, pravico, da se za posameznika ne uporablja avtomatizirano sprejemanje odločitev, pravico poseči v avtomatizirano sprejemanje odločitev in pravico do obveščanja o sprejemanju odločitev. Poleg tega mora upravljavec posameznika, na katerega se nanašajo osebni podatki, obvestiti o obdelavi njegovih osebnih podatkov.

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

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

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

([222]) Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek H: Okvir varstva podatkov s področja državne varnosti in preiskovalnih pristojnosti, strani 15–16, ki je na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Glej tudi sodbo v zadevi Baker proti Secretary of State (glej opombo 220), v kateri je sodišče razveljavilo potrdilo o omejitvah iz razlogov nacionalne varnosti, ki ga je izdal minister za notranje zadeve in ki je potrjevalo uporabo izjeme na podlagi nacionalne varnosti, saj je menilo, da ni razloga, da bi se dovolila splošna izjema od obveznosti odziva na zahteve za dostop do podatkov, ter da bi omogočanje take izjeme v vseh okoliščinah brez analize vsakega primera posebej presegalo tisto, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

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

(131) Nadalje, v zvezi z možnostjo omejitve uporabe navedenih posebnih pravic zaradi zaščite nacionalne varnosti je v členu 79 zakona o varstvu podatkov iz leta 2018 določeno, da lahko upravljavec zaprosi za izdajo potrdila, ki ga podpiše vladni minister ali generalni državni tožilec in ki potrjuje, da je, ali je kadar koli bila, omejitev takih pravic potreben in sorazmeren ukrep za zaščito nacionalne varnosti ([224]). Vlada Združenega kraljestva je izdala smernice za potrdila o omejitvah iz razlogov nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018, ki zlasti poudarjajo, da morajo biti vse omejitve pravic posameznikov, na katere se nanašajo osebni podatki, zaradi zaščite nacionalne varnosti sorazmerne in potrebne ([225]). Vsa potrdila o omejitvah iz razlogov nacionalne varnosti morajo biti objavljena na spletišču urada informacijskega pooblaščenca ([226]).

(132) Potrdilo se izda za določen čas največ pet let, da ga lahko izvršilna oblast redno preverja ([227]). Potrdilo opredeljuje osebne podatke ali kategorije osebnih podatkov, za katere se uporabi izjema, ter določbe zakona o varstvu podatkov iz leta 2018, ki jih zadeva izjema ([228]).

(133) Pomembno je omeniti, da potrdila o omejitvah iz razlogov nacionalne varnosti niso dodatni razlog za omejitev pravic do varstva podatkov iz razlogov nacionalne varnosti. Z drugimi besedami, upravljavec ali obdelovalec se lahko na potrdilo sklicuje le, če ugotovi, da se je treba sklicevati na izjemo zaradi nacionalne varnosti, kar pa mora uporabiti za vsak primer posebej. Tudi če se potrdilo o omejitvah iz razlogov nacionalne varnosti nanaša na posamezno zadevo, lahko urad informacijskega pooblaščenca prouči, ali je bilo v posameznem primeru sklicevanje na izjemo zaradi nacionalne varnosti upravičeno ([229]).

(134) Oseba, ki je neposredno prizadeta zaradi izdaje potrdila, se lahko zaradi tega ([230]) pritoži pri sodišču Upper Tribunal ([231]), če so v potrdilu podatki opredeljeni s splošnim opisom, pa lahko izpodbija uporabo potrdila glede posameznih podatkov ([232]).

(135) Sodišče prouči odločitev o izdaji potrdila in odloči, ali so za izdajo potrdila obstajali utemeljeni razlogi ([233]). Prouči lahko več vprašanj, vključno s potrebnostjo, sorazmernostjo in zakonitostjo, upošteva vpliv na pravice posameznikov, na katere se nanašajo podatki, in pretehta potrebo po zaščiti nacionalne varnosti. Posledično lahko sodišče ugotovi, da se potrdilo ne nanaša na določene osebne podatke, ki so predmet pritožbe ([234]).

([224]) Z zakonom o varstvu podatkov iz leta 2018 je bila ukinjena možnost izdaje potrdila na podlagi člena 28(2) zakona o varstvu podatkov iz leta 1998. Vendar pa možnost izdajanja „starih potrdil“ še vedno obstaja, in sicer v obsegu, kot to izhaja iz možnosti, ki zgodovinsko obstaja na podlagi zakona iz leta 1998 (glej odstavek 17 dela 5 dodatka 20 k zakonu o varstvu podatkov iz leta 2018). Vendar se zdi ta možnost zelo redka in velja samo v omejenem številu primerov, na primer kadar oseba, na katero se nanašajo podatki, izpodbija uporabo izjeme iz razlogov nacionalne varnosti v zvezi z obdelavo s stani javnega organa, ki je obdelavo izvedel v skladu z zakonom iz leta 1998. Treba je omeniti, da se bo v teh primerih v celoti uporabljal člen 28 zakona o varstvu podatkov iz leta 1998, vključno z možnostjo, da lahko posameznik, na katerega se nanašajo podatki, izpodbija potrdilo. Trenutno ne obstaja nobeno potrdilo o omejitvah iz razlogov nacionalne varnosti, izdano na podlagi zakona o varstvu podatkov iz leta 1998.

