PROVEDBENA ODLUKA KOMISIJE (EU) 2021/1773

od 28. lipnja 2021.

u skladu s Direktivom (EU) 2016/680 Europskog parlamenta i Vijeća o primjerenoj zaštiti osobnih podataka u Ujedinjenoj Kraljevini

(priopćeno pod brojem dokumenta C(2021) 4801)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije,

uzimajući u obzir Direktivu (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP ([1]), a posebno njezin članak 36. stavak 3.,

budući da:

1. **UVOD**

(1) U Direktivi (EU) 2016/680 utvrđuju se pravila za prijenos osobnih podataka od strane nadležnih tijela iz Unije trećim zemljama i međunarodnim organizacijama u mjeri u kojoj su takvi prijenosi obuhvaćeni područjem primjene te direktive. Pravila o međunarodnim prijenosima podataka od strane nadležnih tijela utvrđena su u poglavlju V. Direktive (EU) 2016/680, točnije u člancima od 35. do 40. Iako je protok osobnih podataka u zemlje izvan Europske unije i iz njih važan za učinkovitu suradnju u području kaznenog progona, mora se jamčiti da se takvim prijenosima ne narušava razina zaštite osobnih podataka u Europskoj uniji ([2]).

(2) U skladu s člankom 36. stavkom 3. Direktive (EU) 2016/680 Komisija može putem provedbenog akta odlučiti da treća zemlja, područje, ili jedan ili više određenih sektora unutar treće zemlje, ili međunarodna organizacija osigurava primjerenu razinu zaštite. Pod tim uvjetom prijenosi osobnih podataka trećoj zemlji mogu se obavljati bez potrebe za dobivanjem bilo kakvog daljnjeg odobrenja (osim ako druga država članica iz koje su podaci dobiveni mora dati svoje odobrenje za prijenos), kako je predviđeno u članku 35. stavku 1. i uvodnoj izjavi 66. Direktive (EU) 2016/680.

(3) Kako je navedeno u članku 36. stavku 2. Direktive (EU) 2016/680, donošenje odluke o primjerenosti mora se temeljiti na sveobuhvatnoj analizi pravnog poretka treće zemlje. Komisija u svojoj procjeni mora utvrditi jamči li predmetna treća zemlja razinu zaštite koja je „u osnovi istovjetna" onoj koja je osigurana u Europskoj uniji (uvodna izjava 67. Direktive (EU) 2016/680). Je li zaštita „u osnovi istovjetna" procjenjuje se prema standardu utvrđenom u zakonodavstvu EU-a, ponajprije Direktivi (EU) 2016/680, te u sudskoj praksi Suda Europske unije ([3]). U tom je pogledu važan i referentni dokument o primjerenosti koji je izdao Europski odbor za zaštitu podataka ([4]).

(4) Kako je pojasnio Sud Europske unije, to ne zahtijeva utvrđivanje potpuno istovjetne razine zaštite ([5]). Naime, pravna sredstva kojima se predmetna treća zemlja koristi za zaštitu osobnih podataka mogu se razlikovati od onih koja se primjenjuju u Europskoj uniji, pod uvjetom da se u praksi pokažu djelotvornima za osiguravanje primjerene razine zaštite ([6]). Prema tome, standard primjerenosti ne podrazumijeva doslovno ponavljanje pravila Unije. Umjesto toga ispituje se pruža li predmetni strani sustav kao cjelina potrebnu razinu zaštite podataka ([7]) sadržajem prava na privatnost i njihovom djelotvornom provedbom, nadzorom i ostvarivanjem.

([1]) SL L 119, 4.5.2016., str. 89.
([2]) Vidjeti uvodnu izjavu 64. Direktive (EU) 2016/680.
([3]) Vidjeti, kao najnoviji, predmet C-311/18, *Facebook Ireland i Schrems* (dalje u tekstu: „*Schrems II*"), ECLI:EU:C:2020:559.
([4]) Vidjeti Preporuku br. 1/2021 o referentnom dokumentu o primjerenosti na temelju Direktive o zaštiti podataka u svrhe kaznenog progona, koja je donesena u veljači 2021. i dostupna na: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_en.
([5]) Predmet C-362/14, *Maximilian Schrems protiv Data Protection Commissioner* (dalje u tekstu: „*Schrems*"), ECLI:EU:C:2015:650, točka 73.
([6]) Presuda u predmetu *Schrems*, točka 74.
([7]) Vidjeti Komunikaciju Komisije Europskom parlamentu i Vijeću „Razmjena i zaštita osobnih podataka u globaliziranom svijetu", COM(2017) 7 od 10.1.2017., odjeljak 3.1., str. 6.–7., koja je dostupna na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:52017DC0007&from=HR.

(5) Komisija je pažljivo analizirala relevantno pravo i praksu Ujedinjene Kraljevine. Na temelju svojih nalaza, navedenih u nastavku, Komisija zaključuje da Ujedinjena Kraljevina osigurava primjerenu razinu zaštite osobnih podataka koje nadležna tijela iz Unije obuhvaćena područjem primjene Direktive (EU) 2016/680 prenose nadležnim tijelima u Ujedinjenoj Kraljevini koja su obuhvaćena područjem primjene dijela 3. Zakona o zaštiti podataka iz 2018. (DPA iz 2018.) ([8]).

(6) Ova Odluka znači da se takvi prijenosi mogu obavljati bez potrebe za dobivanjem bilo kakvog daljnjeg odobrenja u razdoblju od četiri godine, što podliježe mogućem obnavljanju, i ne dovodeći u pitanje uvjete iz članka 35. Direktive (EU) 2016/680.

2. PRAVILA KOJA SE PRIMJENJUJU NA OBRADU OSOBNIH PODATAKA OD STRANE NADLEŽNIH TIJELA U SVRHE KAZNENOG PROGONA

2.1. Ustavni okvir

(7) Ujedinjena Kraljevina je parlamentarna demokracija. Ima suvereni parlament, koji je nadređen svim ostalim vladinim institucijama, izvršnu vlast koja proizlazi iz parlamenta i odgovorna je parlamentu te neovisno sudstvo. Ovlasti izvršne vlasti proizlaze iz njezine sposobnosti da osigura povjerenje izabranog Zastupničkog doma, a odgovorna je obama domovima Parlamenta (Zastupnički dom i Dom lordova), čija je zadaća preispitivanje rada vlade te raspravljanje o zakonskim prijedlozima i donošenje zakona. Parlament Ujedinjene Kraljevine prenio je određene nadležnosti Škotskom parlamentu (*Scottish Parliament*), Velškom parlamentu (*Senedd Cymru*) i Skupštini Sjeverne Irske (*Northern Ireland Assembly*), koje im omogućuju da uređuju određena domaća pitanja u Škotskoj, Walesu i Sjevernoj Irskoj. Iako je zaštita podataka pitanje za čije je rješavanje nadležan Parlament Ujedinjene Kraljevine, tj. isti se propisi primjenjuju u cijeloj zemlji, druga područja politike relevantna za ovu Odluku obuhvaćena su prenesenim nadležnostima. Na primjer, nadležnosti za sustave kaznenog pravosuđa, uključujući policijsku djelatnost (aktivnosti koje obavljaju policijske snage), u Škotskoj i Sjevernoj Irskoj prenesene su Škotskom parlamentu odnosno Skupštini Sjeverne Irske ([9]).

(8) Iako Ujedinjena Kraljevina nema kodificirani ustav u smislu utvrđenog konstitutivnog dokumenta, njezina ustavna načela nastala su s vremenom i proizlaze iz sudske prakse, a osobito iz običaja. Priznat je ustavnopravni značaj određenih akata, kao što su Velika povelja sloboda (*Magna Carta*), Povelja o pravima iz 1689. (*Bill of Rights 1689*) i Zakon o ljudskim pravima iz 1998. (*Human Rights Act 1998*). Temeljna prava pojedinaca razvila su se, kao dio ustava, u okviru precedentnog prava (*common law*), zakonskih akata i međunarodnih ugovora, osobito Europske konvencije o ljudskim pravima (EKLJP), koju je Ujedinjena Kraljevina ratificirala 1951. Ujedinjena Kraljevina ratificirala je 1987. i Konvenciju Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka (Konvencija br. 108) ([10]).

(9) Zakonom o ljudskim pravima iz 1998. prava iz EKLJP-a ugrađuju se u pravo Ujedinjene Kraljevine. Tim se zakonom svim pojedincima daju temeljna prava i slobode predviđene člancima od 2. do 12. i člankom 14. EKLJP-a te člancima od 1. do 3. Protokola br. 1 uz EKLJP i člankom 1. Protokola br. 13 uz EKLJP, u vezi s člancima od 16. do 18. EKLJP-a. To uključuje pravo na poštovanje osobnog i obiteljskog života, koje pak uključuje pravo na zaštitu podataka, te pravo na pošteno suđenje ([11]). Naime, u skladu s člankom 8. EKLJP-a tijelo javne vlasti smije zadirati u pravo na privatnost samo u skladu sa zakonom i ako je to u demokratskom društvu nužno radi interesa državne sigurnosti, javnog reda i mira ili gospodarske dobrobiti zemlje te radi sprečavanja nereda ili zločina, radi zaštite zdravlja ili morala ili radi zaštite prava i sloboda drugih.

([8]) Zakon o zaštiti podataka iz 2018., dostupan na: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak F: Kazneni progon, dostupan na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Načela iz Konvencije br. 108 izvorno su provedena u pravu Ujedinjene Kraljevine Zakonom o zaštiti podataka iz 1984., koji je zamijenjen Zakonom o zaštiti podataka iz 1998., a zatim Zakonom o zaštiti podataka iz 2018. (tumačenim zajedno s Općom uredbom Ujedinjene Kraljevine o zaštiti podataka). Ujedinjena Kraljevina potpisala je 2018. i Protokol o izmjeni Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (poznat kao „Konvencija br. 108+") te trenutačno radi na ratifikaciji te konvencije.

([11]) Članci 6. i 8. EKLJP-a (vidjeti i Prilog 1. Zakonu o ljudskim pravima iz 1998.).

(10) U skladu sa Zakonom o ljudskim pravima iz 1998. svi postupci tijelâ javne vlasti moraju biti u skladu s pravima zajamčenima u EKLJP-u ([12]). Osim toga, primarno i sekundarno zakonodavstvo moraju se tumačiti i provoditi u skladu s tim pravima ([13]). Ako bilo koji pojedinac smatra da su tijela javne vlasti prekršila njegova prava, uključujući prava na privatnost i zaštitu podataka, može dobiti sudsku zaštitu pred sudovima Ujedinjene Kraljevine na temelju Zakona o ljudskim pravima iz 1998. te konačno, nakon što iscrpi sve nacionalne pravne lijekove, može dobiti sudsku zaštitu pred Europskim sudom za ljudska prava za povrede prava zajamčenih EKLJP-om.

2.2. **Okvir za zaštitu podataka u Ujedinjenoj Kraljevini**

(11) Ujedinjena Kraljevina povukla se iz Unije 31. siječnja 2020. Na temelju Sporazuma o povlačenju Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske iz Europske unije i Europske zajednice za atomsku energiju ([14]) pravo Unije nastavilo se primjenjivati u Ujedinjenoj Kraljevini u prijelaznom razdoblju do 31. prosinca 2020. Prije povlačenja i u prijelaznom razdoblju zakonodavni okvir za zaštitu osobnih podataka u Ujedinjenoj Kraljevini kojim se uređuje obrada osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje, sastojao se od relevantnih dijelova Zakona o zaštiti podataka iz 2018., kojim je prenesena Direktiva (EU) 2016/680.

(12) Kako bi se pripremila za izlazak iz EU-a, Vlada Ujedinjene Kraljevine donijela je Zakon o povlačenju iz Europske unije iz 2018. (*European Union (Withdrawal) Act*, EUWA) ([15]), kojim je izravno primjenjivo zakonodavstvo Unije uključeno u pravo Ujedinjene Kraljevine i kojim je predviđeno da takozvano „domaće zakonodavstvo koje proizlazi iz prava EU-a" i dalje proizvodi pravne učinke nakon kraja prijelaznog razdoblja. Dio 3. DPA-a iz 2018. ([16]) kojom se prenosi Direktiva (EU) 2016/680 sastoji se od „domaćeg zakonodavstva koje proizlazi iz prava EU-a" na temelju Zakona o povlačenju. Prema Zakonu o povlačenju sudovi u Ujedinjenoj Kraljevini neizmijenjeno „domaće zakonodavstvo koje proizlazi iz prava EU-a" moraju tumačiti u skladu s relevantnom sudskom praksom Suda Europske unije (Sud) i općim načelima prava Unije, u skladu s pravnim učinkom koji su ta praksa i načela imali neposredno prije kraja prijelaznog razdoblja (takozvana „zadržana sudska praksa EU-a" odnosno „zadržana opća načela prava EU-a") ([17]).

(13) Na temelju Zakona o povlačenju ministri Ujedinjene Kraljevine imaju ovlast da podređenim zakonskim aktima (*statutory instruments*) donose sekundarno zakonodavstvo kako bi uveli potrebne izmjene zadržanog prava Unije koje su posljedica povlačenja Ujedinjene Kraljevine iz Unije. Ta je ovlast iskorištena za donošenje Uredbe o zaštiti podataka, privatnosti i elektroničkim komunikacijama (izmjene itd.) (izlazak iz EU-a) iz 2019. (Uredba DPPEC) ([18]). Njome se mijenja zakonodavstvo Ujedinjene Kraljevine o zaštiti podataka, uključujući DPA iz 2018., kako bi odgovaralo domaćem kontekstu ([19]).

([12]) Članak 6. Zakona o ljudskim pravima iz 1998.

([13]) Članak 3. Zakona o ljudskim pravima iz 1998.

([14]) Sporazum o povlačenju Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske iz Europske unije i Europske zajednice za atomsku energiju, 2019/C 384 I/01, XT/21054/2019/INIT, SL C 384I, 12.11.2019., str. 1.–177. („Sporazum o povlačenju"), dostupan na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=HR.

([15]) Zakon o povlačenju iz Europske unije iz 2018., dostupan na: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Zakon o zaštiti podataka iz 2018., dostupan na: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([17]) Članak 6. Zakona o povlačenju iz 2018.

([18]) Uredba o zaštiti podataka, privatnosti i elektroničkim komunikacijama (izmjene itd.) (izlazak iz EU-a) iz 2019., dostupna na: https://www.legislation.gov.uk/uksi/2019/419/contents/made, kako je izmijenjena Uredbom DPPEC iz 2020., koja je dostupna na: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) Uredbama o izlasku uvodi se niz izmjena dijela 3. DPA-a iz 2018. Mnoge od njih tehničke su prirode, primjerice, brisanje upućivanja na „državu članicu" ili „Direktivu o zaštiti podataka u svrhe kaznenog progona" (vidjeti, primjerice, članak 48. stavak 8. ili članak 73. stavak 5. točku (a)) u DPA-u iz 2018. koja se zamjenjuju upućivanjem na „domaće pravo", kako bi dio 3. djelotvorno funkcionirao kao domaće pravo nakon isteka prijelaznog razdoblja. Na nekim su mjestima bile potrebne druge vrste izmjena, primjerice, s obzirom na to „tko" donosi „odluke o primjerenosti" za potrebe zakonodavnog okvira Ujedinjene Kraljevine za zaštitu podataka (vidjeti članak 74.A DPA-a iz 2018.), tj. ministar umjesto Europske komisije.

(14) Slijedom toga, pravni standardi za obradu osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje, u Ujedinjenoj Kraljevini nakon prijelaznog razdoblja na temelju Sporazuma o povlačenju i dalje će biti utvrđeni u relevantnim dijelovima DPA-a iz 2018. (ali kako je izmijenjena Uredbom DPPEC), a posebno u njezinu dijelu 3. Opća uredba Ujedinjene Kraljevine o zaštiti podataka ne primjenjuje se na tu vrstu obrade.

(15) U dijelu 3. DPA-a iz 2018. predviđaju se pravila za obradu osobnih podataka u svrhe kaznenog progona, uključujući načela zaštite podataka, pravne osnove za obradu (zakonitost), prava ispitanika, obveze nadležnih tijela kao voditelja obrade i ograničenja daljnjih prijenosa. Istodobno se u dijelovima 5. i 6. DPA-a iz 2018. predviđaju primjenjiva pravila o nadzoru, provedbi i sudskoj zaštiti koja se primjenjuju na sektor kaznenog progona.

(16) Nadalje, kad je riječ o odgovarajućoj ulozi policijskih snaga u sektoru kaznenog progona, trebalo bi voditi računa o pravilima kojima se uređuje policijska djelatnost. Budući da je djelatnost policije pitanje iz prenesene nadležnosti, na nju se u (a) Engleskoj i Walesu, (b) Škotskoj i (c) Sjevernoj Irskoj primjenjuju različiti zakonodavni akti koji su, međutim, sadržajno često slični ([20]). Osim toga, u različitim vrstama smjernica navode se dodatna pojašnjenja o tome kako bi se policijske ovlasti trebale primjenjivati. Tri su glavna oblika policijskih smjernica: 1. zakonske smjernice koje se donose na temelju zakonodavstva, kao što su Etički kodeks ([21]) i Kodeks prakse za upravljanje policijskim informacijama ([22]), koje se donose na temelju Zakona o policiji iz 1996. ([23]), ili kodeksi PACE ([24]), koji se donose na temelju Zakona o policiji i kaznenim dokazima ([25]); 2. odobrena profesionalna praksa za upravljanje policijskim informacijama (Smjernice o odobrenoj profesionalnoj praksi za upravljanje policijskim informacijama) ([26]), koje donosi Nacionalna agencija za policiju (*College of Policing*); i 3. operativne smjernice (koje izdaje sama policija). Nacionalno vijeće načelnika policije (*National Police Chiefs' Council*) (koordinacijsko tijelo za sve policijske snage u Ujedinjenoj Kraljevini) izdaje operativne smjernice koje su prihvatile sve policijske snage te se stoga primjenjuju na nacionalnoj razini ([27]). Tim se smjernicama nastoji osigurati usklađenost među policijskim snagama u načinu upravljanja informacijama ([28]).

(17) Kodeks prakse za upravljanje policijskim informacijama donio je ministar 2005. služeći se ovlastima predviđenima u članku 39.A Zakona o policiji iz 1996. ([29]) Svaki kodeks prakse donesen na temelju Zakona o policiji mora dobiti odobrenje ministra te podliježe obvezi savjetovanja s Nacionalnom agencijom za kriminalitet prije nego što se uputi Parlamentu. U članku 39.A stavku 7. Zakona o policiji zahtijeva se da se policija uredno pridržava kodeksa

([20]) Za detaljnija objašnjenja o policijskim snagama i njihovim ovlastima u Ujedinjenoj Kraljevini vidjeti: Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak F: Kazneni progon (vidjeti bilješku 9.).

([21]) Kodeks prakse za načela i standarde profesionalnog ponašanja za policijsku struku u Engleskoj i Walesu, dostupan na: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Etički kodeks Policijske službe Sjeverne Irske, dostupan na: https://www.nipolicingboard.org.uk/psni-code-ethics; Etički kodeks za policijsku djelatnost u Škotskoj, dostupan na: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) Kodeks prakse za upravljanje policijskim informacijama, dostupan na: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) Zakon o policiji iz 1996., dostupan na: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Kodeksi prakse doneseni na temelju Zakona o policiji i kaznenim dokazima iz 1984. (PACE), dostupni na: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([25]) Zakon o policiji i kaznenim dokazima iz 1984., dostupan na: https://www.legislation.gov.uk/ukpga/1984/60/contents

([26]) Odobrena profesionalna praksa za upravljanje policijskim informacijama, dostupna na: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Priručnik o zaštiti podataka za policijske stručnjake za zaštitu podataka, dostupan na: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) Na primjer, Kodeks prakse za upravljanje policijskim informacijama (vidjeti bilješku 22.) primjenjuje se na zadržavanje operativnih policijskih informacija (vidjeti uvodnu izjavu (47). ove Odluke).

([29]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, u razdoblju rasprava o primjerenosti Nacionalna agencija za policiju bila je u postupku sastavljanja Kodeksa prakse za upravljanje informacijama i evidencijama koji će zamijeniti Kodeks prakse za upravljanje policijskim informacijama. Nacrt kodeksa objavljen je 25. siječnja 2021. radi javnog savjetovanja i dostupan je na: https://www.college.police.uk/article/information-records-management-consultation

donesenih na temelju tog zakona, te se od policije stoga očekuje da postupa u skladu s njima ([30]). Nadalje, izvanzakonske smjernice (kao što su Smjernice o odobrenoj profesionalnoj praksi za upravljanje policijskim informacijama) moraju uvijek biti u skladu s Kodeksom prakse za upravljanje policijskim informacijama, koji im je nadređen ([31]). U svakom slučaju, iako mogu postojati određene operativne situacije u kojima je potrebno da policijski službenici odstupe od tih smjernica, od njih se i dalje zahtijeva da poštuju zahtjeve iz dijela 3. DPA-a iz 2018. ([32])

(18) Dodatne smjernice o zakonodavstvu o zaštiti podataka Ujedinjene Kraljevine za obradu u sektoru kaznenog progona daje povjerenik za informiranje („povjerenik za informiranje" ili „ICO" (Ured povjerenika za informiranje)) ([33]) (za dodatne pojedinosti o ICO-u vidjeti uvodne izjave od (93). do (109).). Iako nisu pravno obvezujuće, u sudskom postupku sudovi bi bili obvezni uzeti u obzir svako kršenje tih smjernica jer su one važne za tumačenje i pokazuju kako povjerenik u praksi tumači i provodi zakonodavstvo o zaštiti podataka ([34]).

(19) Naposljetku, kako je navedeno u uvodnim izjavama od (8). do (10)., tijela kaznenog progona Ujedinjene Kraljevine moraju se pridržavati (EKLJP-a) i Konvencije br. 108.

(20) Stoga su struktura i glavne sastavnice pravnog okvira kojim se uređuje obrada podataka koju obavljaju tijela kaznenog progona u Ujedinjenoj Kraljevini vrlo slične okviru koji se primjenjuje u EU-u. To uključuje činjenicu da se taj okvir ne oslanja samo na obveze utvrđene u nacionalnom pravu, koje su oblikovane pravom Unije, već i na obveze iz međunarodnog prava, osobito obveze Ujedinjene Kraljevine da poštuje EKLJP i Konvenciju br. 108 i priznavanje nadležnosti Europskog suda za ljudska prava. Stoga su te obveze koje proizlaze iz pravno obvezujućih međunarodnih instrumenata, a koje se posebno odnose na zaštitu osobnih podataka, važan element pravnog okvira koji se procjenjuje u ovoj Odluci.

2.3. **Glavno i teritorijalno područje primjene**

(21) Glavno područje primjene dijela 3. DPA-a iz 2018. podudara se s područjem primjene Direktive (EU) 2016/680 kako je navedeno u njezinu članku 2. stavku 2. Dio 3. primjenjuje se na obradu osobnih podataka od strane nadležnog tijela koja se u cijelosti ili djelomično obavlja automatizirano te na neautomatiziranu obradu osobnih podataka od strane nadležnog tijela koji čine dio sustava pohrane ili su namijenjeni tome da budu dio sustava pohrane.

(22) Nadalje, da bi obrada bila obuhvaćena područjem primjene dijela 3., voditelj obrade mora biti „nadležno tijelo" te se obrada mora obavljati „u svrhu kaznenog progona". Stoga se režim zaštite podataka koji se procjenjuje u ovoj Odluci primjenjuje na sve aktivnosti kaznenog progona koje obavljaju ta nadležna tijela.

(23) Pojam „nadležno tijelo" definiran je u članku 30. DPA-a kao osoba navedena u Prilogu 7. DPA-u iz 2018. te bilo koja druga osoba u mjeri u kojoj ima zakonski propisane funkcije u obavljanju bilo koje od svrha kaznenog progona. Među nadležnim tijelima navedenima u Prilogu 7. ne nalaze se samo policijske snage, već i svi vladini odjeli pod izravnim nadzorom ministarstava Ujedinjene Kraljevine kao i druga tijela s istražnim funkcijama (npr. Porezna i carinska uprava Ujedinjene Kraljevine (*Commissioner for Her Majesty's Revenue and Customs*), Velška porezna uprava

([30]) U predmetu *R protiv the Commission of Police of the Metropolis* [2014] EWCA Civ 585 potvrđen je pravni status Kodeksa prakse za upravljanje policijskim informacijama, a viši prizivni sudac Laws ustvrdio je da je načelnik londonske policijske uprave, u skladu s člankom 39.A Zakona o policiji iz 1996., dužan voditi računa o Kodeksu prakse za upravljanje policijskim informacijama i Smjernicama o odobrenoj profesionalnoj praksi za upravljanje policijskim informacijama.

([31]) Inspekciju nad radom policije radi provjere pridržavanja Kodeksa prakse za upravljanje policijskim informacijama obavlja Inspektorat za policiju te vatrogasne i spasilačke službe u Engleskoj i Walesu (*Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services*, HMICFRS).

([32]) Vidjeti u tom pogledu stajalište Nacionalne agencije za policiju o poštovanju smjernica o odobrenoj profesionalnoj praksi s obzirom na sve elemente policijske djelatnosti, u kojem se objašnjava da te smjernice odobrava profesionalno tijelo za policijsku djelatnost (Nacionalna agencija za policiju) kao službeni izvor profesionalne prakse za policijsku djelatnost. Od policijskih službenika i osoblja očekuje se da vode računa o odobrenoj profesionalnoj praksi u obavljanju svojih dužnosti. Međutim, može doći do situacija u kojima postoji legitiman operativni razlog zbog kojeg policija može odstupiti od odobrene profesionalne prakse, pod uvjetom da postoji jasno opravdanje za takvo postupanje. Policija snosi odgovornost za svaki rizik na lokalnoj i nacionalnoj razini povezan s postupanjem koje nije u skladu s nacionalno dogovorenim smjernicama te je u slučaju incidenta ili istrage koji proizlaze iz takvog postupanja (primjerice, istrage koju provodi Neovisni ured za nadzor postupanja policije (Independent Office of Police Conduct)) „odgovorna za sve rizike", dostupno na: https://www.app.college.police.uk/faq-page/.

([33]) Vodič za obradu podataka u svrhe kaznenog progona, dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Vidjeti predmet *Bridges protiv the Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin) u kojem je Visoki sud, iako je uzeo u obzir izvanzakonsku prirodu smjernica povjerenika za informiranje, naveo da će sud „[k]ad razmatra pitanje je li voditelj obrade podataka poštovao obvezu iz članka 64. [o provođenju procjene učinka na zaštitu podataka u vezi s visokorizičnom obradom], uzeti u obzir smjernice koje je donio povjerenik za informiranje u pogledu procjena učinka na zaštitu podataka".

(*Welsh Revenue Authority*), Nadležno tijelo za tržišno natjecanje i tržišta (*Competition and Markets Authority*), Zemljišnoknjižni ured za Englesku i Wales (*Her Majesty's Land Register*) ili Nacionalna agencija za kriminalitet), državna odvjetništva, druga tijela kaznenog pravosuđa i drugi ovlaštenici ili organizacije koji obavljaju aktivnosti kaznenog progona ([35]). Dio 3. DPA-a iz 2018. primjenjuje se i na sudove kad oni izvršavaju svoje sudbene funkcije, osim u dijelu koji se odnosi na prava ispitanika i nadzor koji obavlja ICO ([36]). Popis nadležnih tijela navedenih u Prilogu 7. nije konačan te ga ministar može ažurirati uredbom uzimajući u obzir promjene u organizaciji javnih službi ([37]).

