II

(Neleģislatīvi akti)

LĒMUMI

KOMISIJAS ĪSTENOŠANAS REGULA (ES) 2021/1772

(2021. gada 28. jūnijs)

par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679

(izziņots ar dokumenta numuru C(2021) 4800)

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (Vispārīgā datu aizsardzības regula) ([1]), jo īpaši tās 45. panta 3. punktu,

tā kā:

1. IEVADS

(1) Ar Regulu (ES) 2016/679 ir paredzēti noteikumi, saskaņā ar kuriem Eiropas Savienībā esoši pārziņi vai apstrādātāji var nosūtīt personas datus trešām valstīm un starptautiskām organizācijām, ciktāl šāda nosūtīšana ietilpst regulas piemērošanas jomā. Noteikumi par datu starptautisku nosūtīšanu ir izklāstīti minētās regulas V nodaļā, tas ir, tās 44.–50. pantā. Lai gan personas datu plūsma uz valstīm ārpus Eiropas Savienības un no tām ir būtiska starptautiskās sadarbības un pārrobežu tirdzniecības paplašināšanas nodrošināšanai, datu nosūtīšana uz trešām valstīm nedrīkst samazināt Eiropas Savienībā nodrošināto personas datu aizsardzības līmeni ([2]).

(2) Atbilstoši Regulas (ES) 2016/679 45. panta 3. punktam Komisija ar īstenošanas aktu var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni. Saskaņā ar šo nosacījumu personas datu nosūtīšana uz trešo valsti var notikt bez nepieciešamības saņemt jebkādu turpmāku atļauju, kā paredzēts minētās regulas 45. panta 1. punktā un 103. apsvērumā.

(3) Kā norādīts Regulas (ES) 2016/679 45. panta 2. punktā, lēmums par aizsardzības līmeņa pietiekamību jāpieņem, pamatojoties uz visaptverošu trešās valsts tiesību sistēmas analīzi, gan attiecībā uz noteikumiem, kas piemērojami datu importētājiem, gan attiecībā uz ierobežojumiem un garantijām saistībā ar publisko iestāžu piekļuvi personas datiem. Komisijai novērtējumā jānosaka, vai attiecīgā trešā valsts garantē aizsardzības līmeni, kurš "pēc būtības ir līdzvērtīgs" Eiropas Savienībā nodrošinātajam (Regulas (ES) 2016/679 104. apsvērums). Standarts, pēc kura tiek novērtēta "līdzvērtība pēc būtības", ir paredzēts Eiropas Savienības tiesību aktos, jo īpaši Regulā (ES) 2016/679, kā arī Eiropas Savienības Tiesas judikatūrā ([3]). Šajā ziņā būtiska nozīme ir arī Eiropas Datu aizsardzības kolēģijas (EDAK) pieņemtajām aizsardzības līmeņa pietiekamības atsaucēm ([4]).

([1]) OV L 119, 4.5.2016., 1. lpp.
([2]) Sk. Regulas (ES) 2016/679 101. apsvērumu.
([3]) Sk. spriedumu jaunākajā lietā C-311/18 *Facebook Ireland and Schrems* ("*Schrems II*"), ECLI:EU:C:2020:559.
([4]) Eiropas Datu aizsardzības kolēģijas Pietiekamības atsauces, WP 254 rev. 01, pieejamas vietnē https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Kā ir precizējusi Eiropas Savienības Tiesa, tas nenozīmē, ka ir jākonstatē identisks aizsardzības līmenis ([5]). Konkrēti, attiecīgās trešās valsts izmantotie līdzekļi personas datu aizsardzībai var atšķirties no Eiropas Savienībā izmantotajiem, kamēr vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni ([6]). Tāpēc aizsardzības līmeņa pietiekamības standarts neparedz Savienības noteikumu precīzu replicēšanu. Pārbaude drīzāk atklāj, vai attiecīgās valsts tiesību sistēma spēj nodrošināt nepieciešamo aizsardzības līmeni, ņemot vērā tiesību uz datu aizsardzību būtību un to efektīvu īstenošanu, uzraudzību un izpildi ([7]).

(5) Komisija ir rūpīgi izanalizējusi Apvienotās Karalistes attiecīgos tiesību aktu un praksi. Pamatojoties uz 8.–270. apsvērumā izklāstītajiem konstatējumiem, Komisija secina, ka personas datiem, kas tiek nosūtīti no Eiropas Savienības uz Apvienoto Karalisti Regulas (ES) 2016/679 piemērošanas jomas ietvaros, Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni.