([225]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti na podlagi zakona o varstvu podatkov iz leta 2018 (UK Government Guidance on National Security Certificates under the Data Protection Act 2018) so na voljo na povezavi: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

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

([227]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti, odstavek 15, glej opombo 225.

([228]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti, odstavek 5, glej opombo 225.

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

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

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

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

([233]) V zadevi Baker proti Secretary of State (glej opombo 221) je sodišče Information Tribunal razveljavilo potrdilo o omejitvah iz razlogov nacionalne varnosti, ki ga je izdal minister za notranje zadeve, saj je menilo, da ni razloga, da bi se dovolila splošna izjema od obveznosti odziva na zahteve za dostop do podatkov, ter da bi omogočanje take izjeme v vseh okoliščinah brez analize vsakega primera posebej, presegalo tisto, kar je potrebno in sorazmerno za zaščito nacionalne varnosti.

([234]) Smernice vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti, odstavek 25, glej opombo 224.

(136) Druga vrsta morebitnih omejitev se nanaša na tiste, ki se na podlagi dodatka 11 k zakonu o varstvu podatkov iz leta 2018, nanašajo na nekatere določbe dela 4 zakona o varstvu podatkov iz leta 2018 ([235]), da bi se zaščitili drugi pomembni cilji splošnega javnega interesa ali zaščiteni interesi, kot so na primer parlamentarni privilegij, varovanje zaupnosti sporazumevanja med odvetnikom in stranko, vodenje sodnega postopka ali bojna učinkovitost oboroženih sil. Uporaba teh določb je izvzeta za določene vrste informacij (izjema na podlagi vrste) ali če bi uporaba teh določb verjetno posegala v zaščitene interese (izjema na podlagi poseganja) ([236]). Na izjeme na podlagi poseganja se je mogoče sklicevati le, če je verjetno, da bi uporaba navedene določbe o varstvu podatkov posegala v zadevni posamezni interes. Uporaba izjeme mora torej biti vedno upravičena s sklicevanjem na zadevno poseganje, do katerega bi v posameznem primeru verjetno prišlo. Na izjeme na podlagi vrste se je mogoče sklicevati le glede specifičnih, ozko opredeljenih vrst informacij, glede katerih je uporaba izjeme mogoča. Te so glede na namen in učinek podobne več izjemam od UK GDPR (na podlagi dodatka 2 k zakonu o varstvu podatkov iz leta 2018), ki pa izražajo tiste iz člena 23 Splošne uredbe o varstvu podatkov.

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

(138) Informacijski pooblaščenec nadzoruje obdelavo osebnih podatkov, ki jo izvajajo obveščevalne službe v skladu z delom 4 zakona o varstvu podatkov iz leta DPA 2018 ([237]).

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

(140) Kot je določeno v delu 3 zakona o varstvu podatkov iz leta 2018, je informacijski pooblaščenec pristojen za obveščanje upravljavca o domnevnih kršitvah, izdajanje opozoril, da bo obdelava verjetno kršila pravila, in izrekanje opominov ob potrditvi kršitve. Izdaja lahko tudi obvestila o izvršitvi in o plačilnem nalogu za kršitve določenih določb akta ([238]). Informacijski pooblaščenec pa v nasprotju z drugimi deli zakona o varstvu podatkov iz leta 2018 ne more izdati obvestila o preverjanju organu za nacionalno varnost ([239]).

(141) Poleg tega je v členu 110 zakona o varstvu podatkov iz leta 2018 določena izjema od uporabe določenih pooblastil informacijskega pooblaščenca, ko je to potrebno zaradi zaščite nacionalne varnosti. To vključuje pristojnost informacijskega pooblaščenca, da lahko na podlagi zakona o varstvu podatkov izdaja obvestila (vseh vrst) (obvestilo o predložitvi informacij, obvestilo o preverjanju, obvestilo o izvršitvi in obvestilo o plačilnem nalogu), pristojnost za opravljanje inšpekcijskega nadzora v skladu z mednarodnimi obveznostmi, pristojnost za vstop in inšpekcijski

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

([236]) V skladu z obrazložitvenim okvirom Združenega kraljestva so izjeme na podlagi vrste: (i) informacije o podelitvi državnih častnih odlikovanj; (ii) varovanje zaupnosti sporazumevanja med odvetnikom in stranko; (iii) zaupni sklici na zaposlitev, usposabljanje ali izobraževanje ter (iv) izpitne pole in ocene. Izjeme na podlagi poseganja se nanašajo na te zadeve: (i) preprečevanje ali odkrivanje kaznivih dejanj; prijetje in pregon storilcev; (ii) parlamentarni privilegij; (iii) sodni postopki; (iv) bojna učinkovitost oboroženih sil države; (v) gospodarska blaginja Združenega kraljestva; (vi) pogajanja s posameznikom, na katerega se nanašajo osebni podatki; (vii) znanstvene ali zgodovinske raziskave ali statistični nameni; (viii) arhiviranje v javnem interesu. Obrazložitveni okvir Združenega kraljestva za razpravo o ustreznosti, oddelek H: Nacionalna varnost, stran 13, glej opombo 222.