(24) Predmetna obrada ujedno se mora provoditi „u svrhu kaznenog progona", što se definira kao sprečavanje, istraga, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje ([38]). Obrada koju nadležno tijelo ne provodi u svrhe kaznenog progona nije uređena dijelom 3. DPA-a iz 2018. To će biti slučaj, primjerice, kad Nadležno tijelo za tržišno natjecanje i tržišta istražuje predmete u kojima ne postoje elementi kaznenih djela (npr. koncentracije između trgovačkih društava). U tom će se slučaju primjenjivati Opća uredba Ujedinjene Kraljevine o zaštiti podataka, zajedno s dijelom 2. DPA-a iz 2018., jer nadležna tijela tu obradu osobnih podataka provode u svrhe koje nisu svrhe kaznenog progona. Da bi utvrdilo koji se režim zaštite podataka primjenjuje (dio 3. ili dio 2. DPA-a iz 2018.) na predmetnu obradu osobnih podataka, nadležno tijelo, tj. voditelj obrade, mora ocijeniti je li „primarna svrha" te obrade obuhvaćena svrhama kaznenog progona na temelju DPA-a iz 2018.

(25) Kad je riječ o teritorijalnom području primjene dijela 3. DPA-a iz 2018., u članku 207. stavku 2. predviđa se da se DPA primjenjuje na obradu osobnih podataka u kontekstu aktivnosti osobe koja ima poslovni nastan na cijelom državnom području Ujedinjene Kraljevine. To uključuje tijela javne vlasti na područjima Engleske, Walesa, Škotske i Sjeverne Irske koja su obuhvaćena glavnim područjem primjene iz dijela 3. DPA-a iz 2018. ([39])

2.3.1. *Definicija osobnih podataka i obrade*

(26) Ključni pojmovi „osobni podaci" i „obrada" definirani su u članku 3. DPA-a iz 2018. i primjenjuju se u cijeloj DPA-u. Definicije su vrlo slične odgovarajućim definicijama utvrđenima u članku 3. Direktive (EU) 2016/680. Prema DPA-u iz 2018. pojam „osobni podaci" znači svi podaci koji se odnose na živog pojedinca čiji je identitet utvrđen ili se može utvrditi ([40]). Prema članku 3. stavku 3. DPA-a iz 2018. identitet pojedinca može se utvrditi ako se tog pojedinca može izravno ili neizravno identificirati na temelju tih podataka, među ostalim, s pomoću imena ili identifikatora ili s pomoću jednog ili više čimbenika svojstvenih za fizički, fiziološki, genetski, mentalni, ekonomski, kulturni ili socijalni identitet tog pojedinca. Pojam „obrada" definira se kao postupak ili skup postupaka koji se obavljaju na podacima ili skupovima podataka, kao što su (a) prikupljanje, bilježenje, organizacija, strukturiranje ili pohrana; (b) prilagodba ili izmjena; (c) pronalaženje, obavljanje uvida ili uporaba; (d) otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način; (e) usklađivanje ili kombiniranje; ili (f) ograničavanje, brisanje ili uništavanje. Nadalje, u Zakonu se definira „osjetljiva obrada" kao „(a) obrada osobnih podataka koji otkrivaju rasno ili etničko podrijetlo, politička mišljenja, religijska ili filozofska vjerovanja ili članstvo u sindikatu; (b) obrada genetskih podataka ili biometrijskih podataka u svrhu jedinstvene identifikacije pojedinca; (c) obrada podataka koji se odnose na zdravlje; ili (d) obrada podataka o spolnom životu ili seksualnoj orijentaciji pojedinca" ([41]). S obzirom na to, u članku 205. DPA-a iz 2018. navodi se definicija „biometrijskih podataka" ([42]), „podataka koji se odnose na zdravlje" ([43]) i „genetskih podataka" ([44]).

([35]) Među njima se u Prilogu 7. DPA-u iz 2018. navode glavni javni tužitelj, glavni javni tužitelj za Sjevernu Irsku i povjerenik za informiranje.

([36]) Članak 43. stavak 3. DPA-a iz 2018.

([37]) Članak 30. stavak 3. DPA-a iz 2018. Obavještajne službe (Tajna obavještajna služba (*Secret Intelligence Service*), Sigurnosna služba (*Security Service*) i Vladin komunikacijski stožer (*Government Communications Headquarters*)) nisu nadležna tijela (vidjeti članak 30. stavak 2. DPA-a iz 2018.), pa se dio 3. DPA-a iz 2018. ne primjenjuje ni na jednu od njihovih aktivnosti. Njihove aktivnosti obuhvaćene su područjem primjene dijela 4. DPA-a iz 2018.

([38]) Članak 31. DPA-a iz 2018.

([39]) To znači da se DPA iz 2018., a time i ova Odluka, ne primjenjuju na krunske posjede Ujedinjene Kraljevine i ostala prekomorska područja Ujedinjene Kraljevine, kao što su, primjerice, Falklandski Otoci i područje Gibraltara.

([40]) Osobni podaci koji se odnose na preminule osobe nisu obuhvaćeni područjem primjene DPA-a iz 2018.

([41]) Članak 35. stavak 8. DPA-a iz 2018.

([42]) „Biometrijski podaci" znači osobni podaci dobiveni posebnom tehničkom obradom u vezi s fizičkim obilježjima, fiziološkim obilježjima ili obilježjima ponašanja pojedinca koja omogućuju ili potvrđuju jedinstvenu identifikaciju tog pojedinca, kao što su fotografije lica ili daktiloskopski podaci.

([43]) „Podaci koji se odnose na zdravlje" znači osobni podaci povezani s fizičkim ili mentalnim zdravljem pojedinca, uključujući pružanje zdravstvenih usluga, kojima se daju informacije o njegovu zdravstvenom statusu.

([44]) „Genetski podaci" znači osobni podaci koji se odnose na nasljeđena ili stečena genetska obilježja pojedinca koja daju jedinstvenu informaciju o fiziologiji ili zdravlju tog pojedinca, i koji su dobiveni osobito analizom biološkog uzorka dotičnog pojedinca.

(27) U članku 32. DPA-a iz 2018. pojašnjavaju se definicije pojmova „voditelj obrade” i „izvršitelj obrade” u kontekstu obrade osobnih podataka u svrhe kaznenog progona koje su vrlo slične odgovarajućim definicijama iz Direktive (EU) 2016/680. „Voditelj obrade” znači nadležno tijelo koje određuje svrhe i sredstva obrade osobnih podataka. Ako se obrada zahtijeva zakonom, voditelj obrade je nadležno tijelo kojem je takva obveza uvedena tim zakonom. „Izvršitelj obrade” definiran je kao svaka osoba koja obrađuje osobne podatke u ime voditelja obrade (a koja nije zaposlenik voditelja obrade).

2.4. **Zaštitne mjere, prava i obveze**

2.4.1. *Zakonitost i poštenost obrade*

(28) U skladu s člankom 35. DPA-a iz 2018. obrada osobnih podataka mora biti zakonita i poštena, slično onomu što je predviđeno u članku 4. stavku 1. točki (a) Direktive (EU) 2016/680. U skladu s člankom 35. stavkom 2. DPA-a iz 2018. obrada osobnih podataka u bilo koju svrhu kaznenog progona zakonita je samo ako se temelji na pravu te ako je ispitanik dao privolu za obradu u tu svrhu ili je obrada nužna za izvršavanje zadaće koju u tu svrhu obavlja nadležno tijelo.

2.4.1.1. Obrada na temelju prava

(29) Slično kao i u članku 8. Direktive (EU) 2016/680, da bi se osigurala zakonitost obrade obuhvaćene dijelom 3. DPA-a iz 2018., takva obrada mora se „temeljiti na pravu”. „Zakonita” obrada znači obrada koja je dopuštena na temelju zakona, precedentnog prava ili kraljevskih prerogativa ([45]).

(30) Ovlasti nadležnih tijela općenito su uređene zakonima, što znači da su njihove funkcije i ovlasti jasno utvrđene u zakonodavnim aktima koje je donio Parlament ([46]). U određenim se slučajevima policija i druga nadležna tijela navedena u Prilogu 7. DPA-u iz 2018. mogu pozivati na precedentno pravo (*common law*) radi obrade podataka ([47]). Precedentno pravo nastalo je na temelju presedana utvrđenih u odlukama sudova. Precedentno pravo relevantno je u kontekstu ovlasti kojima raspolaže policija, čija osnovna dužnost zaštite javnosti otkrivanjem i sprečavanjem kaznenih djela proizlazi iz tog izvora prava ([48]). Međutim, policijske snage imaju ovlasti za izvršavanje te dužnosti koje se temelje i na precedentnom

([45]) Objašnjenja DPA-a iz 2018., točka 181., dostupna na: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Ovlasti Nacionalne agencije za kriminalitet proizlaze iz Zakona o kaznenim djelima i sudovima iz 2013., koji je dostupan na: https://www.legislation.gov.uk/ukpga/2013/22/contents. Slično tomu, ovlasti Agencije za standarde hrane predviđene su Zakonom o standardima hrane iz 1999., koji je dostupan na: https://www.legislation.gov.uk/ukpga/1999/28/contents. Ostali primjeri uključuju Zakon o progonu počinitelja kaznenih djela iz 1985., kojim je osnovana Krunska služba za kazneni progon (*Crown Prosecution Service*) (vidjeti: https://www.legislation.gov.uk/ukpga/1985/23/contents); Zakon o povjerenicima za prihod i carine iz 2005., kojim je osnovana Porezna i carinska uprava Ujedinjene Kraljevine (*Her Majesty's Revenue and Customs*) (vidjeti: https://www.legislation.gov.uk/ukpga/2005/11/contents); Zakon o kaznenom postupku za Škotsku iz 1995., kojim je osnovano Škotsko povjerenstvo za preispitivanje kaznenih predmeta (vidjeti: https://www.legislation.gov.uk/ukpga/1995/46/contents); Zakon o pravosuđu za Sjevernu Irsku iz 2002., kojim je osnovano Javno tužiteljstvo (*Public Prosecution Service*) u Sjevernoj Irskoj (vidjeti: https://www.legislation.gov.uk/ukpga/2002/26/contents) te Ured za suzbijanje teških prijevara (*Serious Fraud Office*), koji je osnovan i kojem su dane ovlasti na temelju Zakona o kaznenom pravosuđu iz 1987. (vidjeti: https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Na primjer, prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, u okviru Državnog odvjetništva Škotske (*Crown Office and Procurator Fiscal Service*), koje je odgovorno za kazneni progon u Škotskoj, škotski ministar pravosuđa (*Lord Advocate*), koji je na čelu sustava kaznenog progona u Škotskoj, izvodi svoje ovlasti za provođenje istraga smrtnih slučajeva i za progon kaznenih djela iz precedentnog prava, dok su neke njegove funkcije utvrđene zakonom. Nadalje, Kruna i, u širem smislu, razni vladini odjeli i ministri, isto tako izvode svoje ovlasti iz kombinacije zakonodavstva, precedentnog prava i kraljevskih prerogativa (to su ovlasti iz precedentnog prava koje pripadaju Kruni, ali ih izvršavaju ministri).

([48]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak F: Kazneni progon, str. 8. (vidjeti bilješku 9.).

pravu i na zakonskim ovlastima ([49]). Ako policija ima određenu zakonsku ovlast, ta ovlast ima prednost u odnosu na bilo koju ovlast iz precedentnog prava ([50]).

(31) Sudovi su potvrdili da opseg ovlasti i obveza policijskog službenika koje proizlaze iz precedentnog prava uključuje „sve mjere koje mu se čine nužnima za održavanje mira, sprečavanje kaznenih djela ili zaštitu imovine od štete nanesene kaznenim djelima" ([51]). Ovlasti iz precedentnog prava nisu neograničene ovlasti. One podliježu nizu ograničenja, uključujući ograničenja koja su utvrdili sudovi ([52]) i ograničenja koja su uvedena zakonodavstvom, ponajprije Zakonom o ljudskim pravima iz 1998. i Zakonom o ravnopravnosti iz 2010. ([53]) Osim toga, za nadležna tijela koja obrađuju podatke na temelju dijela 3. DPA-a iz 2018. to uključuje obvezu da ovlasti iz precedentnog prava izvršavaju u skladu sa zahtjevima utvrđenima u DPA-u iz 2018. ([54]) Nadalje, pri odlučivanju o provođenju bilo koje vrste obrade podataka moraju se uzeti u obzir zahtjevi iz primjenjivih smjernica, kao što su Kodeks prakse za upravljanje policijskim informacijama te smjernice koje su specifične za neku od zemalja Ujedinjene Kraljevine ([55]). Vlada i operativna policijska tijela izdaju niz smjernica radi osiguravanja da policijski službenici svoje ovlasti za obradu izvršavaju u okviru ograničenja utvrđenih precedentnim pravom ili odgovarajućim zakonom ([56]).

(32) Kraljevski prerogativi predstavljaju još jednu sastavnicu „prava" i odnose se na određene ovlasti koje pripadaju Kruni i koje može izvršavati izvršna vlast, a koje se ne temelje na zakonu, već proizlaze iz suvereniteta monarha ([57]). Vrlo je malo primjera prerogativnih ovlasti koje su relevantne u kontekstu kaznenog progona. One uključuju, primjerice, okvir za uzajamnu pravnu pomoć kojim se ministru omogućuje razmjena podataka s trećim zemljama u svrhe

([49]) Ključni zakonodavni akti kojima se utvrđuje režim glavnih policijskih ovlasti (uhićenje, pretraga, odobrenje za produljenje pritvora, uzimanje otisaka prstiju, uzimanje uzoraka tjelesnim pregledom, nalog za presretanje, pristup podacima o komunikacijama) jesu: i. za Englesku i Wales: Zakon o policiji i kaznenim dokazima iz 1984. (PACE), dostupan na: https://www.legislation.gov.uk/ukpga/1984/60/contents (kako je izmijenjen Zakonom o zaštiti sloboda iz 2012. (PoFA), dostupnim na: https://www.legislation.gov.uk/ukpga/2012/9/contents), i Zakon o istražnim ovlastima iz 2016. (IPA), dostupan na: https://www.legislation.gov.uk/ukpga/2016/25/contents; ii. za Škotsku: Zakon o kaznenom pravosuđu za Škotsku iz 2016., dostupan na: https://www.legislation.gov.uk/asp/2016/1/contents, i Zakon o kaznenom postupku za Škotsku iz 1995., dostupan na: https://www.legislation.gov.uk/ukpga/1995/46/contents); iii. za Sjevernu Irsku: Uredba o policiji i kaznenim dokazima za Sjevernu Irsku iz 1989., dostupna na: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Tijela Ujedinjene Kraljevine objasnila su da je primat kodificiranog prava odavno ustaljen u Ujedinjenoj Kraljevini, još od presude u predmetu *Entick protiv Carrington* [1765] EWHC KB J98, u kojoj je potvrđeno da postoje granice u kojima izvršna vlast može izvršavati svoje ovlasti te je uspostavljeno načelo da su ovlasti iz precedentnog prava i prerogativne ovlasti monarha i vlade podređene pravnom poretku zemlje.

([51]) Vidjeti predmet *Rice protiv Connolly* [1966] 2 QB 414.

([52]) Vidjeti predmet *R(Catt) protiv Association of Chief police Officers* [2015] AC 1065, u kojem je, u odnosu na policijsku ovlast prikupljanja i čuvanja informacija o pojedincu (koji je počinio kazneno djelo), lord Sumption presudio da prema precedentnom pravu policija ima ovlast prikupljanja i pohrane informacija za potrebe policijskog rada, to jest, općenito govoreći, za održavanje javnog reda te sprečavanje i otkrivanje kaznenih djela. Te ovlasti ne dopuštaju primjenu intruzivnih metoda prikupljanja informacija, kao što su ulazak na privatni posjed ili postupci (osim uhićenja na temelju ovlasti iz precedentnog prava) koji bi činili napad. Sudac je u tom predmetu smatrao da su ovlasti iz precedentnog prava bile sasvim dovoljne za dopuštanje prikupljanja i pohrane one vrste javnih informacija o kojima je bilo riječ u tim žalbenim postupcima.

([53]) Zakon o ravnopravnosti iz 2010., dostupan na: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Za primjer predmeta u kojem se policijske ovlasti iz precedentnog prava ocjenjuju prema okviru iz DPA-a iz 1998. vidjeti odluku Visokog suda u predmetu *Bridges protiv the Chief Constable of South Wales Police* (vidjeti bilješku 33.). Vidjeti i predmete *Vidal-Hall protiv Google Inc* [2015] EWCA Civ 311 i *Richard protiv BBC* [2018] EWHC 1837 (Ch).

([55]) Vidjeti, primjerice, smjernice Policijske službe Sjeverne Irske o službenim uputama za upravljanje evidencijama, dostupne na: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Zastupnički dom Parlamenta objavio je informativni dokument u kojem se navode ključne ovlasti policije u Engleskoj i Walesu iz precedentnog prava i zakona (vidjeti https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Prema tom dokumentu, primjerice, dok ovlasti održavanja javnog reda i mira (*the Crown's peace*) te „primjene prisile" proizlaze iz precedentnog prava, „ovlasti zaustavljanja i pretraživanja" uvijek proizlaze iz zakona. Osim toga, škotska vlada na svojim internetskim stranicama navodi informacije o policijskim ovlastima uhićenja te zaustavljanja i pretraživanja (vidjeti https://www.gov.scot/policies/police/police-powers/).

([57]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, prerogativne ovlasti koje izvršava vlada uključuju, primjerice, sklapanje i ratifikaciju ugovora, vođenje diplomacije, korištenje oružanih snaga unutar Ujedinjene Kraljevine radi održavanja mira kao podrška radu policije.

kaznenog progona, pri čemu ovlast za razmjenu podataka na taj način nije uvijek utvrđena zakonom ([58]). Kraljevski prerogativi ograničeni su načelima precedentnog prava ([59]) i podređeni zakonima, pa stoga podliježu ograničenjima predviđenima u Zakonu o ljudskim pravima iz 1998. i DPA-u iz 2018. ([60])

(33) Slično kao i u članku 8. Direktive (EU) 2016/680, u režimu Ujedinjene Kraljevine zahtijeva se da nadležna tijela radi poštovanja načela zakonitosti osiguraju da obrada, kad se temelji na zakonu, ujedno bude i „nužna" za izvršavanje zadaće koja se obavlja u svrhu kaznenog progona. ICO daje smjernice u tom pogledu u kojima se pojašnjava da se „ta svrha mora ostvariti ciljano i proporcionalno. Zakonita osnova neće se primjenjivati ako se ta svrha može relativno lako ostvariti nekim drugim manje nametljivim sredstvima. Nije dovoljno ustvrditi da je obrada nužna zbog toga što je netko odlučio obavljati svoje poslovanje na određen način. Postavlja se pitanje je li obrada nužna za tu navedenu svrhu" ([61]).

2.4.1.2. Obrada na temelju „privole" ispitanika

(34) Kako je navedeno u uvodnoj izjavi (28)., u članku 35. stavku 2. DPA-a iz 2018. predviđa se mogućnost obrade osobnih podataka na temelju „privole" pojedinca.

(35) Međutim, čini se da privola nije relevantna pravna osnova za postupke obrade koji su obuhvaćeni područjem primjene ove Odluke. Zapravo, postupci obrade obuhvaćeni ovom Odlukom uvijek će se odnositi na podatke koje je na temelju Direktive (EU) 2016/680 nadležno tijelo države članice prenijelo nadležnom tijelu Ujedinjene Kraljevine. Oni stoga obično neće uključivati vrstu izravne interakcije (prikupljanje) između tijela javne vlasti i ispitanikâ koja se može temeljiti na privoli u skladu s člankom 35. stavkom 2. točkom (a) DPA-a iz 2018.

(36) Iako se oslanjanje na privolu stoga ne smatra relevantnim za procjenu koja se provodi u ovoj Odluci, radi potpunosti treba napomenuti da se u kontekstu kaznenog progona obrada nikad ne temelji isključivo na privoli jer nadležno tijelo mora uvijek imati temeljnu ovlast koja mu omogućuje da obrađuje te podatke ([62]). Konkretnije, i slično onomu što je dopušteno na temelju Direktive (EU) 2016/680 ([63]), to znači da privola služi kao dodatan uvjet za omogućivanje određenih ograničenih i posebnih postupaka obrade koji se inače ne bi mogli provesti, na primjer prikupljanja i obrade uzorka DNK-a pojedinca koji nije osumnjičenik. U tom se slučaju obrada ne bi provela ako privola nije dobivena ili je povučena ([64]).

([58]) Vidjeti u tom pogledu procjenu režima Ujedinjene Kraljevine za daljnje prijenose u uvodnim izjavama od (74). do (87).

([59]) Vidjeti predmet *Bancoult protiv Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61, u kojem su sudovi presudili da prerogativna ovlast za donošenje vladinih uredbi (*Orders in Council*) isto podliježe redovnim osnovama za sudsko preispitivanje.

([60]) Vidjeti predmet *Attorney-General protiv De Keyser's Royal Hotel Ltd* [1920] AC 508, u kojem je sud presudio da se prerogativne ovlasti ne mogu koristiti ako su ih zamijenile zakonske ovlasti; predmet *Laker Airways Ltd protiv Department of Trade* [1977] QB 643, u kojem je sud presudio da se prerogativne ovlasti ne mogu koristiti radi onemogućivanja djelovanja kodificiranog prava; predmet *R protiv Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3, u kojem je sud presudio da se prerogativne ovlasti ne mogu koristiti ako su u sukobu s važećim zakonodavstvom, čak i ako to važeće zakonodavstvo nije još stupilo na snagu; predmet *R (Miller) protiv Secretary of State for Exiting the European Union* [2017] UKSC 5, u kojem je sud potvrdio mogućnost da se kodificiranim pravom mijenjaju i ukidaju prerogativne ovlasti. Za opći pregled odnosa između kraljevskih prerogativa i ovlasti iz zakona ili precedentnog prava vidjeti informativni dokument Zastupničkog doma koji je dostupan na: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Vodič za obradu podataka u svrhe kaznenog progona, „O čemu je riječ u prvom načelu?", dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) To proizlazi iz formulacije teksta relevantne odredbe DPA-a iz 2018. prema kojoj je obrada osobnih podataka u bilo koju svrhu kaznenog progona zakonita samo ako se i u mjeri kojoj se „temelji na pravu te ako je (a) ispitanik dao privolu za obradu u tu svrhu ili je (b) obrada nužna za izvršavanje zadaće koju u tu svrhu obavlja nadležno tijelo".

([63]) Vidjeti uvodne izjave 35. i 37. Direktive (EU) 2016/680.

([64]) Tijela Ujedinjene Kraljevine objasnila su da bi jedan od primjera kad bi privola mogla biti primjeren temelj za obradu bio slučaj kad policija prikuplja uzorak DNK-a u vezi s nestalom osobom kako bi ga mogla usporediti s tijelom osobe ako bi ga se pronašlo. U takvim okolnostima ne bi bilo primjereno da policija prisili ispitanika na davanje uzorka; umjesto toga, policija bi tražila privolu tog pojedinca, koja se daje dobrovoljno i može se povući u bilo kojem trenutku. Ako se privola povuče, ti se podaci više ne bi mogli obrađivati osim ako bi se utvrdila nova pravna osnova za nastavak obrade uzorka (npr. ispitanik je postao osumnjičenik). Dodatan primjer mogao bi se pojaviti kad policija istražuje kazneno djelo u kojem bi žrtvi (primjerice, žrtvi razbojništva, seksualnog kaznenog djela ili nasilja u obitelji ili rođacima žrtve ubojstva ili drugog kaznenog djela) moglo koristiti da je se uputi na organizaciju Victim Support – neovisnoj dobrotvornoj organizaciji koja se bavi pružanjem podrške osobama u vezi s kaznenim djelima i traumatičnim incidentima. U takvim će okolnostima policija s organizacijom Victim Support razmijeniti osobne informacije kao što su ime i kontaktni podaci samo ako ima privolu žrtve.

(37) U slučajevima u kojima je potrebna privola pojedinca ta privola mora biti nedvosmislena i mora uključivati jasnu potvrdnu radnju ([65]). Od policijskih snaga zahtijeva se da imaju obavijest o zaštiti osobnih podataka koja uključuje, među ostalim, potrebne informacije koje se odnose na ispravno korištenje privole. Osim toga, neke od njih objavljuju i dodatne materijale o načinu na koji se pridržavaju zakonodavstva o zaštiti podataka, među ostalim i o tome kako i kad koriste privolu kao pravnu osnovu za obradu ([66]).

2.4.1.3. Osjetljiva obrada

(38) Trebale bi postojati posebne zaštitne mjere ako se obrađuju „posebne kategorije" podataka. U tom pogledu, slično onomu što je predviđeno u članku 10. Direktive (EU) 2016/680, u dijelu 3. DPA-a iz 2018. predviđaju se strože zaštitne mjere za takozvanu „osjetljivu obradu" ([67]).

(39) Prema članku 35. stavku 3. DPA-a iz 1998. nadležna tijela mogu obrađivati osjetljive podatke u svrhe kaznenog progona samo u dvama slučajevima: 1. ispitanik je dao privolu za obradu u svrhu kaznenog progona te u trenutku obavljanja obrade voditelj obrade ima dokument o odgovarajućoj politici ([68]); ili 2. obrada je nužna u svrhu kaznenog progona, obrada ispunjava barem jedan od uvjeta iz Priloga 8. DPA-u iz 2018. te u trenutku obavljanja obrade voditelj obrade ima dokument o odgovarajućoj politici ([69]).

(40) Kad je riječ o prvom slučaju, i kako je objašnjeno u uvodnoj izjavi 38., oslanjanje na privolu ne smatra se relevantnim u vrsti situacije prijenosa koja je predmet ove Odluke ([70]).

(41) Ako se obrada osjetljivih podataka ne oslanja na privolu, može se obavljati primjenom jednog od uvjeta navedenih u Prilogu 8. DPA-u iz 2018. Ti se uvjeti odnose na obradu koja je nužna u zakonske svrhe; u svrhe vođenja pravosudnih postupaka, zaštite vitalnih interesa ispitanika ili drugog pojedinca, zaštite djece i pojedinaca u opasnosti, pravnih zahtjeva, sudskih akata, sprečavanja prijevara, arhiviranja; ili ako se obrada odnosi na osobne podatke za koje je očito da ih je objavio ispitanik. Osim u slučaju kad je očito da su podaci javno objavljeni, svi uvjeti iz Priloga 8. podliježu provjeri „nužnosti". Kako je pojasnio ICO, „u ovom kontekstu ‚nužno' znači da se

([65]) Ne postoji zasebna definicija pojma „privola" u svrhe obrade osobnih podataka na temelju dijela 3. DPA-a iz 2018. ICO je izdao smjernice o pojmu „privola" na temelju dijela 3. DPA-a iz 2018., u kojima se pojašnjava da taj pojam ima isto značenje i trebao bi biti usklađen s definicijom navedenom u Općoj uredbi o zaštiti podataka, a ponajprije to da „privola mora biti dobrovoljna, posebna i informirana i mora postojati istinski izbor pri pristajanju na obradu podataka" (Vodič za obradu podataka u svrhe kaznenog progona, „O čemu je riječ u prvom načelu?" (vidjeti bilješku 64.) i Vodič za zaštitu podataka (u dijelu o privoli, koji je dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/)).