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

([238]) Upravljavcu ali obdelovalcu se lahko v skladu s povezanim branjem člena 149(2) in člena 155 zakona o varstvu podatkov iz leta 2018 izdajo opozorila o izvršitvi in o plačilnem nalogu za kršitve poglavja 2 dela 4 zakona o varstvu podatkov iz leta 2018 (načela obdelave), določbe dela 4 zakona o varstvu podatkov iz leta 2018 o prenosu pravic posameznika, na katerega se nanašajo osebni podatki, zahteve o obveščanju informacijskega pooblaščenca o kršitvi varnosti osebnih podatkov v skladu s členom 108 zakona o varstvu podatkov iz leta 2018 ter načel prenosa osebnih podatkov v tretje države, države, ki niso podpisnice konvencije, in mednarodne organizacije iz člena 109 zakona o varstvu podatkov iz leta 2018. (Za več podrobnosti o opozorilih o izvršitvi in o plačilnem nalogu glej uvodni izjavi (102) in (103)).

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

pregled in pravila o kaznivih dejanjih ([240]). Te izjeme se bodo, kot je pojasnjeno v uvodni izjavi (136), uporabljale le, če so potrebne in sorazmerne in za vsak primer posebej. Uporaba teh izjem bi morala biti predmet sodne presoje ([241]).

(142) Urad informacijskega pooblaščenca in obveščevalne službe Združenega kraljestva so podpisale memorandum o soglasju ([242]), ki vzpostavlja okvir za sodelovanje o številnih vprašanjih, vključno z obvestili o kršitvi varnosti podatkov in obravnavanjem pritožb posameznikov, na katere se nanašajo osebni podatki. V njem je določeno zlasti to, da urad informacijskega pooblaščenca ob prejetju pritožbe oceni, ali je bil sklic na izjemo zaradi nacionalne varnosti ustrezen. Odgovor na poizvedbe, ki jih opravi urad informacijskega pooblaščenca pri proučitvi pritožb posameznikov, je treba na podlagi zadevnih smernic vlade Združenega kraljestva za potrdila o omejitvah iz razlogov nacionalne varnosti v skladu z zakonom o varstvu podatkov poslati v 20 delovnih dneh, če gre za zaupne informacije, pa je treba pri tem uporabiti varne komunikacijske kanale. Urad informacijskega pooblaščenca je od aprila 2018 do danes prejel 21 pritožb posameznikov glede obveščevalnih služb. Vsako pritožbo je proučil in rezultat sporočil posamezniku, na katerega se nanašajo osebni podatki ([243]).

(143) Odbor za obveščevalno in varnostno dejavnost (Intelligence and Security Committee) izvaja parlamentarni nadzor nad obdelavo podatkov, ki jo izvajajo obveščevalne službe. Njegova zakonska podlaga je zakon iz leta 2013 o pravosodju in varnosti (Justice and Security Act 2013) ([244]). Z zakonom je bil ustanovljen odbor parlamenta Združenega kraljestva za obveščevalno in varnostno dejavnost. Odbor za obveščevalno in varnostno dejavnost sestavljajo poslanci zgornjega ali spodnjega doma parlamenta Združenega kraljestva, ki jih imenuje predsednik vlade po posvetovanju z vodjem opozicije ([245]). Pripraviti mora letno poročilo za parlament o izvajanju svojih nalog in druga poročila, ki se mu zdijo ustrezna ([246]).

(144) Odboru za obveščevalno in varnostno dejavnost so bila od leta 2013 podeljena večja pooblastila, vključno z nadzorom nad operativnimi dejavnostmi varnostnih služb. V skladu s členom 2 zakona o pravosodju in varnosti iz leta 2013 je naloga tega odbora nadzor nad odhodki, upravljanjem, politiko in operacijami nacionalnih varnostnih agencij. V zakonu o pravosodju in varnosti iz leta 2013 je določeno, da lahko ta odbor izvaja preiskave

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

([241]) Glej na primer sodbo v zadevi Baker proti Secretary of State for the Home Department (glej opombo 221).

([242]) Memorandum o soglasju med uradom informacijskega pooblaščenca in obveščevalno skupnostjo Združenega kraljestva, glej opombo 231.