([66]) Vidjeti, primjerice, informacije na internetskim stranicama policije grofovije Lincolnshire (vidjeti: https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) ili na internetskim stranicama policije grofovije Zapadni Yorkshire (vidjeti: https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Članak 35. stavak 8. DPA-a iz 2018.

([68]) Članak 35. stavak 4. DPA-a iz 2018.

([69]) Članak 35. stavak 5. DPA-a iz 2018.

([70]) Radi potpunosti treba napomenuti da se privola, ako se obrada temelji na njoj, mora dati dobrovoljno, posebno i informirano te mora postojati poseban izbor pri pristajanju na obradu podataka. Osim toga, zahtijeva se da voditelj obrade, kad obavlja obradu na temelju privole ispitanika, ima „dokument o odgovarajućoj politici". U članku 42. DPA-a iz 2018. navode se zahtjevi koje dokument o odgovarajućoj politici mora ispunjavati. Pojašnjava se da se u tom dokumentu moraju, u najmanjoj mjeri, objasniti postupci voditelja obrade za osiguravanje usklađenosti s načelima zaštite podataka i objasniti politike voditelja obrade u pogledu zadržavanja i brisanja osobnih podataka. Prema članku 42. DPA-a iz 2018., to znači da voditelj obrade mora izraditi dokument u kojem se: (a) objašnjavaju postupci voditelja obrade za osiguravanje usklađenosti s načelima zaštite podataka; i (b) objašnjavaju politike voditelja obrade u pogledu zadržavanja i brisanja osobnih podataka koji se obrađuju oslanjanjem na privolu ispitanika ili se daje naznaka o razdoblju u kojem će se ti osobni podaci vjerojatno čuvati. Posebno se zahtijeva da voditelj obrade, poštujući svoju dužnost evidentiranja aktivnosti obrade, uvijek u dokument o politici uključi elemente navedene u točkama (a) i (b). ICO je objavio predložak dokumenta (Vodič za obradu podataka u svrhe kaznenog progona, „Uvjeti za osjetljivu obradu", dostupno na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) i može poduzeti provedbene mjere ako voditelji obrade ne ispune te zahtjeve. Dokument o odgovarajućoj politici pregledavaju i sudovi pri razmatranju mogućih kršenja DPA-a iz 2018. Na primjer, u nedavnom predmetu *R (Bridges) protiv Chief Constable of South Wales Police* sudovi su pregledali dokument o odgovarajućoj politici voditelja obrade i utvrdili da je primjeren, ali da bi bilo korisno kad bi bio podrobniji. Slijedom toga, policija južnog Walesa revidirala je dokument o odgovarajućoj politici i ažurirala ga u skladu s novim smjernicama ICO-a (vidjeti bilješku 33.). Nadalje, u skladu s člankom 42. stavkom 3. DPA-a iz 2018. voditelj obrade bi trebao redovito revidirati dokument o odgovarajućoj politici. Naposljetku, kao dodatna zaštitna mjera, u skladu s člankom 42. stavkom 4. DPA-a iz 2018., od voditelja obrade zahtijeva se da vodi proširenu evidenciju aktivnosti obrade, u koju su uključeni dodatni elementi u odnosu na opću obvezu voditelja obrade o vođenju evidencije o aktivnostima obrade, koja je utvrđena u članku 61. DPA-a iz 2018.

obrada mora odnositi na nužnu društvenu potrebu koja se ne može relativno lako ostvariti manje nametljivim sredstvima” ([71]). Nadalje, neki od tih uvjeta podliježu dodatnim ograničenjima. Na primjer, za oslanjanje na uvjet koji se odnosi na „zakonske svrhe” i uvjet koji se odnosi na „zaštitu” (točke 1. i 4. Priloga 8.) potrebno je dodatno provjeriti postoji li značajan javni interes. Nadalje, s obzirom na uvjete koji se odnose na zaštitu djece (točka 4. Priloga 8.) ispitanik mora ujedno biti odgovarajuće dobi i mora se smatrati da je u opasnosti. Nadalje, voditelj obrade može primijeniti uvjet iz točke 4. Priloga 8. samo u slučaju posebnih okolnosti ([72]). Slično tomu, postoje ograničenja i u pogledu uvjeta koji se odnose na „sudske akte” i „sprečavanje prijevara” (točka 7. odnosno točka 8. Priloga 8.). Oba se uvjeta primjenjuju samo na određene voditelje obrade. U slučaju sudskih akata taj uvjet može primjenjivati samo sud ili drugo pravosudno tijelo, dok u slučaju sprečavanja prijevara taj uvjet mogu primjenjivati samo voditelji obrade koji su organizacije za suzbijanje prijevara.

(42) Naposljetku, ako se obrada oslanja na jedan od uvjeta navedenih u Prilogu 8., u skladu s povezanim člankom 42. DPA-a iz 2018., mora postojati „dokument o odgovarajućoj politici” (u kojem se objašnjavaju postupci voditelja obrade za osiguravanje usklađenosti s načelima zaštite podataka i politike voditelja obrade u pogledu zadržavanja i brisanja osobnih podataka) te se primjenjuje obveza vođenja proširene evidencije.

2.4.2. *Ograničavanje svrhe*

(43) Osobni podaci trebali bi se obrađivati u određenu svrhu i zatim se upotrebljavati samo ako to nije nespojivo sa svrhom obrade. To načelo zaštite podataka zajamčeno je člankom 36. DPA-a iz 2018. Tom se odredbom, slično članku 4. stavku 1. točki (b) Direktive (EU) 2016/680, zahtijeva: (a) da svrha kaznenog progona u koju se osobni podaci prikupljaju mora u svakom slučaju biti posebna, izričita i zakonita; i (b) da se tako prikupljeni osobni podaci ne smiju obrađivati na način koji je nespojiv sa svrhom u koju su prikupljeni.

(44) Ako nadležna tijela obrađuju podatke u svrhu kaznenog progona, to može uključivati svrhe arhiviranja, svrhe znanstvenog ili povijesnog istraživanja i statističke svrhe ([73]). U tim se slučajevima u DPA-u iz 2018. pojašnjava i to da arhiviranje (ili obrada u svrhe znanstvenog ili povijesnog istraživanja i statističke svrhe) nije dopušteno ako se obavlja u pogledu odluka donesenih u odnosu na određenog ispitanika ili ako će se ispitaniku time vjerojatno prouzročiti znatna šteta ili duševna bol ([74]).

2.4.3. *Točnost i smanjenje količine podataka*

(45) Podaci moraju biti točni i, prema potrebi, ažurirani. Osim toga, moraju biti primjereni i relevantni te ne smiju biti pretjerani u odnosu na svrhe u koje se obrađuju. Slično članku 4. stavku 1. točkama (c), (d) i (e) Direktive (EU) 2016/680, ta su načela osigurana u člancima 37. i 38. DPA-a iz 2018. Moraju se poduzeti sve opravdane mjere kako bi se osiguralo da se osobni podaci koji su netočni ([75]) bez odgode izbrišu ili

([71]) Vodič za obradu podataka u svrhe kaznenog progona, „Uvjeti za osjetljivu obradu” (vidjeti bilješku 70.).

([72]) Obrada se obavlja bez privole ispitanika: (a) ako ispitanik ne može dati privolu za obradu; (b) ako se od voditelja obrade ne može opravdano očekivati da pribavi privolu ispitanika za obradu; (c) ako se obrada mora obaviti bez privole ispitanika zbog toga što bi se pribavljanjem privole ispitanika dovelo u pitanje pružanje zaštite navedene u podtočki 1. podpodtočki (a).

([73]) Vidjeti članak 41. stavak 1. DPA-a iz 2018.

([74]) Vidjeti članak 41. stavak 2. DPA-a iz 2018.

([75]) U članku 205. DPA-a iz 2018. pojam „netočni” osobni podaci definira se kao „pogrešni ili zavaravajući” osobni podaci. Tijela Ujedinjene Kraljevine objasnila su da je uobičajeno da su podaci povezani s kaznenim istragama često nepotpuni, no unatoč tomu oni mogu biti točni.

isprave ([76]), vodeći računa o svrsi kaznenog progona u koju se obrađuju ([77]), i kako bi se osiguralo da se osobni podaci koji su netočni, nepotpuni ili više nisu ažurni ne prenose niti stavljaju na raspolaganje u bilo koju od svrha kaznenog progona ([78]).

(46) Nadalje, slično članku 7. Direktive (EU) 2016/680, u okviru režima zaštite podataka Ujedinjene Kraljevine propisuje se da se osobni podaci utemeljeni na činjenicama moraju, u mjeri u kojoj je to moguće, razlikovati od osobnih podataka utemeljenih na osobnim procjenama ([79]). Tamo gdje je to relevantno i u mjeri u kojoj je to moguće mora se napraviti jasna razlika između osobnih podataka koji se odnose na različite kategorije ispitanika, kao što su osumnjičenici, osobe osuđene za kaznena djela, žrtve kaznenih djela i svjedoci ([80]).

2.4.4. *Ograničenje pohrane*

(47) U skladu s člankom 5. Direktive (EU) 2016/680 podaci bi se načelno trebali čuvati samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju. U skladu s člankom 39. DPA-a iz 2018. i slično članku 5. te direktive zabranjeno je osobne podatke koji su obrađivani u bilo koju od svrha kaznenog progona čuvati dulje od vremena koje je potrebno s obzirom na svrhu u koju se obrađuju. U okviru pravnog režima Ujedinjene Kraljevine zahtijeva se da se moraju utvrditi odgovarajući rokovi za periodično preispitivanje potrebe za daljnjom pohranom osobnih podataka u bilo koju od svrha kaznenog progona. Dodatna pravila o praksama koje se odnose na zadržavanje osobnih podataka i odgovarajućim vremenskim rokovima utvrđena su u relevantnom zakonodavstvu i smjernicama kojima se uređuju ovlasti i djelovanje policije. Na primjer, u Engleskoj i Walesu u Kodeksu prakse za upravljanje policijskim informacijama Nacionalne agencije za policiju, zajedno sa Smjernicama o odobrenoj profesionalnoj praksi za upravljanje policijskim informacijama, daje se okvir za upravljanje operativnim policijskim informacijama radi osiguravanja usklađenog postupka zadržavanja, preispitivanja i brisanja podataka koji se temelji na procjeni rizika ([81]). U tom se okviru jasno utvrđuju očekivanja na razini cijele službe u pogledu načina na koji bi se unutar pojedinih policijskih službi i drugih tijela te među njima informacije trebale stvarati, razmjenjivati i koristiti te načina na koji bi njima trebalo upravljati ([82]). Od policije se očekuje da poštuje Kodeks prakse, a poštovanje tog kodeksa provjerava Inspektorat za policiju te vatrogasne i spasilačke službe u Engleskoj i Walesu (*Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services*) ([83]).

(48) Od Policijske službe Sjeverne Irske (PSNI) zakonom se ne zahtijeva da poštuje Kodeks prakse za upravljanje policijskim informacijama. Međutim, okvir za upravljanje policijskim informacijama koji je donesen 2011. dopunjen je Priručnikom Policijske službe Sjeverne Irske ([84]), u kojem se utvrđuju politike i postupci o načinu primjene Kodeksa prakse za upravljanje policijskim informacijama u Sjevernoj Irskoj.

([76]) Članak 38. stavak 1. točka (b) DPA-a iz 2018.

([77]) Prema Okviru za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, „time se osigurava da se u obzir uzimaju i prava ispitanika i operativne potrebe tijela kaznenog progona. Prethodna je točka pažljivo razmotrena u fazama izrade nacrta Prijedloga zakona o zaštiti podataka, s obzirom na to da mogu postojati posebni i ograničeni operativni razlozi zbog kojih se podaci ne mogu ispraviti. To će se najčešće događati u slučajevima kad se predmetni netočni osobni podaci moraju sačuvati u izvornom obliku u dokazne svrhe" (vidjeti Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak F: Kazneni progon, str. 21., vidjeti bilješku 9.).

([78]) Članak 38. stavak 4. DPA-a iz 2018. Nadalje, u skladu s člankom 38. stavkom 5. DPA-a iz 2018. kvalitetu osobnih podataka mora se provjeriti prije prenošenja ili stavljanja na raspolaganje; u sve prijenose osobnih podataka moraju se uključiti potrebne informacije koje primatelju omogućuju da procijeni stupanj točnosti, potpunosti i pouzdanosti podataka i mjeru u kojoj su ažurirani; te, ako se nakon prijenosa osobnih podataka pokaže da su podaci bili netočni ili da je prijenos bio nezakonit, primatelja se mora bez odgode obavijestiti o tome.

([79]) Članak 38. stavak 2. DPA-a iz 2018.

([80]) Članak 38. stavak 3. DPA-a iz 2018.

([81]) Tim se okvirom osigurava usklađenost u primjeni pohrane prikupljenih osobnih podataka. Rokovi za preispitivanje ovise o kaznenim djelima, koja su podijeljena u četiri skupine: 1. određena pitanja zaštite javnosti; 2. druga seksualna nasilna i teška kaznena djela; 3. sva ostala kaznena djela; i 4. razno. Dodatne pojedinosti nalaze se u Smjernicama o odobrenoj profesionalnoj praksi za upravljanje policijskim informacijama (vidjeti bilješku 26.).

([82]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, ostale organizacije, ako žele, mogu se slobodno pridržavati načela Kodeksa prakse za upravljanje policijskim informacijama te su, primjerice, Porezna i carinska uprava Ujedinjene Kraljevine i Nacionalna agencija za kriminalitet dobrovoljno prihvatile mnoga načela iz Kodeksa prakse za upravljanje policijskim informacijama kako bi osigurale usklađenost na razini cijelog sustava kaznenog progona. Općenito, većina organizacija za svoje će osoblje donijeti posebne politike i smjernice za cjelokupno osoblje, prilagođene konkretnoj organizaciji, o načinu postupanja s osobnim podacima u okviru njihovih zadaća. To će obično uključivati i obvezno osposobljavanje.

([83]) Kodeks prakse za upravljanje policijskim informacijama donesen je korištenjem ovlasti predviđenih u Zakonu o policiji iz 1996., koje Nacionalnoj agenciji za policiju omogućuju da izdaje kodekse prakse koji se odnose na djelotvorno funkcioniranje policijske djelatnosti. Svaki kodeks prakse donesen na temelju tog zakona mora dobiti odobrenje ministra te podliježe obvezi savjetovanja s Nacionalnom agencijom za kriminalitet prije njegova upućivanja Parlamentu. U članku 39.A stavku 7. Zakona o policiji iz 1996. zahtijeva se da policija propisno uzima u obzir kodekse donesene na temelju tog zakona.

([84]) Priručnik Policijske službe Sjeverne Irske za upravljanje policijskim informacijama, poglavlja 1.–6.

(49) Policijske snage u Škotskoj oslanjaju se na standardni operativni postupak za zadržavanje evidencije ([85]), kojim se podupire politika upravljanja evidencijom ([86]) Policijske službe Škotske. U okviru standardnog operativnog postupka utvrđuju se posebna pravila za zadržavanje evidencije koju drži škotska policija.

(50) Osim sveobuhvatnog glavnog zahtjeva o preispitivanju evidencija koji se primjenjuje u cijeloj Ujedinjenoj Kraljevini, dodatne pojedinosti predviđene su u lokaliziranim pravilima. U nastavku se navodi nekoliko primjera tih pravila: kad je riječ o Engleskoj i Walesu, u Zakonu o policiji i kaznenim dokazima, kako je izmijenjen Zakonom o zaštiti sloboda iz 2012., utvrđuju se odredbe o zadržavanju otisaka prstiju i profila DNK-a te poseban režim za neosuđene pojedince ([87]). Zakonom o zaštiti sloboda uspostavljen je položaj povjerenika za zadržavanje i korištenje biometrijskog materijala („povjerenik za biometrijske podatke") ([88]). Posebna pravila o fotografijama lica pritvorenika utvrđena su u okviru preispitivanja korištenja i čuvanja fotografija lica zatvorenika iz 2017. ([89]) Kad je riječ o Škotskoj, u Zakonu o kaznenom postupku za Škotsku iz 1995. predviđaju se pravila za uzimanje i zadržavanje otisaka prstiju i bioloških uzoraka ([90]). Kao i u slučaju Engleske i Walesa, zakonodavstvom se uređuje zadržavanje biometrijskih podataka u različitim slučajevima ([91]).

2.4.5. *Sigurnost podataka*

(51) Osobni podaci moraju se obrađivati tako da se jamči njihova sigurnost, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja. U tu svrhu tijela javne vlasti trebaju poduzeti odgovarajuće tehničke ili organizacijske mjere za zaštitu osobnih podataka od mogućih prijetnji. Te mjere moraju se procijeniti tako da se uzmu u obzir najnovija dostignuća i povezani troškovi.

(52) Ta se načela odražavaju u članku 40. DPA-a iz 2018. prema kojem, slično članku 4. stavku 1. točki (f) Direktive (EU) 2016/680, osobni podaci koji se obrađuju u bilo koju od svrha kaznenog progona moraju se obrađivati na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, primjenom odgovarajućih tehničkih ili organizacijskih mjera. To uključuje zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili

([85]) Standardni operativni postupak za zadržavanje evidencije, dostupan na: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Za dodatne pojedinosti o upravljanju evidencijom vidjeti informacije koje se odnose na Nacionalne evidencije Škotske, dostupne na: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Rokovi zadržavanja razlikuju se ovisno o tome je li pojedinac osuđen (članci od 63.I do 63.KI PACE-a iz 1984.). Na primjer, u slučaju odrasle osobe osuđene za kazneno djelo o kojem se vodi evidencija, njezini otisci prstiju i profil DNK-a mogu se zadržati na neodređeno vrijeme (članak 63.I stavak 2. PACE-a iz 1984.), dok je zadržavanje vremenski ograničeno u slučaju da je osuđena osoba mlađa od 18 godina, ako je riječ o „lakšem" kaznenom djelu o kojem se vodi evidencija i ako ta osoba nije prethodno osuđivana (članak 63.K PACE-a iz 1984.). Zadržavanje u slučaju osobe koja je uhićena ili optužena, ali nije osuđena, ograničeno je na razdoblje od tri godine (članak 63.F PACE-a iz 1984.). Produljenje tog roka zadržavanja mora odobriti sudsko tijelo (članak 63.F stavak 7. PACE-a iz 1984.). U slučaju osobe koja je uhićena ili optužena za lakše kazneno djelo, ali nije osuđena, čuvanje nije moguće (članak 63.D i članak 63.H PACE-a iz 1984.).

([88]) Člankom 20. Zakona o zaštiti sloboda iz 2012. uspostavlja se položaj povjerenika za biometrijske podatke. Među ostalim funkcijama, povjerenik za biometrijske podatke odlučuje o tome može li policija čuvati evidencije o profilima DNK-a i otiske prstiju prikupljene od pojedinaca koji su uhićeni, ali nisu optuženi za teže kazneno djelo (članak 63.G PACE-a iz 1984.). Nadalje, povjerenik za biometrijske podatke ima opću dužnost da preispituje zadržavanje i korištenje DNK-a i otisaka prstiju te zadržavanje zbog razloga nacionalne sigurnosti (članak 20. stavak 2. Zakona o zaštiti sloboda iz 2012.). Povjerenik za biometrijske podatke imenuje se u skladu s Kodeksom za javna imenovanja (Kodeks je dostupan na: Kodeks upravljanja za javna imenovanja – GOV.UK (www.gov.uk)) te je iz njegovih uvjeta imenovanja jasno da ga smijeniti može jedino ministar unutarnjih poslova, i to samo u vrlo usko utvrđenim okolnostima, a to su, među ostalim, nemogućnost povjerenika da obavlja svoje dužnosti u razdoblju od tri mjeseca, osuda za kazneno djelo ili nepridržavanje uvjeta svojeg imenovanja.

([89]) Preispitivanje korištenja i zadržavanja fotografija lica zatvorenika, dostupno na: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Članak 18. i dalje Zakona o kaznenom postupku za Škotsku iz 1995.

([91]) Rokovi zadržavanja mogu se razlikovati ovisno o tome je li osoba osuđena (članak 18. stavak 3. Zakona o kaznenom postupku za Škotsku iz 1995.) ili ovisno o tome je li osoba maloljetna. U slučaju da je riječ o maloljetnoj osobi, rok zadržavanja je tri godine od osude na saslušanju za djecu (*children's hearing*) (članak 18.E stavak 8. Zakona o kaznenom postupku za Škotsku iz 1995.). Podaci uhićenih osoba koje nisu osuđene ne mogu se čuvati (članak 18. stavak 3. Zakona o kaznenom postupku za Škotsku iz 1995.) osim u posebnim slučajevima i ovisno o težini kaznenog djela (članak 18.A Zakona o kaznenom postupku za Škotsku iz 1995.). Zakonom o škotskom povjereniku za biometrijske podatke iz 2020. (vidjeti https://www.legislation.gov.uk/asp/2020/8/contents) uspostavlja se položaj škotskog povjerenika za biometrijske podatke čija je zadaća sastavljanje i revidiranje kodeksa prakse (koje odobrava Škotski parlament) o prikupljanju, zadržavanju, korištenju i uništavanju biometrijskih podataka za potrebe kaznenog pravosuđa i policije (članak 7. Zakona o škotskom povjereniku za biometrijske podatke iz 2020.).

oštećenja ([92]). U članku 66. DPA-a iz 2018. dodatno se navodi da svaki voditelj obrade i svaki izvršitelj obrade moraju provesti odgovarajuće tehničke i organizacijske mjere kako bi osigurali razinu sigurnosti koja je primjerena rizicima koji proizlaze iz obrade osobnih podataka. Prema Objašnjenjima voditelj obrade mora procijeniti rizike i na temelju te procjene provesti odgovarajuće sigurnosne mjere, primjerice, enkripciju ili posebne razine sigurnosnog odobrenja za osoblje koje obrađuje podatke ([93]). U procjeni se mora uzeti u obzir i, primjerice, prirodu podataka koji se obrađuju i sve ostale relevantne čimbenike ili okolnosti koji bi mogli utjecati na sigurnost obrade.

(53) Režim kojim se uređuje usklađenost s načelima zaštite podataka vrlo je sličan režimu uspostavljenom člancima od 29. do 31. Direktive (EU) 2016/680. Konkretno, u slučaju povrede osobnih podataka koja se odnosi na osobne podatke za koje je voditelj obrade odgovoran, prema članku 67. stavku 1. DPA-a iz 2018., voditelj obrade mora, bez nepotrebne odgode, i ako je izvedivo, u roku od 72 sata od saznanja za tu povredu izvijestiti povjerenika za informiranje o povredi osobnih podataka ([94]). Obveza izvješćivanja ne primjenjuje se ako povreda osobnih podataka vjerojatno neće rezultirati rizikom za prava i slobode pojedinaca ([95]). Voditelj obrade mora dokumentirati činjenice povezane s bilo kojom povredom osobnih podataka, njezine posljedice i poduzete korektivne mjere tako da se povjereniku za informiranje omogući provjera poštovanja DPA-a ([96]). Ako izvršitelj obrade sazna da je došlo do povrede sigurnosti, mora bez nepotrebne odgode o tome izvijestiti voditelja obrade ([97]).

(54) Prema članku 68. stavku 1. DPA-a iz 2018., ako je vjerojatno da će povreda osobnih podataka prouzročiti visok rizik za prava i slobode pojedinaca, voditelj obrade mora bez nepotrebne odgode obavijestiti ispitanika o toj povredi ([98]). Obavijest mora uključivati iste informacije kao i obavijest povjereniku za informiranje opisana u uvodnoj izjavi (53). Ta se obveza ne primjenjuje ako je voditelj obrade proveo odgovarajuće tehničke i organizacijske mjere zaštite koje su primijenjene na osobne podatke pogođene povredom. Ne primjenjuje se ni ako je voditelj obrade poduzeo naknadne mjere kojima se osigurava da pojava visokog rizika za prava i slobode ispitanika više nije vjerojatna. Naposljetku, od voditelja obrade ne zahtijeva se da obavijesti ispitanika ako bi to uključivalo nerazmjeran napor ([99]). U tom se slučaju ispitanika mora obavijestiti na drugi podjednako djelotvoran način, primjerice, javnim obavješćivanjem ([100]). Ako voditelj obrade nije obavijestio ispitanika o povredi, povjerenik za informiranje, nakon što ga je voditelj obrade izvijestio u skladu s člankom 67. DPA-a i nakon što je razmotrio vjerojatnost da će povreda osobnih podataka rezultirati visokim rizikom, može zahtijevati od voditelja obrade da obavijesti ispitanika o povredi ([101]).

([92]) U skladu s Objašnjenjima DPA-a iz 2018. (vidjeti bilješku 45.) voditelj obrade mora, prije svega: osmisliti i organizirati sigurnost tako da odgovara prirodi osobnih podataka koje voditelj obrade drži i šteti koja bi mogla nastati uslijed povrede sigurnosti; jasno odrediti tko je u njegovoj organizaciji odgovoran za osiguravanje informacijske sigurnosti; pobrinuti se da raspolaže odgovarajućom fizičkom i tehničkom sigurnošću, koju podupiru čvrste politike i postupci te pouzdano i dobro osposobljeno osoblje; i biti spreman brzo i djelotvorno reagirati na svaku povredu sigurnosti.

([93]) Točka 221. Objašnjenja DPA-a iz 2018. (vidjeti bilješku 45.).

([94]) U članku 67. stavku 4. DPA-a iz 2018. propisuje se da to izvješćivanje mora uključivati opis prirode povrede osobnih podataka (uključujući, ako je moguće, kategorije i približan broj ispitanika zahvaćenih povredom te kategorije i približan broj evidencija osobnih podataka zahvaćenih povredom), ime i kontaktne podatke kontaktne točke, opis vjerojatnih posljedica povrede osobnih podataka i opis mjera koje je voditelj obrade poduzeo ili predložio da se poduzmu za rješavanje problema povrede osobnih podataka (uključujući, prema potrebi, mjere za ublažavanje njezinih mogućih štetnih posljedica).

([95]) Članak 67. stavak 2. DPA-a iz 2018.

([96]) Članak 67. stavak 6. DPA-a iz 2018.

([97]) Članak 67. stavak 9. DPA-a iz 2018.

([98]) Prema članku 68. stavku 7. DPA-a iz 2018. voditelj obrade može djelomično ili u potpunosti ograničiti pružanje informacija ispitaniku u onoj mjeri i u onom trajanju u kojem je to ograničavanje, vodeći računa o temeljnim pravima i legitimnim interesima ispitanika, nužna i proporcionalna mjera kako bi se: (a) izbjeglo ometanje službenih ili pravnih ispitivanja, istraga ili postupaka; (b) izbjeglo dovođenje u pitanje sprečavanja, otkrivanja, istrage ili progona kaznenih djela ili izvršavanja kaznenih sankcija; (c) zaštitila javna sigurnost; (d) zaštitila nacionalna sigurnost; (e) zaštitili prava i slobode drugih.

([99]) Članak 68. stavak 3. DPA-a iz 2018.

([100]) Članak 68. stavak 5. DPA-a iz 2018.

([101]) Članak 68. stavak 6. DPA-a iz 2018., podložno ograničenju predviđenom u članku 68. stavku 8. DPA-a iz 2018.

2.4.6. *Transparentnost*

(55) Ispitanike se mora obavijestiti o glavnim obilježjima obrade njihovih osobnih podataka. To načelo zaštite podataka odražava se u članku 44. DPA-a iz 2018. u kojem se, slično članku 13. Direktive (EU) 2016/680, propisuje da voditelj obrade ima opću dužnost da ispitanicima stavi na raspolaganje informacije o obradi njihovih osobnih podataka (bilo na način da te informacije učini općenito dostupnima javnosti bilo na neki drugi način) ([102]). Informacije za koje se zahtijeva da se stave na raspolaganje uključuju: (a) identitet i kontaktne podatke voditelja obrade; (b) ako je primjenjivo, kontaktne podatke službenika za zaštitu podataka; (c) svrhe u koje voditelj obrade obrađuje osobne podatke; (d) postojanje prava ispitanika da od voditelja obrade zatraži pristup osobnim podacima, ispravak osobnih podataka i brisanje osobnih podataka ili ograničavanje njihove obrade; i (e) pravo na podnošenje pritužbe povjereniku za informiranje i kontaktne podatke povjerenika ([103]).

(56) Osim toga, voditelj obrade mora u posebnim slučajevima u svrhu omogućivanja ostvarivanja prava ispitanika na temelju DPA-a iz 2018. (primjerice, ako su osobni podaci koji se obrađuju prikupljeni bez znanja ispitanika) ispitaniku dati: (a) informacije o pravnoj osnovi za obradu; (b) informacije o razdoblju u kojem će osobni podaci biti pohranjeni ili, ako to nije moguće, o kriterijima koji se primjenjuju za određivanje tog razdoblja; (c) ako je primjenjivo, informacije o kategorijama primatelja osobnih podataka (uključujući primatelje u trećim zemljama ili međunarodnim organizacijama); (d) dodatne informacije koje su potrebne kako bi se omogućilo ostvarivanje prava ispitanika na temelju dijela 3. DPA-a iz 2018. ([104])

2.4.7. *Prava pojedinaca*

(57) Ispitanicima se mora priznati niz provedivih prava. U dijelu 3. poglavlju 3. DPA-a iz 2018. predviđaju se prava pojedinaca na pristup podacima, ispravak podataka te brisanje podataka i ograničavanje obrade ([105]), koja su usporediva s pravima predviđenima u poglavlju III. Direktive (EU) 2016/680.

(58) Pravo na pristup podacima utvrđeno je u članku 45. DPA-a iz 2018. Kao prvo, pojedinac ima pravo dobiti potvrdu od voditelja obrade o tome obrađuju li se njegovi osobni podaci ([106]). Kao drugo, ako se osobni podaci obrađuju, ispitanik ima pravo na pristup tim podacima i dobivanje sljedećih informacija o obradi: (a) informacija o svrhama obrade i pravnim osnovama za obradu; (b) informacija o kategorijama predmetnih podataka; (c) informacija o primatelju kojem su ti podaci otkriveni; (d) informacija o razdoblju u kojem će ti osobni podaci biti pohranjeni; (e) informacija o postojanju prava ispitanika na ispravak i brisanje osobnih podataka; (f) informacija o pravu na podnošenje pritužbe; i (g) svih informacija o izvoru predmetnih osobnih podataka ([107]).

(59) U skladu s člankom 46. DPA-a iz 2018. ispitanik ima pravo da od voditelja obrade zatraži ispravljanje netočnih osobnih podataka koji se odnose na njega. Voditelj obrade mora bez nepotrebne odgode ispraviti te podatke (ili ih dopuniti ako su podaci netočni zbog nepotpunosti). Ako se ti osobni podaci moraju sačuvati kao dokaz, voditelj obrade mora (umjesto ispravljanja osobnih podataka) ograničiti njihovu obradu ([108]).

([102]) U Vodiču za obradu podataka u svrhe kaznenog progona navodi se sljedeći primjer: „Na svojim internetskim stranicama imate opću obavijest o zaštiti osobnih podataka koja obuhvaća osnovne informacije o organizaciji, svrhu u koju obrađujete osobne podatke, prava ispitanika i njihovo pravo na pritužbu povjereniku za informiranje. Primili ste obavijest o tome da je određeni pojedinac bio prisutan pri počinjenju kaznenog djela. Pri prvom razgovoru s tim pojedincem morate mu dati opće informacije, kao i dodatne popratne informacije, kako biste mu omogućili ostvarivanje njegovih prava. Davanje informacija o poštenoj obradi možete ograničiti samo ako će to štetno utjecati na istragu koju provodite" (Vodič za obradu podataka u svrhe kaznenog progona, „Koje bismo informacije trebali dati pojedincu?", dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) U Vodiču za obradu podataka u svrhe kaznenog progona navodi se da informacije koje se daju o obradi osobnih podataka moraju biti jezgrovite, razumljive i lako dostupne; pisane jasnim i jednostavnim jezikom, koji je prilagođen potrebama osjetljivih osoba, kao što su djeca; i moraju se davati bez naknade (Vodič za obradu podataka u svrhe kaznenog progona, „Kako bismo trebali davati te informacije?", dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Članak 44. stavak 2. DPA-a iz 2018.

([105]) Za detaljnu analizu prava ispitanika vidjeti: Vodič za obradu podataka u svrhe kaznenog progona (u dijelu o pravima pojedinaca, koji je dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/).

([106]) Članak 45. stavak 1. DPA-a iz 2018.

([107]) Članak 45. stavak 2. DPA-a iz 2018.

([108]) Članak 46. stavak 4. DPA-a iz 2018.

(60) U članku 47. DPA-a iz 2018. pojedincima se priznaje pravo na brisanje podataka i ograničavanje obrade. Voditelj obrade mora ([109]) izbrisati osobne podatke bez nepotrebne odgode ako bi se obradom osobnih podataka kršilo bilo koje od načela zaštite podataka, pravne osnove za obradu ili zaštitne mjere povezane s arhiviranjem i osjetljivom obradom. Voditelj obrade mora podatke izbrisati i ako ima pravnu obvezu da to učini. Ako se ti osobni podaci moraju sačuvati kao dokaz, voditelj obrade mora (umjesto brisanja osobnih podataka) ograničiti njihovu obradu ([110]). Voditelj obrade mora ograničiti obradu osobnih podataka ako ispitanik osporava točnost osobnih podataka, ali nije moguće utvrditi jesu li oni točni ili nisu ([111]).

(61) Ako ispitanik zatraži ispravak ili brisanje osobnih podataka ili ograničavanje njihove obrade, voditelj obrade mora pisanim putem obavijestiti ispitanika o tome je li taj zahtjev odobren, a ako je odbijen, obavijestiti ispitanika o razlozima za odbijanje i raspoloživim mogućnostima za pravnu zaštitu (pravo ispitanika da povjereniku za informiranje podnese zahtjev za istragu zakonitosti primjene ograničavanja, pravo na podnošenje pritužbe povjereniku za informiranje i pravo na obraćanje sudu radi izdavanja naloga za udovoljavanje zahtjevu) ([112]).

(62) Ako voditelj obrade ispravi osobne podatke primljene od drugog nadležnog tijela, mora o tome obavijestiti to drugo tijelo ([113]). Ako voditelj obrade ispravi ili izbriše osobne podatke ili ograniči obradu osobnih podataka koje je voditelj obrade otkrio, voditelj obrade mora o tome obavijestiti primatelje, a ti primatelji moraju na sličan način ispraviti ili izbrisati te osobne podatke ili ograničiti njihovu obradu (u mjeri u kojoj su i dalje dužni to učiniti) ([114]).

(63) Nadalje, ispitanik ima pravo da ga voditelj obrade bez nepotrebne odgode obavijesti o povredi osobnih podataka kad je vjerojatno da će ta povreda rezultirati visokim rizikom za prava i slobode pojedinaca ([115]).

(64) U odnosu na sva ta prava ispitanika i slično onomu što je predviđeno u članku 12. Direktive (EU) 2016/680, voditelj obrade obvezan je osigurati da se sve informacije ispitaniku pružaju u jezgrovitom, razumljivom i lako dostupnom obliku ([116]) te bi se, ako je moguće, trebale pružati u istom obliku u kojem je zahtjev ([117]). Voditelj obrade mora udovoljiti zahtjevu ispitanika bez nepotrebne odgode ili u svakom slučaju, načelno, prije isteka roka od mjesec dana od podnošenja zahtjeva ([118]). Ako voditelj obrade ima opravdane sumnje u pogledu identiteta pojedinca, može zatražiti dodatne informacije i odgoditi postupanje po zahtjevu dok se ne utvrdi identitet pojedinca. Voditelj obrade može zatražiti plaćanje razumne naknade ili odbiti postupiti po zahtjevu ako smatra da je zahtjev očito neutemeljen ([119]). ICO je izdao smjernice o tome kad se zahtjev smatra očito neutemeljenim ili pretjeranim i kad se može zatražiti plaćanje naknade ([120]).

(65) Nadalje, na temelju članka 53. stavka 4. DPA-a iz 2018. ministar može uredbom odrediti najviši iznos naknade.

([109]) Ispitanik može zatražiti od voditelja obrade da izbriše osobne podatke ili ograniči njihovu obradu (ali se dužnosti voditelja obrade da izbriše podatke ili ograniči njihovu obradu primjenjuju bez obzira na to je li takav zahtjev podnesen).
([110]) Članak 46. stavak 4. i članak 47. stavak 2. DPA-a iz 2018.
([111]) Članak 47. stavak 3. DPA-a iz 2018.
([112]) Članak 48. stavak 1. DPA-a iz 2018.
([113]) Članak 48. stavak 7. DPA-a iz 2018.
([114]) Članak 48. stavak 9. DPA-a iz 2018.
([115]) Članak 68. DPA-a iz 2018.
([116]) Članak 52. stavak 1. DPA-a iz 2018.
([117]) Članak 52. stavak 3. DPA-a iz 2018.
([118]) U članku 54. DPA-a iz 2018. definira se značenje pojma „primjenjivo razdoblje”, koji znači razdoblje od mjesec dana ili dulje razdoblje koje se može propisati uredbom, a koje počinje od relevantnog trenutka (kad voditelj obrade zaprimi predmetni zahtjev; kad voditelj obrade zaprimi informacije koje je zatražio (ako ih je zatražio) u vezi sa zahtjevom na temelju članka 52. stavka 4. DPA-a; ili kad se plati naknada koja je naplaćena (ako je naplaćena) u vezi sa zahtjevom u skladu s člankom 53. DPA-a.
([119]) Članak 53. stavak 1. DPA-a iz 2018.
([120]) Prema smjernicama ICO-a voditelj obrade može odlučiti naplatiti naknadu ispitaniku ako je zahtjev ispitanika očito neutemeljen ili pretjeran, ali je voditelj obrade i dalje spreman odgovoriti na taj zahtjev. Naknada mora biti razumna i mora biti opravdana troškovima. Vodič za obradu podataka u svrhe kaznenog progona, „Očito neutemeljeni i pretjerani zahtjevi”, dostupno na: 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. Ograničenja pravâ ispitanika i obveze u pogledu transparentnosti

(66) Nadležno tijelo može u određenim okolnostima ograničiti određena prava ispitanika: pravo ispitanika na pristup podacima ([121]), pravo da bude informiran ([122]), pravo da sazna za povredu osobnih podataka ([123]) i pravo da ga se obavijesti o razlogu odbijanja zahtjeva za ispravak ili brisanje podataka ([124]). Slično režimu koji je predviđen u poglavlju III. Direktive (EU) 2016/680 nadležno tijelo može ograničenje primijeniti samo ako je to, uzimajući u obzir temeljna prava i legitimne interese ispitanika, nužno i proporcionalno kako bi se: (a) izbjeglo ometanje službenog ili pravnog ispitivanja, istrage ili postupka; (b) izbjeglo dovođenje u pitanje sprečavanja, otkrivanja, istrage ili progona kaznenih djela ili izvršavanja kaznenih sankcija; (c) zaštitila javna sigurnost; (d) zaštitila nacionalna sigurnost; (e) zaštitili prava i slobode drugih.

(67) ICO je izdao smjernice o primjeni tih ograničenja. Prema tim smjernicama voditelji obrade moraju provesti analizu na pojedinačnoj osnovi radi uspostavljanja ravnoteže između prava pojedinaca i štete koja bi nastala otkrivanjem. Točnije, moraju obrazložiti svako primijenjeno ograničenje kao nužno i proporcionalno te smiju ograničiti pružene informacije samo ako bi se njima dovele u pitanje prethodno navedene svrhe ([125]).

(68) Postoji i niz drugih smjernica koje su izdala nadležna tijela u kojima se daju detaljne informacije o svim aspektima zakonodavstva o zaštiti podataka, uključujući primjenu ograničenja prava ispitanika ([126]). Na primjer, u odnosu na članak 45. stavak 4. u Priručniku o zaštiti podataka Nacionalnog vijeća načelnika policije navodi se sljedeće: „Važno je imati na umu da se ograničenja mogu primjenjivati samo u mjeri u kojoj je to nužno i samo onoliko dugo koliko je to nužno. Stoga nisu dopuštene opća primjena ograničenja na sve osobne podatke određenog ispitanika ni trajna primjena ograničenja. Kad je riječ o potonjem, često je slučaj da se osobni podaci prikupljeni bez znanja ispitanika koji je osumnjičenik u istrazi moraju na početku zaštititi od otkrivanja tom ispitaniku, da bi se izbjeglo dovođenje u pitanje istrage dok je ona u tijeku, ali kasnije ne bi bilo nikakve štete od otkrivanja ako su osobni podaci otkriveni tom pojedincu za vrijeme razgovora. Policijske snage moraju uvesti postupke koji osiguravaju da se ta ograničenja primjenjuju samo u mjeri u kojoj je to potrebno i u trajanju koje je nužno” ([127]). U tim se smjernicama navode i primjeri situacija u kojima će se svako od ograničenja vjerojatno primjenjivati ([128]).

(69) Nadalje, u odnosu na mogućnost ograničavanja bilo kojeg od prethodno navedenih prava radi zaštite „nacionalne sigurnosti” voditelj obrade može podnijeti zahtjev za potvrdu koju potpisuje ministar koji je član kabineta ili glavni krunski odvjetnik (*Attorney General*) (ili glavni odvjetnik za Škotsku (*Advocate General for Scotland*)), a kojom se potvrđuje da je ograničenje tih prava nužna i proporcionalna mjera za zaštitu nacionalne sigurnosti ([129]). Vlada Ujedinjene Kraljevine izdala je smjernice o potvrdama o nacionalnoj sigurnosti na temelju DPA-a iz 2018. u kojima se ponajprije naglašava da svako ograničenje prava ispitanika radi zaštite nacionalne sigurnosti mora biti proporcionalno i nužno ([130]) (za više pojedinosti o potvrdama o nacionalnoj sigurnosti vidjeti uvodne izjave od (131). do (134).).

([121]) Članak 45. stavak 4. DPA-a iz 2018.
([122]) Članak 44. stavak 4. DPA-a iz 2018.
([123]) Članak 68. stavak 7. DPA-a iz 2018.
([124]) Članak 48. stavak 3. DPA-a iz 2018.
([125]) Vidjeti, primjerice, Vodič za obradu podataka u svrhe kaznenog progona (u dijelu o pravu na pristup podacima, koji je dostupan na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8).
([126]) Vidjeti, primjerice, Priručnik o zaštiti podataka za policijske stručnjake za zaštitu podataka koji je izdalo Nacionalno vijeće načelnika policije (vidjeti bilješku 27.) ili smjernice koje je izdao Ured za suzbijanje teških prijevara, dostupne na: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Priručnik o zaštiti podataka za policijske stručnjake za zaštitu podataka Nacionalnog vijeća načelnika policije, str. 140. (vidjeti bilješku 27.).
([128]) U Priručniku o zaštiti podataka Nacionalnog vijeća načelnika policije navodi se da će ograničenja u svrhu „izbjegavanja ometanja službenog ili pravnog ispitivanja, istrage ili postupka” vjerojatno biti relevantna za osobne podatke koji se obrađuju za potrebe istraga, postupaka na obiteljskim sudovima, istraga za potrebe nekaznenih unutarnjih stegovnih postupaka i istraga kao što su „Neovisna istraga o spolnom zlostavljanju djece” (*Independent Inquiry into Child Sexual Abuse*); dok su ograničenja u svrhu „zaštite prava i sloboda drugih” relevantna za osobne podatke koji bi se odnosili i na druge pojedince, a ne samo na podnositelja zahtjeva (Priručnik o zaštiti podataka Nacionalnog vijeća načelnika policije, str. 140., vidjeti bilješku 27.).
([129]) Članak 79. DPA-a iz 2018.
([130]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, dostupne na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Nadalje, ako se primjenjuje ograničenje prava ispitanika, nadležno tijelo mora obavijestiti ispitanika bez nepotrebne odgode o tome da su njegova prava ograničena, o razlozima za to ograničenje i o raspoloživim mogućnostima za pravnu zaštitu, osim ako bi pružanje tih informacija ugrozilo razlog za primjenu ograničenja ([131]). Kao dodatna zaštitna mjera protiv zloupotrebe ograničenja voditelj obrade mora evidentirati razloge za ograničenje informacija i na zahtjev staviti tu evidenciju na raspolaganje povjereniku za informiranje ([132]).

(71) Ako voditelj obrade odbije dati dodatne informacije o transparentnosti, ili pristup podacima, ili ako odbije zahtjev za ispravak ili brisanje podataka ili ograničavanje obrade, pojedinac može zatražiti od povjerenika za informiranje da istraži je li voditelj obrade ograničenje primijenio zakonito ([133]). Osim toga, predmetni pojedinac može podnijeti i pritužbu povjereniku za informiranje ili se obratiti sudu da izda nalog voditelju obrade za udovoljavanje zahtjevu ([134]).

2.4.7.2. Automatizirano donošenje odluka

(72) Članci 49. i 50. DPA-a iz 2018. obuhvaćaju prava povezana s automatiziranim donošenjem odluka odnosno zaštitnim mjerama koje treba primijeniti ([135]). Slično kao i u članku 11. Direktive (EU) 2016/680, voditelj obrade može donijeti značajnu odluku utemeljenu samo na automatiziranoj obradi osobnih podataka isključivo ako se to zahtijeva ili je odobreno pravom ([136]). Odluka je značajna ako bi dovela do negativnih pravnih posljedica za ispitanika ili bi na njega znatno utjecala ([137]).

(73) Ako se od voditelja obrade pravom zahtijeva ili ako mu je pravom dopušteno da donosi značajne odluke, u članku 50. DPA-a iz 2018. utvrđuju se zaštitne mjere koje će se primjenjivati na takvu odluku (koja se definira kao „kvalificirana značajna odluka"). Voditelj obrade mora, čim je to razumno izvedivo, obavijestiti ispitanika da je takva odluka donesena. Ispitanik potom može u roku od mjesec dana zatražiti od voditelja obrade da preispita tu odluku ili donese novu odluku koja se ne temelji samo na automatiziranoj obradi. Voditelj obrade mora razmotriti zahtjev i obavijestiti ispitanika o ishodu tog razmatranja. U DPA-u iz 2018. ministru se daje ovlast za donošenje uredbi za dodatne zaštitne mjere ([138]). Zasad nisu donesene takve uredbe.

2.4.8. *Daljnji prijenosi*

(74) Razina zaštite osobnih podataka koje tijelo kaznenog progona države članice prenosi tijelu kaznenog progona u Ujedinjenoj Kraljevini ne smije se ugroziti daljnjim prijenosom takvih podataka primateljima u trećoj zemlji. Takvi „daljnji prijenosi", koji su iz perspektive tijela kaznenog progona iz Ujedinjene Kraljevine međunarodni prijenosi iz Ujedinjene Kraljevine, trebali bi biti dopušteni samo ako daljnji primatelj izvan Ujedinjene Kraljevine i sam podliježe pravilima koja osiguravaju razinu zaštite sličnu onoj koja se jamči pravnim poretkom Ujedinjene Kraljevine.

([131]) Članak 44. stavci 5. i 6., članak 45. stavci 5. i 6. te članak 48. stavak 4. DPA-a iz 2018.
([132]) Članak 44. stavak 7., članak 45. stavak 7. i članak 48. stavak 6. DPA-a iz 2018.
([133]) Članak 51. DPA-a iz 2018.
([134]) Članak 167. DPA-a iz 2018.
([135]) Kad je riječ o opsegu automatizirane obrade, u Objašnjenjima DPA-a iz 2018. navodi se sljedeće: „te se odredbe odnose na potpuno automatizirano donošenje odluka, a ne na automatiziranu obradu. Automatizirana obrada (uključujući izradu profila) odnosi se na postupak koji se obavlja na podacima bez potrebe za ljudskom intervencijom. Redovito se koristi u kaznenom progonu radi filtriranja velikih skupova podataka na količine kojima se može upravljati kako bi ih potom koristio ljudski operator. Automatizirano donošenje odluka oblik je automatizirane obrade kod koje je potrebno da se konačna odluka donese bez ljudskog utjecaja". (Objašnjenja DPA-a, točka 204., vidjeti bilješku 45.).
([136]) Osim zaštite predviđene u DPA-u, u pravnom okviru Ujedinjene Kraljevine postoje i druga zakonodavna ograničenja koja se primjenjuju na tijela kaznenog progona i koja bi sprečavala automatiziranu obradu (uključujući izradu profila) čija bi posljedica bila nezakonita diskriminacija. Zakonom o ljudskim pravima iz 1998. prava iz EKLJP-a ugrađuju se u pravo Ujedinjene Kraljevine., uključujući pravo iz članka 14. Konvencije (zabrana diskriminacije). Slično tomu, Zakonom o ravnopravnosti iz 2010. zabranjuje se diskriminacija protiv osoba s osobinama koje se štite (što uključuje spol, rasu, invaliditet itd.).
([137]) Članak 49. stavak 2. DPA-a iz 2018.
([138]) Članak 50. stavak 4. DPA-a iz 2018.

(75) Režim Ujedinjene Kraljevine za međunarodne prijenose uređen je u dijelu 3. poglavlju 5. DPA-a iz 2018. ([139]) i u njemu se odražava pristup primijenjen u poglavlju V. Direktive (EU) 2016/680. Točnije, da bi se osobni podaci prenijeli u treću zemlju, nadležno tijelo mora ispuniti tri uvjeta: (a) prijenos mora biti nužan u svrhu kaznenog progona; (b) prijenos se mora temeljiti na: i. uredbi o primjerenosti koja se odnosi na tu treću zemlju; ii. ako se ne temelji na uredbi o primjerenosti, mora se temeljiti na postojanju odgovarajućih zaštitnih mjera; ili iii. ako se ne temelji na odluci o primjerenosti ni odgovarajućim zaštitnim mjerama, mora se temeljiti na posebnim okolnostima; i (c) primatelj prijenosa mora biti: i. relevantno tijelo (tj. ekvivalent nadležnom tijelu) u toj trećoj zemlji; ii. „relevantna međunarodna organizacija", npr. međunarodno tijelo koje obavlja funkcije koje odgovaraju bilo kojoj od svrha kaznenog progona; iii. osoba koja nije relevantno tijelo, ali samo ako je prijenos nužan za obavljanje jedne od svrha kaznenog progona; ako temeljna prava i slobode predmetnog ispitanika nemaju prednost nad javnim interesom koji iziskuje prijenos; ako bi prijenos osobnih podataka relevantnom tijelu u toj trećoj zemlji bio nedjelotvoran ili neprimjeren; i ako je primatelj obaviješten o svrhama u koje se ti podaci mogu obrađivati ([140]).

(76) Uredbe o primjerenosti koje se odnose na treću zemlju, područje ili sektor unutar treće zemlje, međunarodnu organizaciju ili opis ([141]) takve zemlje, područja, sektora ili organizacije donosi ministar. Kad je riječ o standardu koji treba zadovoljiti, ministar mora procijeniti osigurava li to područje/sektor/organizacija primjerenu razinu zaštite osobnih podataka. U članku 74.A stavku 4. DPA-a iz 2018. propisuje se da u tu svrhu ministar mora razmotriti niz elemenata koji odražavaju elemente navedene u članku 36. Direktive (EU) 2016/680 ([142]). S obzirom na to, od kraja prijelaznog razdoblja, dio 3. DPA-a iz 2018. čini „domaće zakonodavstvo koje proizlazi iz prava EU-a" koje će, kako je objašnjeno, sudovi Ujedinjene Kraljevine tumačiti u skladu s relevantnom sudskom praksom Suda koja je postojala prije izlaska Ujedinjene Kraljevine iz Unije i općim načelima prava Unije, u skladu s pravnim učinkom koji su ta praksa i načela imali neposredno prije kraja prijelaznog razdoblja. To uključuje standard prema kojem se procjenjuje je li zaštita „u osnovi istovjetna" i koji će se stoga primjenjivati na procjene primjerenosti koje provode tijela Ujedinjene Kraljevine.

(77) Na te se uredbe primjenjuju „opći" postupovni zahtjevi predviđeni u članku 182. DPA-a iz 2018. U okviru tog postupka ministar se mora savjetovati s povjerenikom za informiranje kad predlaže donošenje buduće uredbe o

([139]) Taj novi okvir postao je primjenjiv na kraju prijelaznog razdoblja, uključujući ovlast ministra za donošenje uredbi o primjerenosti. Međutim, u Uredbi DPPEC (točnije, u točkama od 10. do 12. Priloga 21. koje se tom uredbom umeću u DPA-u iz 2018.) predviđa se da se na kraju prijelaznog razdoblja i nakon njega s određenim prijenosima osobnih podataka postupa kao da se temelje na uredbi o primjerenosti. Ti prijenosi uključuju prijenose u treće zemlje na koje se na kraju prijelaznog razdoblja primjenjivala odluka o primjerenosti EU-a te u države članice EU-a, države EFTA-e i područje Gibraltara na temelju njihove primjene Direktive o zaštiti podataka u svrhe kaznenog progona na obradu podataka (države EFTA-e primjenjuju Direktivu (EU) 2016/680 kao posljedica svojih obveza na temelju schengenske pravne stečevine). To znači da se na kraju prijelaznog razdoblja prijenosi u te zemlje mogu nastaviti kao i prije izlaska iz EU-a. Nakon kraja prijelaznog razdoblja ministar mora preispitati te nalaze o primjerenosti u roku od četiri godine.

([140]) Članci 73. i 77. DPA-a iz 2018.

([141]) Tijela Ujedinjene Kraljevine objasnila su da se opis zemlje ili međunarodne organizacije odnosi na situaciju u kojoj bi bilo nužno provesti posebno i djelomično utvrđivanje primjerenosti s usmjerenim ograničenjima (na primjer, uredba o primjerenosti koja se odnosi samo na određenu vrstu prijenosa podataka).