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

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

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

([246]) Poročila in izjave odbora so na voljo na povezavi: http://isc.independent.gov.uk/committee-reports. Odbor za obveščevalno in varnostno dejavnost je leta 2015 izdal poročilo z naslovom Privacy and Security: A modern and transparent legal framework (Zasebnost in varnost: sodoben in pregleden pravni okvir; glej: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), v katerem je proučil pravni okvir za tehnike nadzora, ki jih uporabljajo obveščevalne službe, ter izdal vrsto priporočil, ki so bila nato proučena in vključena v osnutek predloga zakona o preiskovalnih pooblastilih, preoblikovanega v zakon, tj. zakon o preiskovalnih pooblastilih iz leta 2016 (Investigatory Powers Act 2016). Odgovori vlade na navedeno poročilo so na voljo na povezavi: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

o operativnih zadevah, kadar se ne nanašajo na potekajoče operacije ([247]). V memorandumu o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost ([248]) so podrobno določeni elementi, ki se upoštevajo pri presoji, ali dejavnost ni del katere koli potekajoče operacije ([249]). Predsednik vlade lahko navedenemu odboru naroči tudi preiskavo tekočih operacij, poleg tega lahko odbor prouči informacije, ki jih agencije predložijo prostovoljno.

(145) Odbor za obveščevalno in varnostno dejavnost lahko v skladu z dodatkom 1 k zakonu o pravosodju in varnosti iz leta 2013 prosi vodjo katere koli od treh obveščevalnih služb, da razkrije informacije. Služba mora take informacije dati na voljo, razen če pristojni minister vloži veto ([250]). Organi Združenega kraljestva so pojasnili, da se v praksi redko zgodi, da temu odboru kakšne informacije ne bi bile razkrite ([251]).

(146) Glede pravnih sredstev lahko posameznik, na katerega se nanašajo osebni podatki, v skladu s členom 165(2) zakona o varstvu podatkov iz leta 2018 vloži pritožbo pri odboru za obveščevalno in varnostno dejavnost, če meni, da v zvezi z osebnimi podatki, ki se nanašajo nanj, obstaja kršitev iz dela 4 zakona o varstvu podatkov iz leta 2018, vključno z zlorabo odstopanj in omejitev na področju nacionalne varnosti.

(147) Poleg tega so posamezniki v skladu z delom 4 zakona o varstvu podatkov iz leta 2018 upravičeni, da pri sodišču High Court (ali sodišču Court of Session na Škotskem) vložijo predlog za izdajo odločbe, ki od upravljavca zahteva, da upošteva pravice do dostopa do podatkov ([252]), do ugovora obdelavi ([253]) in do popravka ali izbrisa.

(148) Posamezniki so prav tako upravičeni zahtevati odškodnino za škodo, ki nastane zaradi kršitve zahteve iz dela 4 zakona o varstvu podatkov iz leta 2018 s strani upravljavca ali obdelovalca ([254]). Škoda vključuje finančno in nefinančno izgubo, kot je na primer stiska ([255]).

(149) Nazadnje, posameznik lahko zaradi ravnanja s strani ali v imenu obveščevalnih agencij Združenega kraljestva ([256]) vloži pritožbo pri sodišču, ki obravnava preiskovalna pooblastila (Investigatory Powers Tribunal). To sodišče je ustanovljeno z zakonom o urejanju preiskovalnih pooblastil iz leta 2000 za Anglijo, Wales in Severno Irsko in zakonom o urejanju preiskovalnih pooblastil (Škotska) iz leta 2000 za Škotsko ter je neodvisno od izvršilne veje oblasti ([257]). Člane tega sodišča v skladu s členom 65 zakona o urejanju preiskovalnih pooblastil iz leta 2000 imenuje kraljica za obdobje petih let.

(150) Člana tega sodišča lahko s funkcije razreši kraljica, na podlagi nagovora ([258]) obeh domov parlamenta ([259]).

(151) Da lahko posameznik vloži tožbo pri sodišču, ki obravnava preiskovalna pooblastila („procesno upravičenje“), mora biti v skladu s členom 65 zakona o urejanju preiskovalnih pooblastil iz leta 2000 prepričan o (i) obstoju ravnanja, ki ga je obveščevalna služba storila v zvezi z njim, njegovim premoženjem, komunikacijami, ki jih je poslal ali so mu bile poslane ali namenjene, ali uporabo poštnih storitev, telekomunikacijskih storitev ali telekomunikacijskega sistema ([260]), ter

([247]) Člen 2 zakona o pravosodju in varnosti iz leta 2013.
([248]) Memorandum o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost je na voljo na povezavi: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Memorandum o soglasju med predsednikom vlade in odborom za obveščevalno in varnostno dejavnost, odstavek 14, glej opombo 248.
([250]) Pristojni minister lahko vloži veto na razkritje informacij le iz dveh razlogov: informacije so občutljive in odboru za obveščevalno in varnostno dejavnost ne smejo biti razkrite zaradi nacionalne varnosti ali je narava informacij taka, da bi se pristojnemu ministru, če bi jih moral predstaviti pred resornim odborom spodnjega doma parlamenta Združenega kraljestva (zaradi razlogov, ki niso omejeni na nacionalno varnost), zdelo ustrezno, da tega ne stori (odstavek 4(2) dodatka 1 k zakonu o pravosodju in varnosti iz leta 2013).
([251]) Obrazložitveni okvir Združenega kraljestva, oddelek H: Nacionalna varnost, str. 43.
([252]) Člen 94(11) zakona o varstvu podatkov iz leta 2018.
([253]) Člen 99(4) zakona o varstvu podatkov iz leta 2018.
([254]) Člen 169 zakona o varstvu podatkov iz leta 2018 dopušča zahtevke „osebe, ki utrpi škodo zaradi kršitve zahteve iz zakonodaje o varstvu podatkov“.
([255]) Člen 169(5) zakona o varstvu podatkov iz leta 2018.
([256]) Glej člen 65(2)(b) zakona o urejanju preiskovalnih pooblastil.
([257]) V skladu z dodatkom 3 k zakonu o urejanju preiskovalnih pooblastil iz leta 2000 morajo imeti člani določene izkušnje na pravosodnem področju in so lahko ponovno imenovani.
([258]) Za pojem „nagovor (Address)“ glej opombo 183.
([259]) Odstavek 1(5) dodatka 3 k zakonu o urejanju preiskovalnih pooblastil iz leta 2000.
([260]) Člen 65(4) zakona o urejanju preiskovalnih pooblastil iz leta 2000.

(ii) o tem, da je bilo ravnanje storjeno v „spornih okoliščinah“ ([261]) ali „storjeno s strani ali v imenu obveščevalnih služb“ ([262]). Ker se je zlasti ta standard prepričanja razlagal precej široko ([263]), se za predložitev zadeve navedenemu sodišču zahteva razmeroma nizek prag procesnega upravičenja.

(152) Sodišče, ki obravnava preiskovalna pooblastila, mora pri obravnavanju vložene pritožbe proučiti, ali so osebe, zoper katere je vložena pritožba, ukrepale v razmerju do pritožnika ter kako je ravnal organ, ki je domnevno vpleten v kršitve, in ali je bilo domnevno ravnanje storjeno ([264]). Kadar sodišče, ki obravnava preiskovalna pooblastila, vodi postopek, mora pri sprejemanju odločitve v tem postopku uporabiti ista načela, kot bi jih uporabilo sodišče na podlagi zahteve za sodno presojo ([265]).

(153) Sodišče, ki obravnava preiskovalna pooblastila, mora pritožnika obvestiti, ali je bila odločitev v njegovo korist ali ne ([266]). Sodišče, ki obravnava preiskovalna pooblastila, lahko v skladu s členom 67(6) in (7) zakona o urejanju preiskovalnih pooblastil iz leta 2000 izdaja začasne odredbe in priznava odškodnine ali izdaja druge odredbe, ki se mu zdijo primerne ([267]). V skladu s členom 67A zakona o urejanju preiskovalnih pooblastil iz leta 2000 se je mogoče pritožiti zoper odločitev sodišča, ki obravnava preiskovalna pooblastila, in sicer na podlagi dovoljenja tega sodišča ali ustreznega pritožbenega sodišča.

(154) Posamezniki lahko pri sodišču, ki obravnava preiskovalna pooblastila, zlasti vložijo tožbo – in uveljavljajo pravna sredstva – kadar menijo, da je javni organ ravnal (ali predlaga ravnanje) na način, ki ni skladen s pravicami iz EKČP, vključno s pravico do zasebnosti in do varstva podatkov, kar je posledično nezakonito na podlagi člena 6(1) zakona o človekovih pravicah iz leta 1998. Sodišču, ki obravnava preiskovalna pooblastila, je bila podeljena izključna pristojnost za vse pritožbene zahtevke v zvezi z obveščevalnimi agencijami, ki se nanašajo na zakon o človekovih pravicah. Kot je navedlo sodišče High Court, to pomeni, da „lahko o tem, ali je bil na podlagi dejstev v posamezni zadevi kršen zakon o človekovih pravicah, načeloma odloča neodvisno sodišče, ki lahko ima dostop do vsega ustreznega gradiva, tudi tajnega. […] Pri tem upoštevamo tudi, da se je zoper odločitev sodišča, ki obravnava preiskovalna pooblastila, zdaj mogoče pritožiti pri ustreznem pritožbenem sodišču (v Angliji in Walesu je to sodišče Court of Appeal), sodišče Supreme Court pa je pred kratkim ugotovilo, da je načeloma mogoče zahtevati sodno presojo zoper odločitve sodišča, ki obravnava preiskovalna pooblastila: glej sodbo v zadevi R (Privacy International) proti Investigatory Powers Tribunal [2019] UKSC 22, [2019] 2 WLR 1219“ ([268]). Če sodišče, ki obravnava preiskovalna pooblastila, ugotovi, da je katero koli dejanje javnega organa nezakonito, lahko odobri odškodnino ali pravno sredstvo ali izda odredbo, kot meni, da je pravično in ustrezno ter za katero je pristojno ([269]).