([142]) Vidjeti članak 74.A stavak 4. DPA-a iz 2018. u kojem se predviđa da pri procjeni primjerenosti razine zaštite „ministar mora ponajprije uzeti u obzir: (a) vladavinu prava, poštovanje ljudskih prava i temeljnih sloboda, mjerodavno zakonodavstvo, i opće i sektorsko, što uključuje zakonodavstvo o javnoj sigurnosti, obrani, nacionalnoj sigurnosti, kaznenom pravu i pristupu tijela javne vlasti osobnim podacima, kao i provedbu takvog zakonodavstva, pravila o zaštiti podataka, pravila struke i mjere sigurnosti, što uključuje pravila za daljnji prijenos osobnih podataka još jednoj trećoj zemlji ili međunarodnoj organizaciji, koja se poštuju u toj zemlji ili međunarodnoj organizaciji, sudsku praksu te postojanje djelotvornih i provedivih prava ispitanika te djelotvorne upravne i sudske zaštite ispitanika čiji se osobni podaci prenose; (b) postojanje i djelotvorno funkcioniranje jednog neovisnog nadzornog tijela ili više njih u trećoj zemlji, ili tijela kojem podliježe međunarodna organizacija, odgovornih za osiguravanje i provođenje poštovanja pravila o zaštiti podataka, uključujući primjerene ovlasti izvršavanja zakonodavstva, za pružanje pomoći ispitanicima i njihovo savjetovanje u ostvarivanju njihovih prava te za suradnju s povjerenikom; i (c) međunarodne obveze koje je predmetna treća zemlja ili međunarodna organizacija preuzela ili druge obveze koje proizlaze iz pravno obvezujućih konvencija ili instrumenata, kao i iz njezina sudjelovanja u multilateralnim ili regionalnim sustavima, osobito u vezi sa zaštitom osobnih podataka".

primjerenosti Ujedinjene Kraljevine ([143]). Nakon što je ministar donese, ta se uredba upućuje Parlamentu i podliježe postupku „negativnog vijećanja" (*negative resolution procedure*) u okviru kojeg oba doma Parlamenta mogu preispitati uredbu i izglasati prijedlog o ukidanju uredbe u roku od 40 dana ([144]).

(78) Prema članku 74.B stavku 1. DPA-a iz 2018. uredbe o primjerenosti moraju se preispitivati u razmacima koji nisu dulji od četiri godine, a ministar mora kontinuirano pratiti promjene u trećim zemljama i međunarodnim organizacijama koje bi mogle utjecati na odluke o donošenju uredbi o primjerenosti ili na izmjenu ili ukidanje takvih uredbi. Ako ministar utvrdi da određena zemlja ili organizacija više ne osigurava primjerenu razinu zaštite osobnih podataka, mora, u mjeri u kojoj je to potrebno, izmijeniti ili ukinuti uredbu i pokrenuti savjetovanje s predmetnom trećom zemljom ili međunarodnom organizacijom kako bi riješili problem nedostatka primjerene razine zaštite.

(79) Slično onomu što je predviđeno u članku 37. Direktive (EU) 2016/680, u nedostatku uredbe o primjerenosti prijenos osobnih podataka u kontekstu sektora kaznenog progona bio bi moguć ako postoje odgovarajuće zaštitne mjere. Takve se zaštitne mjere osiguravaju ili (a) obvezujućim pravnim instrumentom koji sadržava odgovarajuće zaštitne mjere za zaštitu osobnih podataka ili (b) procjenom koju je proveo voditelj obrade koji, nakon što je procijenio sve okolnosti povezane s prijenosom, zaključuje da postoje odgovarajuće zaštitne mjere za zaštitu podataka ([145]). Nadalje, kad se prijenosi temelje na odgovarajućim zaštitnim mjerama, u DPA-u iz 2018. predviđa se da, pored uobičajenog nadzora koji obavlja ICO, nadležna tijela moraju ICO-u dostaviti posebne informacije o prijenosima ([146]).

(80) Ako se prijenos ne temelji na odluci o primjerenosti ili odgovarajućim zaštitnim mjerama, moguć je samo u nekim određenim okolnostima, takozvanim „posebnim okolnostima" ([147]). To su slučajevi u kojima je prijenos nužan: (a) kako bi se zaštitili vitalni interesi ispitanika ili druge osobe; (b) kako bi se zaštitili legitimni interesi ispitanika; (c) kako bi se spriječila neposredna i ozbiljna prijetnja javnoj sigurnosti treće zemlje; (d) u pojedinačnim slučajevima u neku od svrha kaznenog progona; ili (e) u pojedinačnim slučajevima u pravnu svrhu (na primjer, u vezi sa sudskim postupkom ili radi dobivanja pravnog savjeta) ([148]). Treba napomenuti da se točke (d) i (e) ne primjenjuju ako prava i slobode ispitanika imaju prednost pred javnim interesom za prijenos ([149]). Ta skupina okolnosti odgovara posebnim situacijama i uvjetima koji predstavljaju „odstupanja" na temelju članka 38. Direktive (EU) 2016/680.

(81) U tim se okolnostima moraju dokumentirati datum, vrijeme i obrazloženje prijenosa, ime primatelja i sve ostale bitne informacije o primatelju, kao i opis osobnih podataka koji se prenose, i te se informacije moraju dostaviti povjereniku za informiranje na njegov zahtjev ([150]).

(82) U članku 78. DPA-a iz 2018. uređuje se scenarij „naknadnih prijenosa" (*subsequent transfers*), to jest situacija kad se osobni podaci koji su preneseni iz Ujedinjene Kraljevine u treću zemlju nakon toga prenose u još jednu treću zemlju ili međunarodnoj organizaciji. U skladu s člankom 78. stavkom 1. voditelj obrade iz Ujedinjene Kraljevine koji obavlja prijenos mora uvjetovati prijenos time da se podaci ne smiju dalje prenositi u treću zemlju bez odobrenja tog voditelja obrade koji obavlja prijenos. Osim toga, u skladu s člankom 78. stavkom 3., a slično onomu što je predviđeno u članku 35. stavku 1. točki (e) Direktive (EU) 2016/680, ako je takvo odobrenje potrebno, primjenjuje

([143]) Vidjeti Memorandum o razumijevanju između ministra za digitalizaciju, kulturu, medije i sport i Ureda povjerenika za informiranje (ICO) o ulozi ICO-a u odnosu na nove procjene primjerenosti Ujedinjene Kraljevine, koji je dostupan na: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) U tom 40-dnevnom razdoblju oba doma Parlamenta mogu iskoristiti mogućnost, ako žele, da glasaju protiv uredbe; ako se to izglasa, uredba će naposljetku prestati imati daljnji pravni učinak.

([145]) Članak 75. DPA-a iz 2018.

([146]) Prema članku 75. stavku 3. DPA-a iz 2018., ako se prijenos podataka obavlja oslanjanjem na odgovarajuće zaštitne mjere: (a) prijenos se mora dokumentirati; (b) dokumentacija se mora dostaviti povjereniku na zahtjev; i (c) dokumentacija mora uključivati, ponajprije: i. datum i vrijeme prijenosa; ii. ime primatelja i sve ostale bitne informacije o primatelju; iii. obrazloženje prijenosa; i iv. opis prenesenih osobnih podataka.

([147]) Vodič za obradu podataka u svrhe kaznenog progona, „Postoje li posebne okolnosti?", dostupno na: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

([148]) Članak 76. DPA-a iz 2018.

([149]) Članak 76. DPA-a iz 2018.

([150]) Članak 76. stavak 3. DPA-a iz 2018.

se niz materijalnih zahtjeva. Konkretnije, pri odlučivanju o tome hoće li odobriti prijenos nadležno tijelo mora biti sigurno da je daljnji prijenos nužan u svrhu kaznenog progona te bi, među ostalim čimbenicima, trebalo uzeti u obzir: (a) ozbiljnost okolnosti koje su dovele do zahtjeva za odobrenje; (b) svrhu u koju su osobni podaci izvorno preneseni; i (c) standarde za zaštitu osobnih podataka koji se primjenjuju u trećoj zemlji ili međunarodnoj organizaciji kojoj bi se osobni podaci prenijeli.

(83) Nadalje, ako su podaci koji su predmet daljnjeg prijenosa iz Ujedinjene Kraljevine izvorno preneseni iz Europske unije, primjenjuju se dodatne zaštitne mjere.

(84) Prvo, u članku 73. stavku 1. točki (b) DPA-a iz 2018. – slično kao i u članku 35. stavku 1. točki (c) Direktive (EU) 2016/680 – predviđa se da je, u slučaju u kojem je država članica izvorno prenijela osobne podatke ili ih je na drugi način stavila na raspolaganje voditelju obrade ili drugom nadležnom tijelu, ta država članica ili bilo koja osoba iz te države članice koja je nadležno tijelo za potrebe Direktive (EU) 2016/680 morala odobriti taj prijenos u skladu s pravom te države članice.

(85) Međutim, slično kao i u članku 35. stavku 2. Direktive (EU) 2016/680, takvo se odobrenje ne zahtijeva (a) ako je prijenos nužan za sprečavanje neposredne i ozbiljne prijetnje bilo javnoj sigurnosti države članice ili treće zemlje bilo bitnim interesima države članice i (b) ako se odobrenje ne može pravodobno dobiti. U tom se slučaju mora bez odgode obavijestiti tijelo u toj državi članici koje bi bilo odgovorno za odlučivanje o odobravanju tog prijenosa ([151]).

(86) Drugo, isti se pristup primjenjuje u slučaju kad su podaci izvorno preneseni iz Europske unije u Ujedinjenu Kraljevinu, a potom ih je Ujedinjena Kraljevina dalje prenijela u treću zemlju koja bi ih nakon toga dalje prenijela u treću zemlju. U tom slučaju, u skladu s člankom 78. stavkom 4. nadležno tijelo Ujedinjene Kraljevine ne može dati svoje odobrenje za potonji prijenos, na temelju članka 78. stavka 1., osim ako je „država članica [koja je izvorno prenijela predmetne podatke] ili bilo koja osoba iz te države članice, a koja je nadležno tijelo za potrebe Direktive o zaštiti podataka u svrhe kaznenog progona, odobrila taj prijenos u skladu s pravom te države članice". Te su zaštitne mjere važne jer omogućuju tijelima država članica da osiguraju kontinuitet zaštite, u skladu s pravom Unije o zaštiti podataka, u cijelom „lancu prijenosa".

(87) Taj novi okvir za međunarodne prijenose postao je primjenjiv na kraju prijelaznog razdoblja ([152]). Međutim, u točkama od 10. do 12. Priloga 21. (uvedenima Uredbom DPPEC) predviđa se da se na kraju prijelaznog razdoblja s određenim prijenosima osobnih podataka postupa kao da se temelje na propisima o primjerenosti. Ti prijenosi uključuju prijenose državi članici, državi EFTA-e, trećoj zemlji na koju se na kraju prijelaznog razdoblja primjenjivala odluka o primjerenosti EU-a i području Gibraltara. Stoga se prijenosi u te zemlje mogu nastaviti kao i prije povlačenja Ujedinjene Kraljevine iz Unije. Nakon kraja prijelaznog razdoblja ministar mora preispitati te nalaze o primjerenosti u roku od četiri godine, tj. do kraja prosinca 2024. Prema objašnjenju koje su dala tijela Ujedinjene Kraljevine, iako ministar treba provesti to preispitivanje do kraja prosinca 2024., prijelazne odredbe ne sadržavaju odredbu o vremenskom ograničenju valjanosti, pa relevantne prijelazne odredbe neće automatski prestati imati učinak ako se preispitivanje ne dovrši do kraja prosinca 2024.

2.4.9. *Odgovornost*

(88) Na temelju načela odgovornosti tijela javne vlasti koja obrađuju podatke moraju uspostaviti odgovarajuće tehničke i organizacijske mjere kako bi djelotvorno ispunila svoje obveze u pogledu zaštite podataka te mogla dokazati da su ispunjene, prije svega nadležnom nadzornom tijelu.

(89) To se načelo odražava u članku 56. DPA-a iz 2018., u kojem se uvodi opća obveza o odgovornosti voditelja obrade, tj. obveza da provede odgovarajuće tehničke i organizacijske mjere kako bi osigurao, i kako bi mogao dokazati, da je obrada osobnih podataka usklađena sa zahtjevima iz dijela 3. DPA-a iz 2018. Provedene mjere moraju se preispitivati i ažurirati prema potrebi te, ako je to razmjerno s obzirom na obradu, moraju uključivati odgovarajuće politike zaštite podataka.

([151]) Članak 73. stavak 5. DPA-a iz 2018.

([152]) Primjenjivost tog novog okvira mora se tumačiti s obzirom na članak 782. Sporazuma o trgovini i suradnji između Europske unije i Europske zajednice za atomsku energiju, s jedne strane, i Ujedinjene Kraljevine Velike Britanije i Sjeverne Irske, s druge strane (SL L 444, 31.12.2020., str. 14.) („Sporazum o trgovini i suradnji između EU-a i Ujedinjene Kraljevine"), dostupan na: https://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:22020A1231(01)&from=HR

(90) U skladu s poglavljem IV. Direktive (EU) 2016/680, u člancima od 55. do 71. DPA-a iz 2018. predviđaju se različiti mehanizmi za osiguranje odgovornosti i omogućivanje voditeljima obrade i izvršiteljima obrade da dokažu usklađenost. Točnije, od voditelja obrade zahtijeva se da provedu mjere za tehničku i integriranu zaštitu podataka, tj. da osiguraju da su načela zaštite podataka djelotvorno provedena, te se zahtijeva da vode evidencije svih kategorija aktivnosti obrade za koje je voditelj obrade odgovoran (uključujući informacije o identitetu voditelja obrade, kontaktne podatke službenika za zaštitu podataka, svrhe obrade, kategorije primatelja otkrivanja te opis kategorija ispitanika i osobnih podataka) i da na zahtjev tu evidenciju stavljaju na raspolaganje povjereniku za informiranje. Voditelj obrade i izvršitelj obrade moraju bilježiti i zapise za određene postupke obrade i staviti ih na raspolaganje povjereniku za informiranje ([153]). Od voditelja obrade posebno se zahtijeva i da surađuju s povjerenikom za informiranje u obavljanju njegovih zadaća.

(91) U DPA-u iz 2018. utvrđuju se i dodatni zahtjevi za obradu koja će vjerojatno rezultirati visokim rizikom za prava i slobode pojedinaca. To uključuje obvezu provođenja procjena učinka na zaštitu podataka i obvezu savjetovanja s povjerenikom za informiranje prije obrade ako takva procjena ukaže na to da bi obrada mogla rezultirati visokim rizikom za prava i slobode pojedinaca (ako se ne bi poduzele mjere radi ublažavanja rizika).

(92) Nadalje, voditelji obrade moraju imenovati službenika za zaštitu podataka, osim ako je voditelj obrade sud ili drugo sudsko tijelo koje djeluje u svojem sudbenom svojstvu ([154]). Voditelj obrade mora osigurati da je službenik za zaštitu podataka uključen u sva pitanja koja se odnose na zaštitu osobnih podataka, da ima potrebna sredstva te pristup osobnim podacima i postupcima obrade i da može neovisno obavljati svoje zadaće. Zadaće službenika za zaštitu podataka utvrđene su u članku 71. DPA-a iz 2018., uključujući davanje informacija i savjeta, praćenje usklađenosti te suradnju s povjerenikom za informiranje i djelovanje kao kontaktna točka za povjerenika za informiranje. U obavljanju svojih zadaća službenik za zaštitu podataka mora voditi računa o rizicima povezanima s postupcima obrade, uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade.

2.5. **Nadzor i provedba**

2.5.1. *Neovisni nadzor*

(93) Kako bi se primjerena razina zaštite podataka osigurala i u praksi, mora se uspostaviti neovisno nadzorno tijelo s ovlastima za praćenje i osiguravanje usklađenosti s pravilima o zaštiti podataka. To tijelo pri obavljanju svojih dužnosti i izvršavanju svojih ovlasti mora djelovati potpuno neovisno i nepristrano.

(94) U Ujedinjenoj Kraljevini nadzor i provedbu usklađenosti s Općom uredbom Ujedinjene Kraljevine o zaštiti podataka i DPA-om iz 2018. obavlja povjerenik za informiranje ([155]). Osim toga, povjerenik za informiranje nadzire i obradu osobnih podataka koju obavljaju nadležna tijela i koja je obuhvaćena područjem primjene dijela 3. DPA-a iz 2018. ([156]) Povjerenik za informiranje je tijelo pojedinac (*corporation sole*): zaseban pravni subjekt koji se sastoji od jedne osobe. Povjerenika za informiranje u radu podupire ured. Ured povjerenice za informiranje (ICO) 31. ožujka 2020. imao je 768 članova stalnog osoblja ([157]). Povjerenika za informiranje sponzorira Ministarstvo za digitalizaciju, kulturu, medije i sport ([158]).

([153]) Članak 62. DPA-a iz 2018.
([154]) Članak 69. DPA-a iz 2018.
([155]) Članak 36. stavak 2. točka (b) Direktive (EU) 2016/680.
([156]) Članak 116. DPA-a iz 2018.
([157]) Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2019.–2020., dostupno na: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf
([158]) Njihov je odnos uređen sporazumom o upravljanju. Točnije, glavne odgovornosti Ministarstva za digitalizaciju, kulturu, medije i sport kao ministarstva sponzora uključuju: osiguravanje da ICO raspolaže primjerenim financiranjem i resursima, zastupanje interesa ICO-a pred Parlamentom i drugim Vladinim odjelima, osiguravanje da je uspostavljen stabilan nacionalni okvir za zaštitu podataka te davanje smjernica i potpore ICO-u u korporativnim pitanjima kao što su pitanja povezana s imovinom, ugovori o zakupu i javna nabava (Sporazum o upravljanju za 2018.–2021., dostupan na: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Neovisnost povjerenika izričito je utvrđena u članku 52. Opće uredbe Ujedinjene Kraljevine o zaštiti podataka, koji odražava zahtjeve utvrđene u članku 52. stavcima od 1. do 3. Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća ([159]). Povjerenik mora djelovati potpuno neovisno pri obavljanju dužnosti i izvršavanju ovlasti u skladu s Općom uredbom Ujedinjene Kraljevine o zaštiti podataka, mora biti slobodan od vanjskog utjecaja (izravnog ili neizravnog) te ne smije tražiti ni primati upute ni od koga. Povjerenik se mora suzdržati i od svih radnji koje nisu u skladu s njegovim dužnostima i za vrijeme mandata ne smije se baviti nikakvom neusklađenom djelatnošću, bez obzira na to je li plaćena.

(96) Uvjeti za imenovanje i razrješenje povjerenika za informiranje utvrđeni su u Prilogu 12. DPA-u iz 2018. Povjerenika za informiranje imenuje Njezino Veličanstvo na preporuku Vlade na temelju poštenog i otvorenog natječaja. Kandidat mora imati odgovarajuće kvalifikacije, vještine i kompetencije. U skladu s Kodeksom upravljanja za imenovanje javnih službenika (*Governance Code on Public Appointments*) ([160]) savjetodavni odbor za procjenu sastavlja popis kandidata koji se mogu imenovati. Prije nego što ministar za digitalizaciju, kulturu, medije i sport donese konačnu odluku, odgovarajući posebni odbor Parlamenta mora provesti preispitivanje prije imenovanja. Stajalište odbora javno se objavljuje ([161]).

(97) Mandat povjerenika za informiranje traje do sedam godina. Njezino Veličanstvo može povjerenika za informiranje razriješiti dužnosti na molbu obaju domova Parlamenta ([162]). Zahtjev za razrješenje povjerenika za informiranje ne može se podnijeti nijednom domu Parlamenta ako ministar ne dostavi izvješće tom domu u kojem navodi da je uvjeren da je povjerenik za informiranje teško povrijedio dužnosti i/ili da povjerenik više ne ispunjava uvjete koji se zahtijevaju za izvršavanje funkcija povjerenika ([163]).

(98) Tri su izvora financiranja povjerenika za informiranje: i. naknade za zaštitu podataka koje plaćaju voditelji obrade i koje se određuju uredbom ministra ([164]) i čine 85–90 % godišnjeg proračuna Ureda ([165]); ii. subvencija koju Vlada može plaćati povjereniku za informiranje i koja se uglavnom koristi za financiranje troškova poslovanja povjerenika za informiranje u pogledu zadaća koje nisu povezane sa zaštitom podataka ([166]); i iii. naknade koje se naplaćuju za usluge ([167]). Trenutačno se ne naplaćuju takve naknade.

(99) Opće funkcije povjerenika za informiranje u pogledu obrade osobnih podataka obuhvaćene područjem primjene dijela 3. DPA-a iz 2018. utvrđene su u Prilogu 13. DPA-u iz 2018. Te zadaće uključuju praćenje i provedbu dijela 3. DPA-a iz 2018., promicanje javne svijesti, savjetovanje Parlamenta, vlade i drugih institucija o zakonodavnim i upravnim mjerama, informiranje voditelja obrade i izvršitelja obrade o njihovim obvezama, davanje informacija

([159]) Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, .4.5.2016., str. 1.).

([160]) Kodeks upravljanja za imenovanje javnih službenika, dostupan na: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Drugo izvješće zasjedanja Odbora za kulturu, medije i sport Zastupničkog doma u razdoblju 2015.–2016., dostupno na: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) „Molba" (*address*) je prijedlog stavljen na dnevni red Parlamenta kako bi se monarha obavijestilo o mišljenju Parlamenta o određenom pitanju.

([163]) Točka 3. Priloga 12. DPA-u iz 2018.

([164]) Članak 137. DPA-a iz 2018.

([165]) Članci 137. i 138. DPA-a iz 2018. sadržavaju niz zaštitnih mjera kako bi se osigurala primjerena visina tih naknada. Konkretnije, u članku 137. stavku 4. DPA-a iz 2018. navode se pitanja koja ministar mora uzeti u obzir pri donošenju uredbi kojima se određuje iznos koji različite organizacije moraju plaćati. U članku 138. stavku 1. i članku 182. DPA-a iz 2018. zahtijeva se i da se ministar prije donošenja uredbi savjetuje s povjerenikom za informiranje i drugim predstavnicima osoba na koje će te uredbe vjerojatno utjecati kako bi mogao uzeti u obzir njihova mišljenja. Osim toga, na temelju članka 138. stavka 2. DPA-a iz 2018. povjerenik za informiranje dužan je preispitivati funkcioniranje uredbi o naknadama i može ministru podnositi prijedloge izmjena tih uredbi. Naposljetku, uredbe podliježu postupku „pozitivnog vijećanja" (*affirmative resolution procedure*) i ne mogu se donijeti dok ih rezolucijom ne potvrde oba doma Parlamenta, osim ako se uredbe donose samo kako bi se u obzir uzelo povećanje indeksa maloprodajnih cijena (u tom će se slučaju na njih primjenjivati postupak „negativnog vijećanja" (*negative resolution procedure*)).

([166]) U Sporazumu o upravljanju pojašnjeno je da „ministar na temelju točke 9. Priloga 12. DPA-u iz 2018. može izvršavati plaćanja povjereniku za informiranje iz novca koji je osigurao Parlament. Nakon savjetovanja s povjerenikom za informiranje Ministarstvo za digitalizaciju, kulturu, medije i sport isplatit će povjereniku odgovarajuće iznose (subvencija) za administrativne troškove Ureda povjerenika za informiranje i izvršavanje funkcija povjerenika povezanih s nizom posebnih funkcija, uključujući slobodu informiranja" (Sporazum o upravljanju za 2018.–2021., točka 1.12., vidjeti bilješku 158.).

([167]) Članak 134. DPA-a iz 2018.

ispitanicima o ostvarivanju njihovih prava i provođenje istraga. Kako bi se očuvala neovisnost sudstva, povjerenik za informiranje nije ovlašten izvršavati svoje funkcije u vezi s obradom osobnih podataka koju provodi pojedinac koji djeluje u sudbenom svojstvu ili sud u okviru svoje sudske nadležnosti. Međutim, nadzor nad sudstvom osiguravaju specijalizirana tijela, što se razmatra u nastavku.

2.5.1.1. Izvršenje, uključujući sankcije

(100) Povjerenik ima opće istražne, korektivne i savjetodavne ovlasti te ovlasti za izdavanje odobrenja u vezi s obradom osobnih podataka na koju se primjenjuje dio 3. DPA-a iz 2018. Povjerenik ima ovlasti obavijestiti voditelja obrade ili izvršitelja obrade o navodnom kršenju dijela 3., izdavati upozorenja voditelju obrade ili izvršitelju obrade da će se namjeravanim postupcima obrade vjerojatno kršiti odredbe iz dijela 3. i izdavati opomene voditelju obrade ili izvršitelju obrade ako su postupcima obrade prekršene odredbe iz dijela 3. Nadalje, povjerenik može na vlastitu inicijativu ili na zahtjev davati mišljenja Parlamentu Ujedinjene Kraljevine, vladi ili drugim institucijama i tijelima te javnosti o svim pitanjima povezanima sa zaštitom osobnih podataka ([168]).

(101) Nadalje, povjerenik je ovlašten:

— izdavanjem zahtjeva za dostavu informacija naložiti voditelju obrade i izvršitelju obrade (a u određenim okolnostima i bilo kojoj drugoj osobi) da dostave potrebne informacije („zahtjev za dostavu informacija") ([169]),

— provoditi istrage i revizije izdavanjem zahtjeva za provjeru, kojim se od voditelja obrade ili izvršitelja obrade može zahtijevati da povjereniku dopusti ulazak u određene prostore, obavljanje inspekcije ili pregleda dokumenata ili opreme, obavljanje razgovora s osobama koje obrađuju osobne podatke u ime voditelja obrade („zahtjev za provjeru") ([170]),

— na drugi način dobiti pristup dokumentima voditelja obrade i izvršitelja obrade i pristup njihovim prostorima u skladu s člankom 154. DPA-a iz 2018. („ovlasti ulaska i inspekcije"),

— izvršavati korektivne ovlasti, među ostalim, izdavanjem upozorenja i opomena, ili davati naloge u obliku zahtjeva za izvršenje, kojim se od voditelja obrade/izvršitelja obrade zahtijeva da poduzmu određene mjere ili da se suzdrže od njihova poduzimanja („zahtjev za izvršenje") ([171]), i

— izricati upravne novčane kazne u obliku rješenja o kazni („rješenje o kazni") ([172]).

(102) U okviru politike regulatornog djelovanja ICO-a određuju se okolnosti u kojima će povjerenik izdati zahtjev za dostavu informacija, zahtjev za provjeru, zahtjev za izvršenje odnosno rješenje o kazni ([173]). Zahtjevom za izvršenje mogu se uvesti zahtjevi koje povjerenik smatra primjerenima za potrebe ispravljanja propusta. Rješenjem o kazni od osobe se zahtijeva da povjereniku za informiranje plati iznos naveden u rješenju. Rješenje o kazni može se izdati u slučaju nepoštovanja određenih odredbi iz DPA-a iz 2018. ([174]) ili se može izdati voditelju obrade ili izvršitelju obrade koji nije poštovao zahtjev za dostavu informacija, zahtjev za provjeru ili zahtjev za izvršenje.

(103) Konkretnije, pri odlučivanju o tome treba li voditelju obrade ili izvršitelju obrade izdati rješenje o kazni i pri određivanju iznosa te kazne povjerenik za informiranje mora uzeti u obzir elemente navedene u članku 155. stavku 3. DPA-a iz 2018., uključujući prirodu i težinu povrede, ima li povreda obilježje namjere ili nepažnje, sve radnje koje je voditelj obrade ili izvršitelj obrade poduzeo kako bi ublažio štetu koju su pretrpjeli ispitanici, stupanj

([168]) Točka 2. Priloga 13. DPA-u iz 2018.
([169]) Članak 142. DPA-a iz 2018. (podložno ograničenjima iz članka 143. DPA-a iz 2018.).
([170]) Članak 146. DPA-a iz 2018. (podložno ograničenjima iz članka 147. DPA-a iz 2018.).
([171]) Članci od 149. do 151. DPA-a iz 2018. (podložno ograničenjima iz članka 152. DPA-a iz 2018.).
([172]) Članak 155. DPA-a iz 2018. (podložno ograničenjima iz članka 156. DPA-a iz 2018.).
([173]) Politika regulatornog djelovanja, dostupno na: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) Konkretno, ICO može izdati rješenje o kazni za nepoštovanje obveza i odredbi navedenih u članku 149. stavcima 2., 3., 4. ili 5. DPA-a iz 2018.

odgovornosti voditelja obrade ili izvršitelja obrade (uzimajući u obzir tehničke i organizacijske mjere koje su primijenili), sve relevantne prijašnje povrede voditelja obrade ili izvršitelja obrade, kategorije osobnih podataka na koje je povreda utjecala te bi li kazna bila djelotvorna, proporcionalna i odvraćajuća.