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

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

([263]) Glej sodbo v zadevi Human Rights Watch proti Secretary of State [2016] UKIPTrib15_165-CH. V tej zadevi je sodišče, ki obravnava preiskovalna pooblastila, s sklicevanjem na sodno prakso Evropskega sodišča za človekove pravice ugotovilo, da se prepričanje, da je bilo s strani ali v imenu katere koli obveščevalne službe storjeno katero koli ravnanje, ki spada v podčlen 68(5) zakona o urejanju preiskovalnih pooblastil iz leta 2000, ustrezno preskusi z obstojem podlage za tako prepričanje, kar pomeni tudi, da lahko posameznik trdi, da je žrtev kršitve, ki jo povzroči že sam obstoj tajnih ukrepov ali zakonodaje, ki dovoljuje tajne ukrepe, le, če lahko dokaže, da je zaradi svojega osebnega položaja v morebitni nevarnosti za izpostavljenost takim ukrepom (glej sodbo v zadevi Human Rights Watch proti Secretary of State, točka 41).

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

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

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

([267]) To lahko zajema odredbo, s katero se zahteva uničenje evidenc informacij, ki jih imajo javni organi glede katere koli osebe.

([268]) Sodba High Court of Justice v zadevi Liberty, [2019] EWHC 2057 (Admin), točka 170.

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

(155) Ko posameznik izčrpa nacionalna pravna sredstva, se lahko obrne na Evropsko sodišče za človekove pravice zaradi kršitev pravic, zagotovljenih na podlagi EKČP, vključno s pravico do zasebnosti in do varstva podatkov.

(156) Iz navedenega izhaja, da izmenjava podatkov, prenesenih na podlagi tega sklepa, med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj Združenega kraljestva in drugimi javnimi organi, vključno z obveščevalnimi agencijami, poteka v okviru omejitev in pogojev, ki zagotavljajo, da bodo taki nadaljnji prenosi potrebni in sorazmerni ter da se pri njih upoštevajo posebni zaščitni ukrepi za varstvo podatkov na podlagi zakona o varstvu podatkov iz leta 2018. Poleg tega obdelavo podatkov s strani zadevnih javnih organov nadzorujejo neodvisni javni organi, zadevni posamezniki pa imajo dostop do učinkovitih pravnih sredstev.

3. SKLEPNA UGOTOVITEV

(157) Komisija meni, da del 3 zakona o varstvu podatkov iz leta 2018 zagotavlja, da je raven varstva osebnih podatkov, ki jih za namene preprečevanja, odkrivanja in preiskovanja kaznivih dejanj pristojni organi v Uniji prenašajo pristojnim organom Združenega kraljestva, v osnovi enakovredna ravni, zagotovljeni z Direktivo (EU) 2016/680.

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

(159) Komisija glede na razpoložljive informacije o pravnem redu Združenega kraljestva nazadnje meni, da so vsi posegi v temeljne pravice posameznikov, katerih osebne podatke iz Evropske unije v Združeno kraljestvo prenašajo javni organi Združenega kraljestva v imenu javnega interesa, tudi v okviru izmenjave osebnih podatkov med organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj in drugimi javnimi organi, kot so organi nacionalne varnosti, omejeni na tisto, kar je nujno potrebno za doseganje zadevnega zakonitega cilja, ter da obstaja učinkovita pravna zaščita zoper take posege.

(160) Zato bi bilo treba odločiti, da Združeno kraljestvo zagotavlja ustrezno raven varstva v smislu člena 36(2) Direktive (EU) 2016/680, kot se razlaga ob upoštevanju Listine EU o temeljnih pravicah.

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

4. UČINKI TEGA SKLEPA IN UKREPI ORGANOV ZA VARSTVO PODATKOV

(162) Države članice in njihovi organi morajo sprejeti ukrepe, potrebne za zagotavljanje skladnosti z akti institucij Unije, saj se domneva, da so ti zakoniti in imajo pravne učinke, dokler se njihova veljavnost ne izteče, dokler niso preklicani, razglašeni za nične v okviru ničnostne tožbe ali razglašeni za neveljavne v okviru postopka predhodnega odločanja ali ugovora nezakonitosti.

(163) Zato je sklep Evropske komisije o ustreznosti, sprejet na podlagi člena 36(3) Direktive (EU) 2016/680, zavezujoč za vse organe držav članic, na katere je naslovljen, vključno z njihovimi neodvisnimi nadzornimi organi. Natančneje, prenosi od upravljavca ali obdelovalca v Uniji upravljavcu ali obdelovalcu v Združenem kraljestvu lahko v obdobju uporabe tega sklepa potekajo, ne da bi bilo treba pridobiti nadaljnje dovoljenje.

(164) Hkrati je treba opozoriti, da v skladu s členom 47(5) Direktive (EU) 2016/680 in glede na pojasnila Sodišča v sodbi v zadevi Schrems velja, da če ima nacionalni organ za varstvo podatkov, med drugim kadar je prejel pritožbo, pomisleke o skladnosti sklepa Komisije o ustreznosti s temeljnimi pravicami posameznika do zasebnosti in varstva podatkov, mu mora nacionalno pravo zagotavljati pravno sredstvo za predložitev teh očitkov nacionalnemu sodišču, od katerega se lahko zahteva, da Sodišču predloži predlog za sprejetje predhodne odločbe ([270]).