(104) Najviši iznos kazne koji se može izreći rješenjem o kazni iznosi (a) 17 500 000 GBP za nepoštovanje načela zaštite podataka (članci 35., 36. i 37., članak 38. stavak 1., članak 39. stavak 1. i članak 40. DPA-a iz 2018.), nepoštovanje obveza u pogledu transparentnosti i prava pojedinaca (članci 44., 45., 46., 47., 48., 49., 52. i 53. DPA-a iz 2018.) i nepoštovanje načela za međunarodne prijenose osobnih podataka (članci 73., 75., 76., 77. i 78. DPA-a iz 2018.); i (b) 8 700 000 GBP u ostalim slučajevima ([175]). Za nepoštovanje zahtjeva za dostavu informacija, zahtjeva za provjeru ili zahtjeva za izvršenje najveći iznos kazne koji se može izreći u rješenju o kazni iznosi 17 500 000 GBP.

(105) Prema posljednjim godišnjim izvješćima (za 2018.–2019. ([176]), 2019.–2020. ([177])) povjerenica za informiranje provela je niz istraga povezanih s obradom osobnih podataka koju provode tijela kaznenog progona. Na primjer, povjerenica je provela istragu i u listopadu 2019. objavila mišljenje o primjeni tehnologije prepoznavanja lica na javnim mjestima kojom se služe tijela kaznenog progona. Istraga je konkretno bila usmjerena na korištenje tehnologije za prepoznavanje lica u stvarnom vremenu kojom se služe policija južnog Walesa i londonska policijska uprava (MPS). Osim toga, povjerenica za informiranje istražila je i „matricu za bande" ([178]) londonske policijske uprave i utvrdila niz teških kršenja zakona o zaštiti podataka koja bi vjerojatno mogla narušiti povjerenje javnosti u matricu i način korištenja podataka.

(106) U studenome 2018. povjerenica za informiranje izdala je zahtjev za izvršenje, a londonska policijska uprava potom je poduzela mjere potrebne za povećanje sigurnosti i odgovornosti te osiguravanje proporcionalnog korištenja podataka.

(107) Još jedan primjer nedavne mjere izvršenja jest novčana kazna od 325 000 GBP koju je povjerenica u svibnju 2018. izrekla Državnom tužiteljstvu Ujedinjene Kraljevine (*Crown Prosecution Service*) zbog gubitka nešifriranih DVD-ova sa snimkama policijskih obavijesnih razgovora/ispitivanja. Nadalje, povjerenica za informiranje provela je i istrage o širim temama, na primjer u prvoj polovini 2020. o izvlačenju podataka iz mobilnih telefona za potrebe policije i načinu na koji policija obrađuje podatke o žrtvama.

(108) Osim tih izvršnih ovlasti povjerenika za informiranje, određena kršenja zakonodavstva o zaštiti podataka čine kaznena djela i stoga se na njih mogu primjenjivati kaznene sankcije (članak 196. DPA-a iz 2018.). To se, na primjer, odnosi na prikupljanje ili otkrivanje osobnih podataka bez pristanka voditelja obrade i omogućavanje otkrivanja osobnih podataka drugoj osobi bez pristanka voditelja obrade ([179]); ponovnu identifikaciju anonimiziranih osobnih podataka bez pristanka voditelja obrade odgovornog za anonimizaciju osobnih podataka ([180]); namjerno ometanje povjerenika u izvršavanju njegovih ovlasti povezanih s pregledom osobnih podataka u skladu s međunarodnim obvezama ([181]), davanje lažnih izjava kao odgovor na zahtjev za dostavu informacija ili uništavanje informacija povezanih sa zahtjevima za dostavu informacija i zahtjevima za provjeru ([182]).

(109) Povjerenik za informiranje ima i dužnost u skladu s člankom 139. DPA-a iz 2018. da svakom od domova Parlamenta uputi opće izvješće o izvršavanju svojih funkcija na temelju tog zakona ([183]).

([175]) Članak 157. DPA-a iz 2018.

([176]) Godišnje izvješće i financijski izvještaji povjerenice za informiranje za 2018.-2019., dostupno na: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Godišnje izvješće povjerenice za informiranje za 2019.–2020. (vidjeti bilješku 157.).

([178]) Baza podataka u kojoj su evidentirane obavještajne informacije o navodnim članovima bandi i žrtvama kaznenih djela koja su povezana s bandama.

([179]) Članak 170. DPA-a iz 2018.

([180]) Članak 171. DPA-a iz 2018.

([181]) Članak 119. DPA-a iz 2018.

([182]) Članci 144. i 148. DPA-a iz 2018.

([183]) Kako je utvrđeno u Sporazumu o upravljanju: i. godišnje izvješće mora obuhvaćati sve korporativne, supsidijarne ili zajedničke pothvate pod kontrolom ICO-a; ii. godišnje izvješće mora biti u skladu s Priručnikom za financijsko izvještavanje Ministarstva financija (FReM); iii. godišnje izvješće mora sadržavati izjavu o upravljanju, u kojoj se navodi kako je računovodstveni službenik tijekom godine upravljao sredstvima koja se koriste u toj organizaciji i kako ih je kontrolirao, i u kojoj se prikazuje koliko je dobro organizacija upravljala rizicima u ostvarivanju svojih ciljeva; i iv. u godišnjem izvješću moraju se ukratko prikazati glavne aktivnosti i rezultati iz prethodne financijske godine i sažeto navesti planovi za budućnost (Sporazum o upravljanju za 2018.–2021., točka 3.26., vidjeti bilješku 158).

2.5.2. *Nadzor nad sudstvom*

(110) Nadzor nad obradom osobnih podataka koju provode sudovi i pravosuđe dvostran je. Ako nositelj sudačke dužnosti ili sud ne djeluje u okviru sudske nadležnosti, nadzor obavlja povjerenik za informiranje (ICO). Ako voditelj obrade djeluje u okviru sudske nadležnosti, ICO ne može izvršavati svoje nadzorne funkcije ([184]) pa nadzor provode posebna tijela. To odražava pristup iz članka 32. Direktive (EU) 2016/680.

(111) Točnije, u drugom slučaju nadzor nad sudovima u Engleskoj i Walesu te Prvostupanjskim sudom i Višim sudom u Engleskoj i Walesu obavlja Odbor za sudsku zaštitu podataka ([185]). Osim toga, vrhovni sudac (*Lord Chief Justice*) i visoki predsjednik sudova (*Senior President of Tribunals*) objavili su obavijest o zaštiti osobnih podataka ([186]) u kojoj je navedeno kako sudovi u Engleskoj i Walesu obrađuju osobne podatke za sudbenu funkciju. Sličnu obavijest objavili su i suci Sjeverne Irske ([187]) i Škotske ([188]).

(112) Osim toga, vrhovni sudac Sjeverne Irske imenovao je suca Visokog suda koji u Sjevernoj Irskoj djeluje kao sudac za nadzor podataka ([189]). Objavljene su i smjernice za suce Sjeverne Irske o tome kako postupati u slučaju gubitka ili mogućeg gubitka podataka i postupku za rješavanje svih pitanja koja iz toga mogu proizaći ([190]).

(113) U Škotskoj je predsjednik Vrhovnog građanskog suda (*Lord President*) imenovao suca za nadzor podataka, koji ispituje sve pritužbe u vezi sa zaštitom podataka. To je utvrđeno na temelju pravila o pravosudnim pritužbama koja odražavaju pravila utvrđena za Englesku i Wales ([191]).

(114) Naposljetku, na Vrhovnom sudu jedan od njegovih sudaca predlaže se za funkciju nadziranja zaštite podataka.

([184]) Članak 117. DPA-a iz 2018.

([185]) Odbor je odgovoran za davanje smjernica i osposobljavanje sudaca. Bavi se i pritužbama ispitanika na obradu osobnih podataka koju obavljaju sudovi i pojedinci koji djeluju u sudbenom svojstvu. Svrha je Odbora pružiti sredstvo kojim se mogu riješiti sve pritužbe. Ako podnositelj pritužbe nije zadovoljan odlukom Odbora i dostavi dodatne dokaze, Odbor bi mogao preispitati svoju odluku. Iako sam Odbor ne izriče financijske sankcije, ako smatra da je došlo do dovoljno teškog kršenja DPA-a iz 2018., može uputiti slučaj Uredu za preispitivanje sudačkog postupanja (*Judicial Conduct Investigation Office*, JCIO), koji će ispitati pritužbu. Ako se potvrdi osnovanost pritužbe, lord kancelar (*Lord Chancellor*) i vrhovni sudac (ili viši sudac kojem je delegirano da djeluje u njegovo ime) trebaju odlučiti koju bi mjeru trebalo poduzeti protiv nositelja sudačke dužnosti. To bi moglo uključivati, prema stupnju ozbiljnosti: službeni savjet, službeno upozorenje, opomenu i, naposljetku, razrješenje dužnosti. Ako pojedinac nije zadovoljan načinom na koji je JCIO ispitao pritužbu, može se dalje žaliti Ombudsmanu za sudska imenovanja i postupanje (vidjeti https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsman je ovlašten tražiti od JCIO-a da ponovno ispita pritužbu i može predložiti da se podnositelju pritužbe plati naknada ako smatra da je podnositelj pretrpio štetu kao rezultat nepravilnosti u postupanju.

([186]) Obavijest vrhovnog suca i visokog predsjednika sudova o zaštiti osobnih podataka dostupna je na: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Obavijest o zaštiti osobnih podataka koju je objavio vrhovni sudac Sjeverne Irske dostupna je na: https://judiciaryni.uk/data-privacy.

([188]) Obavijest o zaštiti osobnih podataka za škotske sudove dostupna je na: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Sudac za nadzor podataka sucima daje smjernice i ispituje povrede i/ili pritužbe na obradu osobnih podataka koju provode sudovi ili pojedinci koji djeluju u sudbenom svojstvu.

([190]) Ako se smatra da je pritužba ili povreda teška, upućuje se službeniku za pravosudne pritužbe radi daljnje istrage u skladu s Kodeksom prakse za pritužbe koji je objavio vrhovni sudac Sjeverne Irske. Ishod takve pritužbe mogao bi biti: bez daljnjeg djelovanja, savjet, osposobljavanje ili mentorstvo, neslužbeno upozorenje, službeno upozorenje, konačno upozorenje, ograničenje prakse ili upućivanje sudu predviđenom zakonom. Kodeks dobre prakse za pritužbe koji je objavio vrhovni sudac Sjeverne Irske dostupan je na: 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]) Sve pritužbe koje su utemeljene ispituje sudac za nadzor podataka i upućuju se predsjedniku Vrhovnog građanskog suda, koji je ovlašten izdati savjet, službeno upozorenje ili opomenu ako smatra da je to potrebno (jednaka pravila postoje za članove sudova i dostupna su na: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Sudska zaštita*

(115) Kako bi se osigurala primjerena zaštita, a naročito ostvarivanje prava pojedinca, ispitaniku bi trebalo pružiti učinkovitu upravnu i sudsku zaštitu, uključujući naknadu štete.

(116) Prvo, ispitanik ima pravo podnijeti pritužbu povjereniku za informiranje ako smatra da u vezi s osobnim podacima koji se odnose na njega postoji kršenje dijela 3. DPA-a iz 2018. ([192]) Kako je opisano u uvodnim izjavama od (100). do (109)., povjerenik za informiranje ovlašten je ocjenjivati usklađenost voditelja obrade i izvršitelja obrade s DPA-om iz 2018., zahtijevati od njih da poduzmu potrebne korake u slučaju neusklađenosti ili da se suzdrže od njih i izricati novčane kazne.

(117) Drugo, u DPA-u iz 2018. predviđa se pravo na pravni lijek protiv povjerenika za informiranje. Ako povjerenik ne „ostvari napredak" ([193]) u pogledu pritužbe koju je podnio ispitanik, podnositelj pritužbe ima pristup sudskom pravnom lijeku, odnosno može se obratiti Prvostupanjskom sudu ([194]) koji će naložiti povjereniku da poduzme odgovarajuće korake kao odgovor na pritužbu ili obavijesti podnositelja pritužbe o ostvarenom napretku u pogledu pritužbe ([195]). Osim toga, svaka osoba kojoj povjerenik izda bilo koji od navedenih zahtjeva ili rješenja (zahtjev za dostavu informacija, provjeru ili izvršenje ili rješenje o kazni) može podnijeti žalbu Prvostupanjskom sudu. Ako Sud smatra da odluka povjerenika nije u skladu sa zakonom ili da je povjerenik za informiranje trebao drukčije izvršavati svoje pravo na odlučivanje, Sud mora prihvatiti žalbu ili zamijeniti zahtjev, rješenje ili odluku koju je povjerenik za informiranje izdao ili donio drugim zahtjevom, rješenjem ili odlukom ([196]).

(118) Treće, pojedinci mogu dobiti sudsku zaštitu protiv voditelja obrade i izvršitelja obrade izravno pred sudovima na temelju članka 167. DPA-a iz 2018. Ako je sud, na zahtjev ispitanika, uvjeren da je došlo do povrede prava ispitanika na temelju zakonodavstva o zaštiti podataka, može naložiti voditelju obrade, ili izvršitelju obrade koji djeluje u ime tog voditelja, da poduzme mjere navedene u nalogu ili da se suzdrži od poduzimanja mjera navedenih u nalogu. Nadalje, u skladu s člankom 169. DPA-a iz 2018. svaka osoba koja pretrpi štetu zbog kršenja zahtjeva iz zakonodavstva o zaštiti podataka (uključujući dio 3. DPA-a iz 2018.), osim Opće uredbe Ujedinjene Kraljevine o zaštiti podataka, ima pravo na naknadu te štete od voditelja obrade ili izvršitelja obrade, osim ako voditelj obrade ili izvršitelj obrade dokaže da ni na koji način nije odgovoran za događaj koji je prouzročio štetu. Šteta obuhvaća i financijski gubitak i štetu koja ne uključuje financijski gubitak, kao što je pretrpljena duševna bol.

(119) Četvrto, svaka osoba koja smatra da su tijela javne vlasti prekršila njezina prava, uključujući prava na privatnost i zaštitu podataka, može dobiti sudsku zaštitu od sudova Ujedinjene Kraljevine na temelju Zakona o ljudskim pravima iz 1998. Voditelji obrade iz dijela 3. DPA-a iz 2018., tj. nadležna tijela, uvijek su tijela javne vlasti u smislu Zakona o ljudskim pravima iz 1998. Pojedinac koji tvrdi da je tijelo javne vlasti djelovalo (ili namjerava djelovati) na način koji nije u skladu s pravom iz Konvencije, a time i nezakonito na temelju članka 6. stavka 1. Zakona o ljudskim pravima iz 1998., može pokrenuti postupak protiv tog tijela pred odgovarajućim sudom ili se može pozvati na predmetna prava u svim sudskim postupcima ako jest (ili bi bio) žrtva nezakonite radnje ([197]).

([192]) Članak 165. DPA-a iz 2018.

([193]) U članku 166. DPA-a iz 2018. konkretno se navode sljedeće situacije: (a) povjerenik nije poduzeo odgovarajuće korake kako bi odgovorio na pritužbu; (b) povjerenik nije dostavio podnositelju pritužbe informacije o napretku ili ishodu pritužbe prije isteka roka od tri mjeseca koji počinje teći od dana kad je povjerenik primio pritužbu; ili (c) ako povjerenik u tom roku nije završio s ispitivanjem pritužbe te o tome nije obavijestio podnositelja pritužbe u narednom razdoblju od tri mjeseca.

([194]) Prvostupanjski sud je sud nadležan za rješavanje žalbi protiv odluka koje donose državna regulatorna tijela. Za odluke povjerenika za informiranje nadležno je Opće regulatorno vijeće (*General Regulatory Chamber*), koje je nadležno za cijelu Ujedinjenu Kraljevinu.

([195]) Članak 166. DPA-a iz 2018.

([196]) Članci 161. i 162. DPA-a iz 2018.

([197]) Vidjeti predmet *Brown protiv Commissioner of the Met* iz 2016., u kojem je sud pružio zaštitu tužiteljici u kontekstu zaštite podataka u tužbi podnesenoj protiv policije. Sud je presudio u korist tužiteljice i potvrdio njezine tvrdnje o kršenju obveza iz DPA-a iz 1998., kršenju Zakona o ljudskim pravima iz 1998. (i povezanog prava iz članka 8. EKLJP-a) i štetnoj radnji uslijed zloupotrebe osobnih informacija (tuženik je naposljetku priznao kršenje DPA-a i EKLJP-a pa je presuda bila usmjerena na razmatranje primjerene odštete). Sud je zbog tih kršenja tužiteljici dodijelio novčanu naknadu štete.

(120) Ako utvrdi da je neka radnja tijela javne vlasti nezakonita, sud može u okviru svojih ovlasti odobriti mjeru ili pravni lijek, ili izdati nalog, kako smatra da je pravedno i primjereno ([198]). Sud može odlučiti i da odredba iz primarnog zakonodavstva nije u skladu s pravom zajamčenim EKLJP-om.

(121) Naposljetku, nakon što iscrpi sve nacionalne pravne lijekove, pojedinac može dobiti sudsku zaštitu pred Europskim sudom za ljudska prava za povrede prava zajamčenih EKLJP-om.

2.6. **Daljnja razmjena**

(122) Pravom Ujedinjene Kraljevine dopušta se da tijelo kaznenog progona razmjenjuje podatke s drugim tijelima Ujedinjene Kraljevine u svrhe u koje podaci nisu izvorno prikupljeni (takozvana „daljnja razmjena"), što podliježe određenim uvjetima.

(123) Slično onomu što je predviđeno u članku 4. stavku 2. Direktive (EU) 2016/680, u članku 36. stavku 3. DPA-a iz 2018. određeno je da je daljnja obrada (bilo da je obavlja prvotni ili neki drugi voditelj obrade) osobnih podataka koje je prikupilo nadležno tijelo u svrhu kaznenog progona dopuštena u bilo koju drugu svrhu kaznenog progona ako je voditelj obrade zakonski ovlašten za obradu u tu drugu svrhu te ako je obrada nužna i proporcionalna ([199]). U tom se slučaju sve zaštitne mjere predviđene u dijelu 3. DPA-a iz 2018., koje su analizirane prethodno u tekstu, primjenjuju na obradu koju obavlja tijelo primatelj.

(124) U pravnom poretku Ujedinjene Kraljevine više zakona izričito dopušta daljnju razmjenu. Točnije, i. Zakon o digitalnom gospodarstvu iz 2017. dopušta razmjenu podataka između tijela javne vlasti u nekoliko svrha, na primjer u slučaju svih prijevara na štetu javnog sektora koje bi uključivale gubitak ili rizik od gubitka za tijelo javne vlasti ([200]) ili u slučaju duga prema tijelu javne vlasti ili Kruni ([201]); ii. Zakon o kaznenim djelima i sudovima iz 2013. dopušta razmjenu informacija s Nacionalnom agencijom za kriminalitet (NCA) ([202]) u svrhu suzbijanja, istrage i kaznenog progona teških kaznenih djela i organiziranog kriminala; iii. Zakon o teškim kaznenim djelima iz 2007. dopušta tijelima javne vlasti da otkriju informacije organizacijama za borbu protiv prijevara za potrebe sprečavanja prijevara ([203]).

(125) U tim je zakonima izričito predviđeno da bi razmjena informacija trebala biti u skladu s pravilima utvrđenima u DPA-u iz 2018. Osim toga, Nacionalna agencija za policiju (*College of Policing*) izdala je odobrenu profesionalnu praksu za razmjenu informacija ([204]) kako bi pomogla policiji da ispuni svoje obveze u pogledu zaštite podataka na temelju Opće uredbe o zaštiti podataka Ujedinjene Kraljevine, DPA-a i Zakona o ljudskim pravima iz 1998. Usklađenost razmjene s primjenjivim pravnim okvirom za zaštitu podataka može, naravno, podlijegati sudskom preispitivanju ([205]).

(126) Nadalje, slično odredbama članka 9. Direktive (EU) 2016/680, u DPA-u iz 2018. predviđeno je da se osobni podaci prikupljeni u bilo koju svrhu kaznenog progona mogu obrađivati u svrhu koja nije kazneni progon ako je obrada odobrena pravom ([206]). Ta vrsta razmjene obuhvaća dva scenarija: 1. tijelo kaznenog progona razmjenjuje podatke s tijelom za izvršavanje zakonodavstva koje se ne bavi kaznenim progonom osim obavještajne agencije (na primjer, financijsko ili porezno tijelo, tijelo za tržišno natjecanje, ured za skrb o mladima); i 2. tijelo kaznenog progona

([198]) Članak 8. stavak 1. Zakona o ljudskim pravima iz 1998.

([199]) Članak 36. stavak 3. DPA-a iz 2018.

([200]) Članak 56. Zakona o digitalnom gospodarstvu iz 2017., dostupno na: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) Članak 48. Zakona o digitalnom gospodarstvu iz 2017.

([202]) Članak 7. Zakona o kaznenim djelima i sudovima iz 2013., dostupno na: https://www.legislation.gov.uk/ukpga/2013/22/contents.

([203]) Članak 68. Zakona o teškim kaznenim djelima iz 2007., dostupno na: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([204]) Odobrena profesionalna praksa za razmjenu informacija, dostupna na: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

([205]) Vidjeti, na primjer, predmet *M protiv the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), u kojem se od Visokog suda tražilo da preispita razmjenu podataka između policije i Partnerstva za smanjenje gospodarskog kriminala (BCRP), organizacije koja je ovlaštena upravljati programima obavijesti o isključenju, kojima se osobama zabranjuje da uđu u poslovne prostore članova tog partnerstva. Sud je preispitao tu razmjenu podataka, koja se odvijala na temelju sporazuma čija je svrha bila zaštita javnosti i sprečavanje kaznenih djela, te je naposljetku zaključio da je većina aspekata razmjene podataka bila zakonita, osim određenih osjetljivih informacija koje su policija i BCRP razmjenjivali. Drugi je primjer predmet *Cooper protiv NCA* [2019] EWCA Civ 16 u kojem je Žalbeni sud (*Court of Appeal*) potvrdio zakonitost razmjene podataka između policije i Agencije za borbu protiv teškog organiziranog kriminala (*Serious Organised Crime Agency*, SOCA), tijela kaznenog progona koje je trenutačno dio Nacionalne agencije za kriminal.

([206]) Članak 36. stavak 4. DPA-a iz 2018.

razmjenjuje podatke s obavještajnom agencijom. U prvom scenariju obrada osobnih podataka bit će obuhvaćena područjem primjene Opće uredbe Ujedinjene Kraljevine o zaštiti podataka te dijela 2. DPA-a iz 2018. Kako je navedeno u odluci koja je donesena na temelju Uredbe (EU) 2016/679, zaštitne mjere koje su predviđene u Općoj uredbi Ujedinjene Kraljevine o zaštiti podataka i dijelu 2. DPA-a iz 2018. pružaju razinu zaštite koja je u osnovi istovjetna onoj koja se pruža u Uniji ([207]).

(127) U drugom scenariju, u kojem je riječ o razmjeni podataka koje je prikupilo tijelo kaznenog progona s obavještajnom agencijom u svrhe nacionalne sigurnosti, pravna osnova koja omogućuje takvu razmjenu je Zakon o borbi protiv terorizma iz 2008. (CTA iz 2008.) ([208]). Na temelju tog zakona sve osobe mogu dati informacije bilo kojoj obavještajnoj službi u svrhu obavljanja bilo koje funkcije te službe, uključujući „nacionalnu sigurnost".

(128) Kad je riječ o uvjetima pod kojima se podaci mogu razmjenjivati u svrhe nacionalne sigurnosti, Zakon o obavještajnim službama i Zakon o sigurnosnim službama ograničavaju mogućnost obavještajnih službi da prikupljaju podatke na ono što je nužno za obavljanje njihovih zakonski propisanih funkcija. Nadležna tijela koja su obuhvaćena područjem primjene dijela 3. DPA-a iz 2018. i koja žele razmjenjivati podatke s obavještajnim službama morat će uzeti u obzir nekoliko čimbenika/ograničenja povrh zakonski propisanih funkcija agencija koje su utvrđene u Zakonu o obavještajnim službama i Zakonu o sigurnosnim službama ([209]). U članku 20. Zakona o borbi protiv terorizma iz 2008. pojašnjava se da sve razmjene podataka na temelju članka 19. tog zakona i dalje moraju biti u skladu sa zakonodavstvom o zaštiti podataka , što znači da se primjenjuju sva ograničenja i zahtjevi iz DPA-a iz 2018. Nadalje, tijela kaznenog progona i obavještajne službe su javna tijela za potrebe Zakona o ljudskim pravima iz 1998., stoga moraju djelovati u skladu s pravima zajamčenima EKLJP-om, uključujući članak 8. EKLJP-a. Drugim riječima, ti zahtjevi znače da sve razmjene podataka između tijela kaznenog progona i obavještajnih službi moraju biti u skladu sa zakonodavstvom o zaštiti podataka i EKLJP-om.

(129) Obrada koju obavještajne službe obavljaju u vezi s osobnim podacima koje prime ili dobiju od tijelâ kaznenog progona u svrhe nacionalne sigurnosti podliježe nizu uvjeta i zaštitnih mjera ([210]). Dio 4. DPA-a iz 2018. primjenjuje se na svu obradu koju vrše obavještajne službe ili koja se vrši u njihovo ime. U njemu se utvrđuju

([207]) Provedbena odluka Komisije na temelju Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj zaštiti osobnih podataka u Ujedinjenoj Kraljevini C(2021)4800.

([208]) Članak 19. Zakona o borbi protiv terorizma iz 2008., dostupno na: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) U članku 2. stavku 2. Zakona o obavještajnim službama iz 1994. (vidjeti https://www.legislation.gov.uk/ukpga/1994/13/contents) navodi se sljedeće: „Načelnik obavještajne službe odgovoran je za učinkovitost te službe i njegova je dužnost osigurati: (a) da su uspostavljeni mehanizmi kojima se osigurava da obavještajna služba prikuplja samo informacije koje su nužne za propisno obavljanje njezinih funkcija i da informacije otkriva samo ako je to nužno: i. u tu svrhu; ii. u interesu nacionalne sigurnosti; iii. u svrhu sprečavanja ili otkrivanja teških kaznenih djela; ili iv. za potrebe kaznenih postupaka; i (b) da obavještajna služba ne poduzima nikakve mjere radi promicanja interesa neke političke stranke u Ujedinjenoj Kraljevini", dok se u članku 2. stavku 2. Zakona o sigurnosnim službama iz 1989. (vidjeti https://www.legislation.gov.uk/ukpga/1989/5/contents) navodi sljedeće: „Glavni direktor odgovoran je za učinkovitost službe i njegova je dužnost osigurati: (a) da su uspostavljeni mehanizmi kojima se osigurava da služba prikuplja samo informacije koje su nužni za propisno obavljanje njezinih funkcija i da ih otkriva samo ako je to nužno u tu svrhu ili u svrhu [sprečavanja ili otkrivanja] teških kaznenih djela [ili za potrebe kaznenih postupaka]; i (b) da služba ne poduzima nikakve mjere radi promicanja interesa neke političke stranke; i (c) da su uspostavljeni mehanizmi, dogovoreni s glavnim direktorom Nacionalne agencije za kriminalitet, za koordinaciju aktivnosti službe usmjerenih na ostvarivanje članka 1. stavka 4. ovog Zakona s aktivnostima policijskih snaga, Nacionalne agencije za kriminal i drugih tijela kaznenog progona".