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

5. **SPREMLJANJE, ZAČASNO ZADRŽANJE IZVAJANJA, RAZVELJAVITEV ALI SPREMEMBA TEGA SKLEPA**

(165) Komisija v skladu s členom 36(4) Direktive (EU) 2016/680 redno spremlja razvoj dogodkov v Združenem kraljestvu po sprejetju tega sklepa, da lahko presodi, ali Združeno kraljestvo še vedno zagotavlja v osnovi enakovredno raven varstva. Tako spremljanje je v tem primeru še posebej pomembno, saj bo Združeno kraljestvo upravljalo, uporabljalo in izvajalo novo ureditev varstva podatkov, za katero se ne uporablja več pravo Unije in se bo morda spremenila. Posebna pozornost v okviru tega spremljanja bo namenjena temu, kako Združeno kraljestvo v praksi uporablja svoja pravila za prenose osebnih podatkov v tretje države, vključno s sklenitvijo mednarodnih sporazumov, ter učinek, ki ga lahko to ima na raven varstva, ki se zagotavlja za podatke, ki se prenesejo na podlagi tega sklepa, pa tudi na učinkovitost uveljavljanja pravic posameznika na področjih, zajetih s tem sklepom. Komisija bo pri spremljanju med drugim upoštevala razvoj sodne prakse ter nadzor, ki ga izvajajo urad informacijskega pooblaščenca in drugi neodvisni organi.

(166) Za lajšanje tega spremljanja bi morali organi Združenega kraljestva Komisijo brez odlašanja in redno obveščati o vsaki bistveni spremembi pravnega reda Združenega kraljestva, ki vpliva na pravni okvir, ki je predmet tega sklepa, ter o vsakem razvoju praks v zvezi z obdelavo osebnih podatkov, ocenjenih v tem sklepu, zlasti glede elementov, omenjenih v uvodni izjavi (165).

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

(168) Če se na podlagi razpoložljivih informacij, zlasti tistih, ki izhajajo iz spremljanja tega sklepa ali ki jih zagotovijo organi Združenega kraljestva ali držav članic, ugotovi, da raven varstva, ki ga zagotavlja Združeno kraljestvo, morda ni več ustrezna, bi morala Komisija o tem nemudoma obvestiti pristojne organe Združenega kraljestva in zahtevati, da v določenem roku, ki ne sme presegati treh mesecev, sprejmejo ustrezne ukrepe. To obdobje se lahko po potrebi podaljša za določeno obdobje, pri čemer se upoštevata narava zadevnega vprašanja in/ali ukrepov, ki jih je treba sprejeti.

(169) Če pristojni organi Združenega kraljestva ob preteku tega določenega roka ne sprejmejo navedenih ukrepov ali drugače zadovoljivo dokažejo, da ta sklep še naprej temelji na ustrezni ravni varstva, bo Komisija začela postopek iz člena 58(2) Direktive (EU) 2016/680 za začasno zadržanje izvajanja ali za razveljavitev dela ali celotnega tega sklepa.

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

(171) Komisija bo v nujnih in ustrezno utemeljenih primerih uporabila možnost, da v skladu s postopkom iz člena 58(3) Direktive (EU) 2016/680 sprejme izvedbene akte, ki se začnejo uporabljati takoj in s katerimi se začasno zadrži izvajanje tega sklepa oziroma se sklep razveljavi ali spremeni.

6. **TRAJANJE IN PODALJŠANJE VELJAVNOSTI TEGA SKLEPA**

(172) Upoštevati je treba, da bo Združeno kraljestvo ob koncu prehodnega obdobja, določenega v sporazumu o izstopu, in takoj po prenehanju uporabe začasne določbe iz člena 782 sporazuma o trgovini in sodelovanju med EU in Združenim kraljestvom upravljalo, uporabljalo in izvajalo novo ureditev varstva podatkov, ne pa več ureditve, ki je veljala, ko jo je zavezovalo pravo Evropske unije. To lahko vključuje zlasti dopolnitve ali spremembe okvira varstva podatkov, ki se ocenjuje v tem sklepu, ter drug ustrezen razvoj.

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

(174) Kadar zlasti iz informacij, ki izhajajo iz spremljanja tega sklepa, izhaja, da so ugotovitve, ki se nanašajo na ustreznost ravni varstva, ki se zagotavlja v Združenem kraljestvu, še vedno dejansko in pravno upravičene, bi morala Komisija najpozneje šest mesecev pred prenehanjem uporabe tega sklepa začeti postopek za spremembo tega sklepa, tako da se veljavnost načeloma podaljša za dodatna štiri leta. Vsak tak izvedbeni akt, ki spreminja ta sklep, mora biti sprejet v skladu s postopkom iz člena 58(2) Direktive (EU) 2016/680.

7. **SKLEPNE UGOTOVITVE**

(175) Evropski odbor za varstvo podatkov je objavil svoje mnenje ([271]), ki je bilo upoštevano pri pripravi tega sklepa.

(176) Ukrepi iz tega sklepa so v skladu z mnenjem odbora, ustanovljenega na podlagi člena 58 Direktive (EU) 2016/680.