([210]) Zaštitne mjere za obavještajne službe i ograničenja ovlasti obavještajnih službi uređeni su i Zakonom o istražnim ovlastima iz 2016., koji, zajedno sa Zakonom o regulaciji istražnih ovlasti iz 2000. za Englesku, Wales i Sjevernu Irsku te Zakonom o regulaciji istražnih ovlasti (Škotska) iz 2000. za Škotsku, čini pravnu osnovu za primjenu tih ovlasti. Međutim, te ovlasti nisu relevantne u kontekstu „daljnje razmjene" jer obuhvaćaju izravno prikupljanje osobnih podataka koje obavljaju obavještajne agencije. Za ocjenu ovlasti dodijeljenih obavještajnim agencijama na temelju Zakona o istražnim ovlastima vidjeti Provedbenu odluku Komisije na temelju Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća o primjerenoj zaštiti osobnih podataka u Ujedinjenoj Kraljevini C(2021)4800.

glavna načela zaštite podataka (zakonitost, poštenost i transparentnost ([211]), ograničavanje svrhe ([212]), smanjenje količine podataka ([213]), točnost ([214]), ograničenje pohrane ([215]) i sigurnost ([216])), uvode se uvjeti za obradu posebnih kategorija podataka ([217]), predviđaju se prava ispitanika ([218]), zahtijeva se tehnička zaštita podataka ([219]) i uređuju se međunarodni prijenosi osobnih podataka ([220]).

(130) Isto tako, u članku 110. DPA-a iz 2018. predviđa se izuzeće od određenih odredbi iz dijela 4. DPA-a iz 2018. kad je to izuzeće potrebno radi zaštite nacionalne sigurnosti. U članku 110. stavku 2. DPA-a iz 2018. navedene su odredbe od kojih je dopušteno izuzeće. One uključuju načela zaštite podataka (osim načela zakonitosti), prava ispitanika, obvezu obavješćivanja povjerenika za informiranje o povredi podataka, ovlasti povjerenika za informiranje povezane s inspekcijom u skladu s međunarodnim obvezama, određene izvršne ovlasti povjerenika za informiranje, odredbe prema kojima su određena kršenja zaštite podataka kazneno djelo i odredbe o posebnim svrhama obrade kao što su novinarske, akademske ili umjetničke svrhe. Na to se izuzeće može pozvati na temelju analize za svaki pojedinačni slučaj ([221]). Kako su objasnila tijela Ujedinjene Kraljevine i kako potvrđuje sudska praksa sudova u Ujedinjenoj Kraljevini, „(a) voditelj obrade mora uzeti u obzir stvarne posljedice za nacionalnu sigurnost ili obranu ako bi morao poštovati određenu odredbu o zaštiti podataka i može li opravdano poštovati uobičajeno pravilo bez utjecaja na nacionalnu sigurnost ili obranu” ([222]). ICO nadzire je li izuzeće primijenjeno na odgovarajući način ([223]).

([211]) Prema članku 86. stavku 6. DPA-a iz 2018. kako bi se utvrdila poštenost i transparentnost obrade, u obzir se mora uzeti metoda kojom su podaci dobiveni. U tom je smislu zahtjev za poštenost i transparentnost ispunjen ako su podaci dobiveni od osobe koja je zakonito ovlaštena ili dužna dostaviti te podatke.

([212]) Prema članku 87. DPA-a iz 2018. svrhe obrade moraju biti posebne, izričite i zakonite. Podaci se ne smiju obrađivati na način koji nije u skladu sa svrhama u koje su prikupljeni. Prema članku 87. stavku 3. daljnja usklađena obrada osobnih podataka dopuštena je samo ako je voditelj obrade zakonski ovlašten obrađivati podatke u tu svrhu i ako je obrada nužna i proporcionalna toj drugoj svrsi. Obradu bi trebalo smatrati usklađenom ako se obavlja u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe i ako se na nju primjenjuju odgovarajuće zaštitne mjere (članak 87. stavak 4. DPA-a iz 2018.).

([213]) Osobni podaci moraju biti primjereni, relevantni i ne smiju biti pretjerani (članak 88. DPA-a iz 2018.).

([214]) Osobni podaci moraju biti točni i ažurirani (članak 89. DPA-a iz 2018.).

([215]) Osobni podaci moraju se čuvati samo onoliko dugo koliko je potrebno (članak 90. DPA-a iz 2018.).

([216]) Šesto načelo zaštite podataka nalaže da se osobni podaci moraju obrađivati na način koji uključuje poduzimanje odgovarajućih sigurnosnih mjera za rizike koji proizlaze iz obrade osobnih podataka. Ti rizici uključuju (ali nisu ograničeni na) slučajan ili neovlašten pristup osobnim podacima ili njihovo uništavanje, gubitak, uporabu, izmjenu ili otkrivanje (članak 91. DPA-a iz 2018.). U članku 107. zahtijeva se i sljedeće: 1. svaki voditelj obrade mora provesti odgovarajuće sigurnosne mjere koje odgovaraju rizicima koji proizlaze iz obrade osobnih podataka; i 2. u slučaju automatizirane obrade svaki voditelj obrade i izvršitelj obrade mora provesti preventivne mjere ili mjere ublažavanja na temelju procjene rizika.

([217]) Članak 86. stavak 2. točka (b) DPA-a iz 2018. i Prilog 10. DPA-u iz 2018.

([218]) Dio 4. poglavlje 3. DPA-a iz 2018., osobito: pravo na pristup, ispravak i brisanje, pravo na ulaganje prigovora na obradu i pravo ispitanika da ne podliježe automatiziranom donošenju odluka, pravo na intervenciju u automatizirano donošenje odluka i pravo na obavijest o donošenju odluka. Osim toga, voditelj obrade mora ispitaniku dati informacije o obradi njegovih osobnih podataka.

([219]) Članak 103. DPA-a iz 2018.

([220]) Članak 109. DPA-a iz 2018. Prijenosi osobnih podataka međunarodnim organizacijama ili zemljama izvan Ujedinjene Kraljevine mogući su ako je prijenos nužna i proporcionalna mjera koja se provodi u svrhe zakonom propisanih funkcija voditelja obrade ili u drugu svrhu predviđenu u određenim člancima Zakona o sigurnosnim službama iz 1989. i Zakona o obavještajnim službama iz 1994.

([221]) Vidjeti predmet *Baker protiv ministra unutarnjih poslova* [2001] UKIT NSA2 („*Baker protiv ministra u Vladi*”).

([222]) Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Okvir za zaštitu podataka i istražne ovlasti s obzirom na nacionalnu sigurnost, str. 15.–16., dostupno na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.. Vidjeti i predmet *Baker protiv ministra u Vladi* (vidjeti prethodnu bilješku 220), u kojem je Sud ukinuo potvrdu o nacionalnoj sigurnosti koju je izdao ministar unutarnjih poslova (*Home Secretary*) i koja potvrđuje primjenu iznimke radi nacionalne sigurnosti jer je smatrao da nije postojao razlog za opću iznimku od obveze odgovora na zahtjeve za pristup podacima te da dopuštanje takve iznimke u svim okolnostima bez pojedinačne analize svakog slučaja premašuje ono što je nužno i proporcionalno za zaštitu nacionalne sigurnosti.

([223]) Vidjeti Memorandum o razumijevanju između ICO-a i obavještajne zajednice Ujedinjene Kraljevine u kojem je navedeno sljedeće: „Po zaprimanju pritužbe ispitanika ICO se treba uvjeriti da je pitanje pravilno riješeno i, prema potrebi, da su sva izuzeća primijenjena na odgovarajući način.” (Memorandum o razumijevanju između Ureda povjerenika za informiranje i obavještajne zajednice Ujedinjene Kraljevine, točka 16., dostupan na: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Nadalje, u odnosu na mogućnost ograničavanja bilo kojeg od prethodno navedenih prava radi zaštite „nacionalne sigurnosti", u članku 79. DPA-a iz 2018. predviđa se mogućnost da voditelj obrade podnese zahtjev za potvrdu koju potpisuje ministar koji je član kabineta ili glavni krunski odvjetnik (*Attorney General*), kojom se potvrđuje da je ograničenje tih prava sad, ili je u nekom trenutku bilo, nužna i proporcionalna mjera za zaštitu nacionalne sigurnosti ([224]). Vlada Ujedinjene Kraljevine objavila je smjernice o potvrdama o nacionalnoj sigurnosti na temelju DPA-a iz 2018., u kojima je osobito istaknuto da svako ograničavanje prava ispitanika radi zaštite nacionalne sigurnosti mora biti proporcionalno i nužno ([225]). Sve potvrde o nacionalnoj sigurnosti moraju se objaviti na internetskim stranicama ICO-a ([226]).

(132) Potvrda bi trebala imati ograničeno trajanje koje nije dulje od pet godina kako bi je izvršna vlast redovito preispitivala ([227]). U potvrdi se navode osobni podaci ili kategorije osobnih podataka na koje se izuzeće primjenjuje i odredbe iz DPA-a iz 2018. na koje se izuzeće primjenjuje ([228]).

(133) Važno je napomenuti da potvrde o nacionalnoj sigurnosti ne pružaju dodatnu osnovu za ograničavanje pravâ na zaštitu podataka iz razlogâ nacionalne sigurnosti. Drugim riječima, voditelj obrade ili izvršitelj obrade može se pozvati na potvrdu samo ako je zaključio da je nužno pozvati se na izuzeće radi nacionalne sigurnosti, koje se mora primjenjivati na pojedinačnoj osnovi. Čak i ako se potvrda o nacionalnoj sigurnosti primjenjuje na predmetno pitanje, ICO može istražiti je li pozivanje na izuzeće radi nacionalne sigurnosti bilo opravdano u konkretnom slučaju ([229]).

(134) Sve osobe na koje izdavanje potvrde izravno utječe mogu podnijeti žalbu Višem sudu ([230]) protiv potvrde ([231]) ili, ako su u potvrdi podaci identificirani općenitim opisom, osporiti primjenu potvrde na konkretne podatke ([232]).

(135) Sud će preispitati odluku o izdavanju potvrde i odlučiti jesu li postojali opravdani razlozi za izdavanje potvrde ([233]). Može razmotriti širok raspon pitanja, uključujući nužnost, proporcionalnost i zakonitost, a pritom mora uzeti u obzir učinak na prava ispitanika i uspostaviti ravnotežu s potrebom zaštite nacionalne sigurnosti. Stoga sud može utvrditi da se potvrda ne primjenjuje na konkretne osobne podatke koji su predmet žalbe ([234]).

([224]) DPA-om iz 2018. ukinuta je mogućnost izdavanja te potvrde na temelju članka 28. stavka 2. Zakona o zaštiti podataka iz 1998. Međutim, mogućnost izdavanja „starih potvrda" i dalje postoji ako se osporava neki postupak iz prošlosti koji se temelji na Zakonu iz 1998. (vidjeti dio 5. točku 17. Priloga 20. DPA-u iz 2018.). Međutim, čini se da je ta mogućnost vrlo rijetka i primjenjivat će se samo u ograničenom broju slučajeva, primjerice ako ispitanik pokrene spor o primjeni izuzeća na temelju nacionalne sigurnosti u odnosu na obradu koju je provelo tijelo javne vlasti na temelju Zakona iz 1998. Treba napomenuti da će se u tim slučajevima članak 28. DPA-a iz 1998. primjenjivati u cijelosti, uključujući stoga i mogućnost ispitanika da osporava potvrdu. Trenutačno ne postoji nijedna potvrda o nacionalnoj sigurnosti izdana na temelju DPA-a iz 1998.

([225]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti na temelju Zakona o zaštiti podataka iz 2018., dostupne na: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

([226]) U skladu s člankom 130. DPA-a iz 2018. ICO može odlučiti ne objaviti tekst ili dio teksta potvrde ako bi to bilo suprotno interesu nacionalne sigurnosti ili ako bi bilo suprotno javnom interesu ili bi se time mogla ugroziti sigurnost neke osobe. Međutim, u tim će slučajevima ICO objaviti činjenicu da je potvrda izdana.

([227]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, točka 15., vidjeti bilješku 225.

([228]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, točka 5., vidjeti bilješku 225.

([229]) U članku 102. DPA-a iz 2018. zahtijeva se da voditelj obrade može dokazati da je poštovao DPA-u iz 2018. To znači da bi obavještajna služba trebala ICO-u dokazati da je pri pozivanju na izuzeće uzela u obzir posebne okolnosti slučaja. ICO objavljuje i evidenciju potvrda o nacionalnoj sigurnosti, koja je dostupna na: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Viši sud nadležan je za žalbe protiv odluka nižih upravnih sudova, a posebno je nadležan za izravne žalbe protiv odluka određenih vladinih tijela.

([231]) Članak 111. stavak 3. DPA-a iz 2018.

([232]) Članak 111. stavak 5. DPA-a iz 2018.

([233]) U predmetu *Baker protiv ministra u Vladi* (vidjeti bilješku 221.) Sud za informacije ukinuo je potvrdu o nacionalnoj sigurnosti koju je izdao ministar unutarnjih poslova jer je Sud smatrao da nije postojao razlog za opću iznimku od obveze odgovora na zahtjeve za pristup podacima te da dopuštanje takve iznimke u svim okolnostima bez analize za svaki pojedinačni slučaj premašuje ono što je nužno i proporcionalno za zaštitu nacionalne sigurnosti.

([234]) Smjernice Vlade Ujedinjene Kraljevine o potvrdama o nacionalnoj sigurnosti, točka 25., vidjeti bilješku 225.

(136) Drugi skup mogućih ograničenja odnosi se na ona koja se primjenjuju, na temelju Priloga 11. DPA-u iz 2018., na određene odredbe iz dijela 4. DPA-a iz 2018. ([235]) radi zaštite drugih važnih ciljeva od općeg javnog interesa ili zaštićenih interesa kao što su parlamentarni imunitet, odvjetnička tajna, vođenje sudskog postupka ili bojna pripravnost oružanih snaga. Primjena tih odredbi izuzeta je za određene kategorije informacija („izuzeća na temelju razreda") ili je izuzeta u mjeri u kojoj bi primjena tih odredbi vjerojatno dovela u pitanje zaštićeni interes („izuzeća na temelju ugrožavanja") ([236]). Na izuzeća na temelju ugrožavanja moguće je pozvati se samo ako bi primjena navedenih odredbi o zaštiti podataka vjerojatno dovela u pitanje predmetni posebni interes. Stoga primjena izuzeća uvijek mora biti opravdana upućivanjem na relevantno ugrožavanje do kojeg bi vjerojatno došlo u pojedinačnom slučaju. Na izuzeća na temelju razreda moguće je pozvati se samo u pogledu posebne, usko definirane kategorije informacija za koju je odobreno izuzeće. Ona su prema svrsi i učinku slična određenim izuzećima od Opće uredbe Ujedinjene Kraljevine o zaštiti podataka (na temelju Priloga 2. DPA-u iz 2018.), koja odražavaju izuzeća predviđena člankom 23. Opće uredbe o zaštiti podataka.

(137) Iz prethodno navedenog proizlazi da su u primjenjivim pravnim odredbama Ujedinjene Kraljevine, kako su ih tumačili i sudovi i povjerenik za informiranje, uspostavljena ograničenja i uvjeti koji osiguravaju da ta izuzeća i ograničenja ostanu u granicama onog što je nužno i proporcionalno za zaštitu nacionalne sigurnosti.

(138) Obradu osobnih podataka koju obavljaju obavještajne službe na temelju dijela 4. DPA-a iz 2018. nadzire povjerenik za informiranje ([237]).

(139) Opće funkcije povjerenika za informiranje u pogledu obrade osobnih podataka koju obavljaju obavještajne službe na temelju dijela 4. DPA-a iz 2018. utvrđene su u Prilogu 13. DPA-u iz 2018. Te zadaće ponajprije obuhvaćaju, ali nisu ograničene na, praćenje i provedbu dijela 4. DPA-a iz 2018., promicanje javne svijesti, savjetovanje Parlamenta, vlade i drugih institucija o zakonodavnim i upravnim mjerama, informiranje voditelja obrade i izvršitelja obrade o njihovim obvezama, davanje informacija ispitanicima o ostvarivanju njihovih prava i provođenje istraga.

(140) Povjerenik je, kao i za dio 3. DPA-a iz 2018., ovlašten obavijestiti voditelje obrade o navodnom kršenju pravila te izdavati upozorenja o tome da će se obradom vjerojatno prekršiti pravila i izdavati opomene u slučaju potvrde kršenja pravila. Može izdavati i zahtjeve za izvršenje i rješenja o kazni zbog kršenja određene odredbe zakona ([238]). Međutim, za razliku od situacije s drugim dijelovima DPA-a iz 2018., povjerenik ne može izdati zahtjev za provjeru nacionalnom sigurnosnom tijelu ([239]).

(141) Nadalje, u članku 110. DPA-a iz 2018. predviđa se iznimka od primjene određenih ovlasti povjerenika kad je to potrebno radi zaštite nacionalne sigurnosti. To uključuje ovlast povjerenika da izdaje zahtjeve i rješenja (bilo koje vrste) na temelju DPA-a (zahtjevi za dostavu informacija, provjeru i izvršenje te rješenja o kazni), ovlast provođenja

([235]) To uključuje: i. načela zaštite podataka iz dijela 4., osim zahtjeva za zakonitost obrade na temelju prvog načela i činjenice da obrada mora ispunjavati jedan od relevantnih uvjeta utvrđenih u prilozima 9. i 10.; ii. prava ispitanika; i iii. dužnosti povezane s prijavljivanjem povreda ICO-u.

([236]) Prema Okviru za objašnjenja Ujedinjene Kraljevine izuzeća „na temelju razreda" su sljedeća: i. informacije o dodjeli časti i odličja Krune; ii. odvjetnička tajna; iii. povjerljivi podaci o zaposlenju, osposobljavanju ili obrazovanju; i iv. ispitni radovi i ocjene. Izuzeća „na temelju ugrožavanja" odnose se na sljedeća pitanja: i. sprečavanje ili otkrivanje kaznenog djela; uhićenje i kazneni progon počiniteljâ; ii. parlamentarni imunitet; iii. sudski postupak; iv. bojnu pripravnost oružanih snaga Krune; v. gospodarsku dobrobit Ujedinjene Kraljevine; vi. pregovore s ispitanikom; vii. znanstveno ili povijesno istraživanje ili statističke svrhe; viii. arhiviranje u javnom interesu. Okvir za objašnjenja za rasprave o primjerenosti Ujedinjene Kraljevine, odjeljak H: Nacionalna sigurnost, str. 13., vidjeti bilješku 222.

([237]) Članak 116. DPA-a iz 2018.

([238]) U skladu sa zajedničkim tumačenjem članka 149. stavka 2. i članka 155. DPA-a iz 2018. voditelju obrade ili izvršitelju obrade mogu se izdati zahtjevi za izvršenje i rješenja o kazni u vezi s kršenjima dijela 4. poglavlja 2. DPA-a iz 2018. (načela obrade), odredbe iz dijela 4. DPA-a iz 2018. o davanju prava ispitaniku, zahtjeva za obavještavanje povjerenika o povredama osobnih podataka na temelju članka 108. DPA-a iz 2018. i načelâ za prijenos osobnih podataka trećim zemljama, državama koje nisu potpisnice Konvencije i međunarodnim organizacijama iz članka 109. DPA-a iz 2018. (Za dodatne pojedinosti o zahtjevu za izvršenje i rješenju o kazni vidjeti uvodne izjave od (102). do (103).).

([239]) U skladu s člankom 147. stavkom 6. DPA-a iz 2018. povjerenik za informiranje ne smije izdati zahtjev za provjeru tijelu iz članka 23. stavka 3. Zakona o slobodi informiranja iz 2000. To uključuje Sigurnosnu službu (MI5), Tajnu obavještajnu službu (MI6) i Vladin komunikacijski stožer.

inspekcija u skladu s međunarodnim obvezama, ovlasti ulaska i inspekcije te pravila o kaznenim djelima ([240]). Kako je objašnjeno u uvodnoj izjavi (136)., te će se iznimke primjenjivati samo ako je to nužno i proporcionalno te na pojedinačnoj osnovi. Primjena tih iznimaka može podlijegati sudskom preispitivanju ([241]).

(142) ICO i obavještajne službe Ujedinjene Kraljevine potpisale su Memorandum o razumijevanju ([242]) kojim se uspostavlja okvir za suradnju u brojnim pitanjima, uključujući obavijesti o povredi podataka i postupanje s pritužbama ispitanika. Konkretno, njime se predviđa da će ICO nakon zaprimanja pritužbe provjeriti je li neko pozivanje na izuzeće radi nacionalne sigurnosti primijenjeno na odgovarajući način. Odgovore na upite ICO-a u kontekstu ispitivanja pojedinačnih pritužbi predmetna obavještajna agencija mora dati u roku od 20 radnih dana, koristeći odgovarajuće sigurne kanale ako odgovori uključuju klasificirane podatke. Od travnja 2018. do danas ICO je zaprimio 21 pritužbu koju su podnijeli pojedinci u pogledu rada obavještajnih službi. Svaka je pritužba provjerena, a ispitanik obaviješten o ishodu provjere ([243]).

(143) Nadalje, parlamentarni nadzor nad obradom podataka koju obavljaju obavještajne agencije vrši Odbor za obavještajne poslove i sigurnost (ISC). Zakonska je osnova za taj odbor Zakon o pravosuđu i sigurnosti iz 2013. (JSA iz 2013.) ([244]). Tim se zakonom osniva ISC kao odbor Parlamenta Ujedinjene Kraljevine. ISC se sastoji od članova koji pripadaju obama domovima Parlamenta, a imenuje ih predsjednik Vlade nakon savjetovanja s čelnikom oporbe ([245]). ISC je obvezan podnositi godišnje izvješće Parlamentu o obavljanju svojih funkcija i druga izvješća koja smatra primjerenima ([246]).

(144) Od 2013. ISC je dobio veće ovlasti, uključujući nadzor operativnih aktivnosti sigurnosnih službi. U skladu s člankom 2. JSA-e iz 2013. ISC ima zadaću nadzirati rashode, upravljanje, politiku i operacije nacionalnih sigurnosnih agencija. U JSA-i iz 2013. propisuje se da ISC može provoditi istrage o operativnim pitanjima ako se

([240]) Mogu se izuzeti sljedeće odredbe: članak 108. (obavješćivanje povjerenika o povredi osobnih podataka), članak 119. (inspekcija u skladu s međunarodnim obvezama); članci od 142. do 154. i Prilog 15. (zahtjevi i rješenja te ovlasti povjerenika za ulazak i inspekciju); članci od 170. do 173. (kažnjiva djela povezana s osobnim podacima). Osim toga, u pogledu obrade koju obavljaju obavještajne službe u Prilogu 13. (ostale opće funkcije povjerenika), točki 1. podtočkama (a) i (g) i točki 2.

([241]) Vidjeti, primjerice, predmet *Baker protiv ministra unutarnjih poslova* (vidjeti bilješku 221.).

([242]) Memorandum o razumijevanju između ICO-a i obavještajne zajednice Ujedinjene Kraljevine, vidjeti bilješku 231.

([243]) U sedam od tih slučajeva ICO je savjetovao podnositelju pritužbe da se u vezi sa svojim prigovorom obrati voditelju obrade podataka (to je slučaj kad je pojedinac iznio prigovor ICO-u, a trebao se prvo obratiti voditelju obrade podataka), u jednom od tih slučajeva ICO je dao općenite savjete voditelju obrade podataka (to se primjenjuje kad se čini da voditelj obrade nije svojim postupcima prekršio zakonodavstvo, ali se poboljšanjem prakse moglo izbjeći podnošenje prigovora ICO-u), a u preostalih 13 slučajeva nije bilo potrebno da voditelj obrade podataka poduzme ikakve mjere (to se primjenjuje ako pojedinac iznese prigovore koji su obuhvaćeni Zakonom o zaštiti podataka iz 2018. jer se odnose na obradu osobnih podataka, ali na temelju dostavljenih informacija čini se da voditelj obrade nije prekršio zakonodavstvo).

([244]) Kako su objasnila tijela Ujedinjene Kraljevine, JSA-om je proširena nadležnost ISC-a kako bi se uključila funkcija nadzora obavještajne zajednice povrh triju glavnih agencija te omogućio naknadni nadzor operativnih aktivnosti agencija u pitanjima od velikog nacionalnog interesa.

([245]) Članak 1. JSA-a iz 2013. Ministri ne mogu biti imenovani za članove ISC-a. Članovi zadržavaju svoje mjesto u ISC-u dok traje mandat Parlamenta za vrijeme kojeg su imenovani. Može ih se razriješiti dužnosti odlukom doma koji ih je imenovao ili ako prestanu biti zastupnici u Parlamentu ili postanu ministri. Član može i podnijeti ostavku.

([246]) Izvješća i izjave Odbora dostupni su na: http://isc.independent.gov.uk/committee-reports. ISC je 2015. objavio izvješće pod nazivom *Privacy and Security: A modern and transparent legal framework* (Privatnost i sigurnost: moderan i transparentan pravni okvir) (vidjeti: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf) u kojem je razmatrao pravni okvir za tehnike nadzora koje koriste obavještajne agencije i izdao niz preporuka koje su potom uzete u obzir i uključene u nacrt Prijedloga zakona o istražnim ovlastima koji je kasnije postao zakon – Zakon o istražnim ovlastima iz 2016. (IPA). Odgovor Vlade na to izvješće o privatnosti i sigurnosti dostupan je na: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

ona ne odnose na operacije koje su u tijeku ([247]). U Memorandumu o razumijevanju koji su sklopili predsjednik Vlade i ISC ([248]) detaljno se navode elementi koje treba uzeti u obzir pri utvrđivanju je li određena aktivnost dio operacije koja je u tijeku ([249]). Predsjednik Vlade može od ISC-a zatražiti i da istraži operacije koje su u tijeku te ISC može pregledavati informacije koje mu agencije dobrovoljno dostave.

(145) U skladu s Prilogom 1. JSA-i iz 2013. ISC može od voditelja bilo koje od triju obavještajnih službi zatražiti da otkrije bilo koju informaciju. Agencija mora te informacije staviti na raspolaganje, osim ako ministar to ne zabrani ([250]). Tijela Ujedinjene Kraljevine objasnila su da se u praksi ISC-u uskraćuje vrlo malo informacija ([251]).

(146) Kad je riječ o pravnoj zaštiti, kao prvo, u skladu s člankom 165. stavkom 2. DPA-a iz 2018. ispitanik može podnijeti pritužbu ICO-u ako smatra da je u vezi s osobnim podacima koji se na njega odnose došlo do kršenja dijela 4. DPA-a iz 2018., uključujući svaku zloupotrebu odstupanja i ograničenja povezanih s nacionalnom sigurnošću.

(147) Nadalje, na temelju dijela 4. DPA-a iz 2018. pojedinci imaju pravo obratiti se Visokom sudu (ili Vrhovnom građanskom sudu u Škotskoj (*Court of Session*)) da izda nalog kojim se od voditelja obrade zahtijeva da poštuje prava na pristup podacima ([252]), podnošenje prigovora na obradu ([253]) te ispravak ili brisanje podataka.