(177) V skladu s členom 6a Protokola št. 21 o stališču Združenega kraljestva in Irske v zvezi z območjem svobode, varnosti in pravice, ki je priložen PEU in PDEU, pravila iz Direktive (EU) 2016/680 in zato tega izvedbenega sklepa, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar opravljajo dejavnosti s področja uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU, za Irsko niso zavezujoča, če je ne zavezujejo pravila, ki urejajo oblike pravosodnega sodelovanja v kazenskih zadevah ali policijskega sodelovanja, v okviru katerih je treba upoštevati določbe, sprejete na podlagi člena 16 PDEU. Poleg tega Irska na podlagi Izvedbenega sklepa Sveta (EU) 2020/1745 ([272]) od 1. januarja 2021 začasno izvaja in uporablja Direktivo (EU) 2016/680. Irsko zato zavezuje ta izvedbeni sklep pod enakimi pogoji, kot veljajo za uporabo Direktive (EU) 2016/680 na Irskem, kakor so bili določeni v Izvedbenem sklepu Sveta (EU) 2020/1745 glede schengenskega pravnega reda, v katerem sodeluje.

(178) V skladu s členoma 2 in 2a Protokola št. 22 o stališču Danske, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, pravila iz Direktive (EU) 2016/680 in zato tega izvedbenega sklepa, ki se nanašajo na obdelavo osebnih podatkov s strani držav članic, kadar opravljajo dejavnosti s področja uporabe poglavja 4 ali 5 naslova V tretjega dela PDEU, za Dansko niso zavezujoča in se v njej ne uporabljajo. Ker Direktiva (EU) 2016/680 nadgrajuje schengenski pravni red, je Danska v skladu s členom 4 navedenega protokola 26. oktobra 2016 priglasila svojo odločitev o izvajanju Direktive (EU) 2016/680. Danska je tako v skladu z mednarodnim pravom zavezana izvajati ta izvedbeni sklep.

(179) Kar zadeva Islandijo in Norveško, ta izvedbeni sklep pomeni razvoj določb schengenskega pravnega reda v smislu Sporazuma, sklenjenega med Svetom Evropske unije in Republiko Islandijo ter Kraljevino Norveško v zvezi s pridružitvijo teh dveh držav k izvajanju, uporabi in razvoju schengenskega pravnega reda ([273]).

(180) Kar zadeva Švico, ta izvedbeni sklep pomeni razvoj določb schengenskega pravnega reda v smislu Sporazuma med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda ([274]).

(181) Kar zadeva Lihtenštajn, ta izvedbeni sklep pomeni razvoj določb schengenskega pravnega reda v smislu Protokola med Evropsko unijo, Evropsko skupnostjo, Švicarsko konfederacijo in Kneževino Lihtenštajn o pristopu Kneževine Lihtenštajn k Sporazumu med Evropsko unijo, Evropsko skupnostjo in Švicarsko konfederacijo o pridružitvi Švicarske konfederacije k izvajanju, uporabi in razvoju schengenskega pravnega reda ([275]) –

([271]) Mnenje št. 15/2021 o osnutku izvedbenega sklepa Evropske komisije v skladu z Direktivo (EU) 2016/680 o ustreznem varstvu osebnih podatkov v Združenem kraljestvu, na voljo na naslednji povezavi: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Izvedbeni sklep Sveta (EU) 2020/1745 z dne 18. novembra 2020 o začetku izvajanja določb schengenskega pravnega reda o varstvu podatkov in začetku začasnega izvajanja nekaterih določb schengenskega pravnega reda na Irskem (UL L 393, 23.11.2020, str. 3).

([273]) UL L 176, 10.7.1999, str. 36.

([274]) UL L 53, 27.2.2008, str. 52.

([275]) UL L 160, 18.6.2011, str. 21.

SPREJELA NASLEDNJI SKLEP:

Člen 1

Združeno kraljestvo za namene člena 36 Direktive (EU) 2016/680 zagotavlja ustrezno raven varstva osebnih podatkov, ki se iz Evropske unije prenesejo javnim organom v Združenem kraljestvu, pristojnim za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij.

Člen 2

Kadar pristojni nadzorni organi države članice zaradi varstva posameznikov pri obdelavi njihovih osebnih podatkov izvajajo svoja pooblastila na podlagi člena 47 Direktive (EU) 2016/680 v zvezi s prenosi podatkov javnim organom v Združenem kraljestvu na področju uporabe iz člena 1, zadevna država članica o tem brez odlašanja obvesti Komisijo.

Člen 3

1. Komisija stalno spremlja uporabo pravnega okvira, na katerem temelji ta sklep, vključno s pogoji, pod katerimi se izvajajo nadaljnji prenosi in uveljavljajo pravice posameznika, da se oceni, ali Združeno kraljestvo še naprej zagotavlja ustrezno raven varstva v smislu člena 1.

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

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

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

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

Člen 4

Ta sklep preneha veljati 27. junija 2025, razen če je podaljšan v skladu s postopkom iz člena 58(2) Direktive (EU) 2016/680.

Člen 5

Ta sklep je naslovljen na države članice.

V Bruslju, 28. junija 2021

Za Komisijo
Didier REYNDERS
član Komisije