(148) Pojedinci imaju pravo i na naknadu pretrpljene štete zbog kršenja zahtjeva iz dijela 4. DPA-a iz 2018. koju isplaćuje voditelj obrade ili izvršitelj obrade ([254]). Šteta obuhvaća i financijski gubitak i štetu koja ne uključuje financijski gubitak, kao što je pretrpljena duševna bol ([255]).

(149) Naposljetku, pojedinac može podnijeti pritužbu Sudu za istražne ovlasti za svaki postupak koji su provele obavještajne agencije Ujedinjene Kraljevine ili je proveden u njihovo ime ([256]). Sud za istražne ovlasti osnovan je Zakonom o regulaciji istražnih ovlasti iz 2000. za Englesku, Wales i Sjevernu Irsku te Zakonom o regulaciji istražnih ovlasti (Škotska) iz 2000. za Škotsku (RIPA iz 2000.) i neovisan je od izvršne vlasti ([257]). U skladu s člankom 65. RIPA-e iz 2000. članove Suda za istražne ovlasti imenuje Njezino Veličanstvo na razdoblje od pet godina.

(150) Njezino Veličanstvo može člana tog suda razriješiti dužnosti na molbu ([258]) obaju domova Parlamenta ([259]).

(151) Za pokretanje postupka pred Sudom za istražne ovlasti („zahtjev u pogledu procesne legitimacije"), u skladu s člankom 65. RIPA-e iz 2000. pojedinac mora biti uvjeren: i. da se postupak obavještajne službe odnosio na njega, bilo koju njegovu imovinu, bilo koju komunikaciju koju je poslao ili koja mu je poslana ili koja mu je bila namijenjena ili na njegovo korištenje bilo koje poštanske usluge, telekomunikacijske usluge ili telekomunikacijskog sustava ([260]); i ii. da je

([247]) Članak 2. JSA-a iz 2013.
([248]) Memorandum o razumijevanju između predsjednika Vlade i ISC-a, dostupan na: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) Memorandum o razumijevanju između predsjednika Vlade i ISC-a, točka 14., vidjeti bilješku 248.
([250]) Ministar može zabraniti otkrivanje informacija samo na temelju dvaju razloga: informacije su osjetljive i ne smiju se otkriti ISC-u u interesu nacionalne sigurnosti; ili su informacije takve prirode da bi ministar, ako bi se od njega zatražilo da dostavi te informacije posebnom resornom odboru Zastupničkog doma, smatrao (zbog razloga koji nisu ograničeni na nacionalnu sigurnost) da nije primjereno da to učini. (točka 4. podtočka 2. Priloga 1. JSA-i iz 2013.).
([251]) Okvir za objašnjenja Ujedinjene Kraljevine – odjeljak H: Nacionalna sigurnost, str. 43.
([252]) Članak 94. stavak 11. DPA-a iz 2018.
([253]) Članak 99. stavak 4. DPA-a iz 2018.
([254]) Članak 169. DPA-a iz 2018., kojim se dopušta da „osoba koja trpi štetu zbog kršenja zahtjeva iz zakonodavstva o zaštiti podataka" podnese zahtjev za naknadu štete.
([255]) Članak 169. stavak 5. DPA-a iz 2018.
([256]) Vidjeti članak 65. stavak 2. točku (b) RIPA-e.
([257]) Prema Prilogu 3. RIPA-i iz 2000. članovi Suda moraju imati utvrđeno pravosudno iskustvo i mogu biti ponovno imenovani.
([258]) Više o pojmu „molba" (*address*) vidjeti u bilješci 183.
([259]) Točka 1. podtočka 5. Priloga 3. RIPA-i iz 2000.
([260]) Članak 65. stavak 4. RIPA-e iz 2000.

postupak proveden u „okolnostima koje se mogu osporavati” ([261]) ili „da su ga provele obavještajne službe ili je izvršen u njihovo ime” ([262]). Budući da se posebno taj standard „uvjerenja” prilično široko tumači ([263]), pokretanje postupka pred Sudom podliježe relativno niskim zahtjevima u pogledu procesne legitimacije.

(152) Ako Sud za istražne ovlasti razmatra pritužbu koja mu je podnesena, dužnost mu je istražiti jesu li osobe protiv kojih se iznosi bilo kakva tvrdnja u pritužbi bile u nekoj vrsti odnosa s podnositeljem pritužbe, kao i provesti istragu o tijelu koje je navodno počinilo kršenje te o tome je li navodni postupak počinjen ([264]). Sud u svakom postupku koji vodi mora primijeniti ista načela za donošenje odluka u tim postupcima koje bi primjenjivao opći sud u slučaju zahtjeva za sudsko preispitivanje ([265]).

(153) Sud za istražne ovlasti mora obavijestiti podnositelja pritužbe o tome je li donesena odluka u njegovu korist ili nije ([266]). Na temelju članka 67. stavaka 6. i 7. RIPA-e iz 2000. Sud ima ovlast izdavati privremene odluke i dodjeljivati naknadu štete ili druge naloge koji smatra primjerenima ([267]). Na temelju članka 67.A RIPA-e iz 2000. na odluku Suda može se podnijeti žalba podložno dopuštenju koje dodjeljuje Sud ili mjerodavni žalbeni sud.

(154) Konkretno, pojedinci mogu podnijeti tužbeni zahtjev – i dobiti sudsku zaštitu – pred Sudom za istražne ovlasti u slučaju da smatraju da je tijelo javne vlasti djelovalo (ili namjerava djelovati) na način koji je nespojiv s pravima iz EKLJP-a, uključujući pravo na privatnost i zaštitu podataka, i stoga je nezakonit na temelju članka 6. stavka 1. Zakona o ljudskim pravima iz 1998. Sudu za istražne ovlasti dodijeljena je isključiva nadležnost za sve zahtjeve na temelju Zakona o ljudskim pravima povezane s obavještajnim agencijama. To znači, kako je istaknuo Visoki sud, da „utvrđivanje postojanja kršenja Zakona o ljudskim pravima na temelju činjenica pojedinog slučaja u načelu je nešto što razmatra i o čemu odlučuje neovisni sud koji ima pravo na pristup svim relevantnim materijalima, uključujući tajni materijal. […] U tom kontekstu treba voditi računa i o tome da sad i odluke samog Suda za istražne ovlasti podliježu mogućnosti žalbe mjerodavnom žalbenom sudu (u Engleskoj i Walesu to bi bio Žalbeni sud); i da je Vrhovni sud nedavno odlučio da je Sud za istražne ovlasti u načelu podložan sudskom preispitivanju: vidjeti predmet *R (Privacy International) protiv Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219” ([268]). Ako Sud za istražne ovlasti utvrdi da je neka radnja tijela javne vlasti nezakonita, može u okviru svojih ovlasti odobriti mjeru ili pravni lijek, ili izdati nalog, kako smatra da je pravedno i primjereno ([269]).

([261]) Takve okolnosti odnose se na postupke tijela javne vlasti s ovlaštenjem (npr. nalog, odobrenje/zahtjev za pribavljanje komunikacija itd.) ili ako su okolnosti takve (bez obzira na to postoji li takvo ovlaštenje) da ne bi bilo primjereno da se postupak provodi bez ovlaštenja ili da se prethodno barem ne razmotri bi li trebalo zatražiti takvo ovlaštenje. Smatra se da su se postupci koje je odobrio pravosudni povjerenik dogodili u okolnostima koje se mogu osporavati (članak 65. stavak 7.ZA RIPA-e iz 2000.), dok se za druge postupke koji se provode uz dozvolu osobe koja obavlja sudačku dužnost smatra da se nisu dogodili u okolnostima koje se mogu osporavati (članak 65. stavci 7. i 8. RIPA-e iz 2000.).

([262]) Prema informacijama koje su dostavila tijela Ujedinjene Kraljevine, nizak prag za podnošenje pritužbe dovodi do toga da nije neuobičajeno da se u istrazi Suda utvrdi da podnositelj pritužbe doista nije nikad bio predmet istrage tijela javne vlasti. U posljednjem statističkom izvješću Suda za istražne ovlasti navodi se da je Sud 2016. zaprimio 209 pritužbi, od čega se 52 % njih smatralo neutemeljenima ili zlonamjernima, a 25 % njih zaključeno je „bez odluke”. Tijela Ujedinjene Kraljevine objasnila su da to znači da se u odnosu na podnositelja pritužbe ne upotrebljavaju tajne aktivnosti/ovlasti ili da su korištene tajne tehnike, ali je Sud utvrdio da je aktivnost zakonita. Osim toga, 11 % pritužbi odbačeno je zbog nenadležnosti Suda ili su povučene ili proglašene nevažećima, 5 % ih je odbačeno zbog isteka roka, a u 7 % pritužbi odlučeno je u korist podnositelja pritužbe. Statističko izvješće Suda za istražne ovlasti za 2016. dostupno je na: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) Vidjeti predmet *Human Rights Watch protiv ministra u Vladi* [2016] UKIPTrib15_165-CH. U tom je predmetu Sud za istražne ovlasti, pozivajući se na sudsku praksu Europskog suda za ljudska prava, odgovarajućom provjerom uvjerenja smatrao utvrđivanje postoji li bilo kakva osnova za uvjerenje da je određeni postupak obuhvaćen člankom 68. stavkom 5. RIPA-e iz 2000. provela neka obavještajna služba ili da je proveden u njezino ime, uključujući činjenicu da pojedinac može tvrditi da je žrtva kršenja do kojeg dolazi zbog samog postojanja tajnih mjera ili zakonodavstva kojim se omogućuju tajne mjere samo ako može dokazati da je zbog svoje osobne situacije mogao biti izložen opasnosti od toga da bude podvrgnut takvim mjerama (vidjeti predmet *Human Rights Watch protiv ministra u Vladi*, točku 41.).

([264]) Članak 67. stavak 3. RIPA-e iz 2000.

([265]) Članak 67. stavak 2. RIPA-e iz 2000.

([266]) Članak 68. stavak 4. RIPA-e iz 2000.

([267]) To može uključivati odluku kojom se zahtijeva uništenje bilo koje evidencije informacija koju drži bilo koje tijelo javne vlasti u vezi s bilo kojom osobom.

([268]) Visoki sud (*High Court of Justice*), predmet *Liberty* [2019] EWHC 2057 (Admin), točka 170.

([269]) Članak 8. stavak 1. Zakona o ljudskim pravima iz 1998.

(155) Nakon što iscrpi sve nacionalne pravne lijekove, pojedinac može dobiti sudsku zaštitu pred Europskim sudom za ljudska prava za povrede prava zajamčenih EKLJP-om, uključujući pravo na privatnost i zaštitu podataka.

(156) Iz prethodno navedenog proizlazi da se razmjena podataka koje tijela kaznenog progona Ujedinjene Kraljevine na temelju ove Odluke prenose drugim tijelima javne vlasti, uključujući obavještajne agencije, odvija u okviru ograničenja i uvjeta koji osiguravaju da će takva daljnja razmjena biti nužna i proporcionalna i podlijegati posebnim zaštitnim mjerama za zaštitu podataka na temelju DPA-a iz 2018. Nadalje, obradu podataka koju obavljaju predmetna javna tijela nadziru neovisna tijela, a pojedinci na koje to utječe imaju pristup učinkovitim sudskim pravnim lijekovima.

3. ZAKLJUČAK

(157) Komisija smatra da dio 3. DPA-a iz 2018. osigurava razinu zaštite osobnih podataka koje nadležna tijela iz Unije prenose nadležnim tijelima u Ujedinjenoj Kraljevini u svrhe kaznenog progona koja je u osnovi istovjetna onoj koja se jamči Direktivom (EU) 2016/680.

(158) Nadalje, Komisija smatra da, u cjelini, nadzorni mehanizmi i mogućnosti za sudsku zaštitu u pravu Ujedinjene Kraljevine omogućavaju da se u praksi utvrde i sankcioniraju povrede te ispitaniku pružaju pravne lijekove za dobivanje pristupa osobnim podacima koji se odnose na njega te, konačno, za ispravak ili brisanje takvih podataka.

(159) Konačno, na temelju dostupnih informacija o pravnom poretku Ujedinjene Kraljevine Komisija smatra da će se svako zadiranje u temeljna prava pojedinaca čije osobne podatke iz Europske unije u Ujedinjenu Kraljevinu prenose tijela javne vlasti Ujedinjene Kraljevine za potrebe javnog interesa, među ostalim i u kontekstu razmjene osobnih podataka među tijelima kaznenog progona i drugim tijelima javne vlasti, kao što su nacionalna sigurnosna tijela, ograničiti na ono što je nužno za ostvarivanje predmetnog legitimnog cilja te da postoji djelotvorna pravna zaštita od takvog zadiranja.

(160) Stoga bi trebalo potvrditi da Ujedinjena Kraljevina osigurava primjerenu razinu zaštite u smislu članka 36. stavka 2. Direktive (EU) 2016/680, tumačeno s obzirom na Povelju o temeljnim pravima.

(161) Taj se zaključak temelji na relevantnom nacionalnom sustavu Ujedinjene Kraljevine i njezinim međunarodnim obvezama, posebno poštovanju Europske konvencije o ljudskim pravima i prihvaćanju nadležnosti Europskog suda za ljudska prava. Kontinuirano poštovanje tih međunarodnih obveza stoga je osobito važan element procjene na kojoj se temelji ova Odluka.

4. UČINCI OVE ODLUKE I AKTIVNOSTI TIJELA ZA ZAŠTITU PODATAKA

(162) Države članice i njihovi organi dužni su poduzeti mjere potrebne za usklađivanje s aktima institucija Unije jer se potonji smatraju zakonitima i proizvode pravne učinke do njihova isteka, povlačenja, poništenja u postupku za poništenje ili proglašavanja nevažećima nakon zahtjeva za prethodnu odluku ili tužbenog zahtjeva za proglašenje nezakonitosti.

(163) Stoga je odluka Komisije o primjerenosti donesena u skladu s člankom 36. stavkom 3. Direktive (EU) 2016/680 obvezujuća za sva tijela država članica kojima je upućena, uključujući njihova neovisna nadzorna tijela. Konkretnije, dok se primjenjuje ova Odluka, za prijenos podataka od voditelja obrade ili izvršitelja obrade u Uniji voditeljima obrade ili izvršiteljima obrade u Ujedinjenoj Kraljevini nisu potrebna daljnja odobrenja.

(164) Istodobno bi trebalo podsjetiti da, u skladu s člankom 47. stavkom 5. Direktive (EU) 2016/680 i kako je objašnjeno u presudi Suda EU-a u predmetu *Schrems*, ako nacionalno tijelo za zaštitu podataka ima sumnje, među ostalim nakon što je zaprimilo pritužbu, u pogledu spojivosti odluke Komisije o primjerenosti s temeljnim pravima pojedinca na privatnost i zaštitu podataka, nacionalnim pravom mora biti predviđen pravni lijek za iznošenje tih prigovora pred nacionalnim sudom od kojeg se može tražiti da Sudu EU-a uputi zahtjev za prethodnu odluku ([270]).

([270]) Presuda u predmetu *Schrems*, točka 65.

5. **PRAĆENJE, SUSPENZIJA, STAVLJANJE IZVAN SNAGE ILI IZMJENA OVE ODLUKE**

(165) U skladu s člankom 36. stavkom 4. Direktive (EU) 2016/680 Komisija treba kontinuirano pratiti relevantne procese u Ujedinjenoj Kraljevini nakon donošenja ove Odluke kako bi procijenila osigurava li se njome još uvijek u osnovi istovjetna razina zaštite. Takvo je praćenje posebno važno u ovom slučaju jer će Ujedinjena Kraljevina donijeti, primjenjivati i provoditi novi sustav zaštite podataka koji više ne podliježe pravu Unije i koji bi mogao biti podložan promjenama. S obzirom na to, posebna će se pozornost pridavati praktičnoj primjeni pravila Ujedinjene Kraljevine o prijenosima osobnih podataka trećim zemljama, među ostalim i sklapanjem međunarodnih sporazuma, i učinku koji bi to moglo imati na razinu zaštite podataka koji se prenose na temelju ove Odluke te djelotvornosti ostvarivanja prava pojedinaca u područjima obuhvaćenima ovom Odlukom. Praćenje Komisije temeljit će se, među ostalim elementima, na promjenama u sudskoj praksi i nadzoru koji obavljaju ICO i druga neovisna tijela.

(166) Kako bi se olakšalo to praćenje, tijela Ujedinjene Kraljevine trebala bi u najkraćem roku i redovito obavješćivati Komisiju o svim bitnim izmjenama pravnog poretka Ujedinjene Kraljevine koje utječu na pravni okvir koji je predmet ove Odluke, kao i o svim promjenama praksi povezanih s obradom osobnih podataka koja je procijenjena u ovoj Odluci, a ponajprije s obzirom na elemente navedene u uvodnoj izjavi (165).

(167) Nadalje, kako bi Komisija mogla djelotvorno obavljati svoju funkciju praćenja, države članice trebale bi je obavješćivati o svim relevantnim mjerama koje poduzimaju nacionalna tijela za zaštitu podataka, naročito u pogledu upita ili pritužbi ispitanika iz EU-a o prijenosu osobnih podataka iz Unije nadležnim tijelima u Ujedinjenoj Kraljevini. Komisiju bi trebalo obavijestiti i o svakoj naznaci da mjere tijela javne vlasti Ujedinjene Kraljevine odgovornih za sprečavanje, istragu, otkrivanje ili progon kaznenih djela, uključujući nadzorna tijela, ne osiguravaju potrebnu razinu zaštite.

(168) Ako dostupne informacije, naročito informacije dobivene praćenjem primjene ove Odluke ili informacije koje dostavljaju tijela Ujedinjene Kraljevine ili država članica, pokazuju da razina zaštite koju pruža Ujedinjena Kraljevina možda više nije primjerena, Komisija bi o tome trebala u najkraćem roku obavijestiti nadležna tijela Ujedinjene Kraljevine i zatražiti poduzimanje odgovarajućih mjera u određenom roku, koji ne smije biti dulji od tri mjeseca. Prema potrebi, taj se rok može produljiti na određeno vrijeme, uzimajući u obzir prirodu predmetnog problema i/ili mjera koje treba poduzeti.

(169) Ako po isteku navedenog roka nadležna tijela Ujedinjene Kraljevine ne poduzmu te mjere ili na drugi zadovoljavajući način ne dokažu da se ova Odluka i dalje temelji na primjerenoj razini zaštite, Komisija će pokrenuti postupak iz članka 58. stavka 2. Direktive (EU) 2016/680 radi djelomične ili potpune suspenzije ili stavljanja izvan snage ove Odluke.

(170) Alternativno, Komisija će pokrenuti taj postupak radi izmjene Odluke, ponajprije utvrđivanjem dodatnih uvjeta za prijenose podataka ili ograničavanjem područja primjene zaključka o primjerenosti samo na prijenose podataka za koje se i dalje osigurava primjerena razina zaštite.

(171) Bude li valjano utemeljenih krajnje hitnih razloga, Komisija će iskoristiti mogućnost donošenja, u skladu s postupkom iz članka 58. stavka 3. Direktive (EU) 2016/680, odmah primjenjivih provedbenih akata o suspenziji, stavljanju izvan snage ili izmjeni Odluke.

6. **TRAJANJE I PRODULJENJE OVE ODLUKE**

(172) Trebalo bi uzeti u obzir da će nakon isteka prijelaznog razdoblja predviđenog Sporazumom o povlačenju i čim privremena odredba na temelju članka 782. Sporazuma o trgovini i suradnji između EU-a i Ujedinjene Kraljevine prestane važiti, Ujedinjena Kraljevina primjenjivati i provoditi novi sustav zaštite podataka koji se razlikuje od onog koji je uspostavljen pravom Europske unije. To može ponajprije uključivati izmjene ili promjene okvira za zaštitu podataka procijenjenog u ovoj Odluci, kao i druge relevantne promjene.

(173) Stoga je primjereno osigurati da se ova Odluka primjenjuje u razdoblju od četiri godine od njezina stupanja na snagu.

(174) Ako se određenim informacijama koje proizlaze iz praćenja primjene ove Odluke otkrije da su zaključci koji se odnose na primjerenost razine zaštite osigurane u Ujedinjenoj Kraljevini i dalje činjenično i pravno opravdani, Komisija bi trebala najkasnije šest mjeseci prije nego što se ova Odluka prestane primjenjivati pokrenuti postupak izmjene ove Odluke proširenjem vremenskog okvira primjene, u načelu, na dodatno razdoblje od četiri godine. Svaki takav provedbeni akt o izmjeni ove Odluke treba se donijeti u skladu s postupkom iz članka 58. stavka 2. Direktive (EU) 2016/680.

7. **ZAVRŠNA RAZMATRANJA**

(175) Europski odbor za zaštitu podataka objavio je svoje mišljenje ([271]), koje je uzeto u obzir pri pripremi ove Odluke.

(176) Mjere predviđene ovom Odlukom u skladu su s mišljenjem Odbora osnovanog na temelju članka 58. Direktive (EU) 2016/680.

(177) U skladu s člankom 6.a Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područja slobode, sigurnosti i pravde, priloženog UEU-u i UFEU-u, Irsku ne obvezuju pravila utvrđena u Direktivi (EU) 2016/680, a stoga ni pravila u ovoj Provedbenoj odluci, koja se odnose na obradu osobnih podataka od strane država članica pri obavljanju djelatnosti koje su obuhvaćene područjem primjene dijela trećeg glave V. poglavlja 4. ili poglavlja 5. UFEU-a, a pritom Irsku ne obvezuju pravila koja uređuju oblike pravosudne suradnje u kaznenim stvarima ili policijske suradnje za koja se traži usklađenost s odredbama utvrđenima na temelju članka 16. UFEU-a. Nadalje, na temelju Provedbene odluke Vijeća (EU) 2020/1745 ([272]), Direktiva (EU) 2016/680 privremeno će se staviti na snagu i primjenjivati u Irskoj od 1. siječnja 2021. Irsku stoga ova Provedbena odluka obvezuje pod istim uvjetima koji se primjenjuju na primjenu Direktive (EU) 2016/680 u Irskoj kako je utvrđeno u Provedbenoj odluci (EU) 2020/1745 u pogledu schengenske pravne stečevine u kojoj Irska sudjeluje.

(178) U skladu s člancima 2. i 2.a Protokola br. 22 o stajalištu Danske, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, Dansku ne obvezuju pravila utvrđena u Direktivi (EU) 2016/680, a stoga ni pravila u ovoj Provedbenoj odluci, niti ona podliježe njihovoj primjeni koja se odnosi na obradu osobnih podataka od strane država članica pri obavljanju djelatnosti koje su obuhvaćene područjem primjene dijela trećeg glave V. poglavlja 4. ili poglavlja 5. UFEU-a. Međutim, s obzirom na to da se Direktiva (EU) 2016/680 temelji na schengenskoj pravnoj stečevini, Danska je, u skladu s člankom 4. tog protokola, 26. listopada 2016. priopćila svoju odluku da će provesti Direktivu (EU) 2016/680. Danska je stoga u skladu s međunarodnim pravom obvezna provoditi ovu Provedbenu odluku.

(179) Kad je riječ o Islandu i Norveškoj, ova Provedbena odluka predstavlja razvoj odredaba schengenske pravne stečevine, u smislu Sporazuma između Vijeća Europske Unije i Republike Islanda i Kraljevine Norveške o pridruživanju tih dviju država provedbi, primjeni i razvoju schengenske pravne stečevine ([273]).

(180) Kad je riječ o Švicarskoj, ova Provedbena odluka predstavlja razvoj odredaba schengenske pravne stečevine, u smislu Sporazuma između Europske Unije, Europske zajednice i Švicarske Konfederacije o pridruživanju Švicarske Konfederacije provedbi, primjeni i razvoju schengenske pravne stečevine ([274]).

(181) Kad je riječ o Lihtenštajnu, ova Provedbena odluka predstavlja razvoj odredaba schengenske pravne stečevine, u smislu Protokola između Europske unije, Europske zajednice, Švicarske Konfederacije i Kneževine Lihtenštajna o pristupanju Kneževine Lihtenštajna Sporazumu između Europske unije, Europske zajednice i Švicarske Konfederacije o pridruživanju Švicarske Konfederacije provedbi, primjeni i razvoju schengenske pravne stečevine ([275]),

([271]) Mišljenje br. 15/2021 o Nacrtu provedbene odluke Europske komisije u skladu s Direktivom (EU) 2016/680 o primjerenoj zaštiti osobnih podataka u Ujedinjenoj Kraljevini, dostupno na: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Provedbena odluka Vijeća (EU) 2020/1745 od 18. studenoga 2020. o stavljanju na snagu odredaba schengenske pravne stečevine o zaštiti podataka i o privremenom stavljanju na snagu određenih odredaba schengenske pravne stečevine u Irskoj (SL L 393, 23.11.2020., str. 3.).

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

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

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

DONIJELA JE OVU ODLUKU:

Članak 1.

Za potrebe članka 36. Direktive (EU) 2016/680 Ujedinjena Kraljevina osigurava primjerenu razinu zaštite osobnih podataka koji se iz Europske unije prenose tijelima javne vlasti u Ujedinjenoj Kraljevini odgovornima za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenih sankcija.

Članak 2.

Svaki put kad nadležna nadzorna tijela u državama članicama, radi zaštite pojedinaca u vezi s obradom njihovih osobnih podataka, izvršavaju svoje ovlasti u skladu s člankom 47. Direktive (EU) 2016/680 u pogledu prijenosa podataka tijelima javne vlasti u Ujedinjenoj Kraljevini koji su obuhvaćeni područjem primjene navedenim u članku 1., predmetna država članica o tome bez odgode obavješćuje Komisiju.

Članak 3.

1. Komisija kontinuirano prati primjenu pravnog okvira na kojem se temelji ova Odluka, uključujući uvjete pod kojima se odvija daljnji prijenos i ostvaruju prava pojedinaca, kako bi ocijenila osigurava li Ujedinjena Kraljevina i dalje primjerenu razinu zaštite u smislu članka 1.

2. Države članice i Komisija međusobno se obavješćuju o slučajevima u kojima povjerenik za informiranje ili bilo koje drugo nadležno tijelo u Ujedinjenoj Kraljevini ne osigura poštovanje pravnog okvira na kojem se temelji ova Odluka.

3. Države članice i Komisija međusobno se obavješćuju o naznakama da zadiranje tijela javne vlasti Ujedinjene Kraljevine u pravo pojedinaca na zaštitu njihovih osobnih podataka prelazi ono što je nužno ili da ne postoji djelotvorna sudska zaštita od takvog zadiranja.

4. Ako ima informacije o tome da primjerena razina zaštite više nije osigurana, Komisija obavješćuje nadležna tijela Ujedinjene Kraljevine i može suspendirati, staviti izvan snage ili izmijeniti ovu Odluku.

5. Komisija može suspendirati, staviti izvan snage ili izmijeniti ovu Odluku ako zbog nesuradnje vlade Ujedinjene Kraljevine Komisija ne može utvrditi utječe li to na zaključak iz članka 1. ove Odluke.

Članak 4.

Ova Odluka prestaje važiti 27. lipnja 2025., osim ako se produlji u skladu s postupkom iz članka 58. stavka 2. Direktive (EU) 2016/680.

Članak 5.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu 28. lipnja 2021.

Za Komisiju
Didier REYNDERS
Član Komisije