(6) Šis secinājums neattiecas uz personas datiem, kas nosūtīti Apvienotās Karalistes imigrācijas kontroles vajadzībām vai uz ko citādi attiecas atbrīvojums no konkrētām datu subjektu tiesībām efektīvas imigrācijas kontroles nodrošināšanas vajadzībām ("imigrācijas atbrīvojums") saskaņā ar Apvienotās Karalistes Datu aizsardzības likuma 2. pielikuma 4. punkta 1. apakšpunktu. Imigrācijas atbrīvojuma spēkā esība un interpretācija saskaņā ar Apvienotās Karalistes tiesību aktiem nav noteikta; tas ir saistīts ar lēmumu, kuru 2021. gada 26. maijā pieņēmusi Anglijas un Velsas Apelācijas tiesa. Lai gan Apelācijas tiesa atzīst, ka datu subjektu tiesības kā svarīgs sabiedrības interešu aspekts principā var tikt ierobežotas imigrācijas kontroles vajadzībām, tā ir konstatējusi, ka imigrācijas atbrīvojums pašreizējā formā nav saderīgs ar Apvienotās Karalistes tiesību aktiem, jo leģislatīvajam pasākumam nav konkrētu noteikumu, ar kuriem paredz Apvienotās Karalistes Vispārīgās datu aizsardzības regulas (Apvienotās Karalistes VDAR) 23. panta 2. punktā uzskaitītās garantijas ([8]). Šajos apstākļos tādu personas datu nosūtīšana no ES uz Apvienoto Karalisti, kuriem var piemērot imigrācijas atbrīvojumu, būtu jāizslēdz no šā lēmuma darbības jomas ([9]). Tiklīdz nesaderība ar Apvienotās Karalistes tiesību aktiem būs novērsta, būtu atkārtoti jāizvērtē imigrācijas atbrīvojums, kā arī nepieciešamība saglabāt šā lēmuma darbības jomas ierobežojumus.

(7) Šim lēmumam nevajadzētu ietekmēt Regulas (ES) 2016/679 tiešu piemērošanu organizācijām, kas ir reģistrētas Apvienotajā Karalistē, ja ir izpildīti šīs regulas 3. pantā paredzētie nosacījumi attiecībā uz tās teritoriālo darbības jeb piemērošanas jomu.

2. PERSONAS DATU APSTRĀDEI PIEMĒROJAMIE NOTEIKUMI

2.1. Konstitucionālais regulējums

(8) Apvienotā Karaliste ir parlamentāra demokrātija, un saskaņā ar konstitūciju valsts galva ir monarhs. Tai ir suverēns parlaments (augstāks par visām valdības iestādēm), parlamenta izveidota un tā priekšā atbildīga izpildvara, kā arī neatkarīga tiesu vara. Izpildvaras pilnvaras izriet no tās spējas gūt ievērētās Pārstāvju palātas uzticību, un tā par savu darbību atbild abām parlamenta palātām, kas ir atbildīgas par valdības pārbaudi, kā arī tiesību aktu apspriešanu un to pieņemšanu.

([5]) Spriedums lietā C-362/14 *Schrems* ("*Schrems I*"), ECLI:EU:C:2015:650, 73. punkts.

([6]) *Schrems I*, 74. punkts.

([7]) Sk. Komisijas paziņojumu Eiropas Parlamentam un Padomei "Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē", COM(2017) 7, 10.1.2017., 3.1. iedaļa, 6. un 7. lpp., pieejams šādā vietnē: https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:52017DC0007&from=LV.

([8]) Apelācijas tiesa (Civillietu palāta), *Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, 53.–56. punkts. Apelācijas tiesa atcēla Augstās tiesas lēmumu, kura ietvaros atbrīvojums tika novērtēts iepriekš, ņemot vērā Regulu (ES) 2016/679 (jo īpaši tās 23. pantu) un Eiropas Savienības Pamattiesību hartu, un konstatēja, ka atbrīvojums ir likumīgs (*Open Rights Group & Anor, R (On the Application Of) v Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

([9]) Ar noteikumu, ka piemērojamie nosacījumi tiek ievēroti, datus Apvienotās Karalistes imigrācijas kontroles vajadzībām var nosūtīt, balstoties uz Regulas (ES) 2016/679 46.–49. pantā minētajiem nosūtīšanas mehānismiem.

(9) Apvienotās Karalistes parlaments ir deleģējis Skotijas parlamentam, Velsas parlamentam (*Senedd Cymru*) un Ziemeļīrijas asamblejai atbildību par tiesību aktu izstrādi attiecībā uz tādiem vietējiem jautājumiem Skotijā, Velsā un Ziemeļīrijā, kuru reglamentēšana nav Apvienotās Karalistes parlamenta kompetencē. Lai gan datu aizsardzība ir Apvienotās Karalistes parlamenta kompetencē, t. i., vienus un tos pašus tiesību aktus piemēro visā valstī, citas ar šo lēmumu saistītās politikas jomas ir decentralizētas. Piemēram, Skotijas un Ziemeļīrijas krimināltiesību sistēmas, tostarp policijas darbs, ir deleģētas attiecīgi Skotijas parlamentam un Ziemeļīrijas asamblejai. Apvienotajā Karalistē nepastāv kodificēta konstitūcija kā iesakņojies konstitucionāls dokuments. Konstitucionālie principi ir attīstījušies laika gaitā, jo īpaši no judikatūras un paražām. Tiesas ir atzinušas, ka dažiem likumiem, piemēram, Lielajai brīvības hartai, 1689. gada Tiesību likumam un 1998. gada Cilvēktiesību likumam, ir konstitucionāls saturs. Cilvēka pamattiesības kā daļa no konstitūcijas ir attīstītas, izmantojot anglosakšu tiesības, iepriekš minētos likumus un starptautiskos līgumus, jo īpaši Eiropas Cilvēktiesību konvenciju, ko Apvienotā Karaliste ratificēja 1951. gadā. Apvienotā Karaliste 1987. gadā ir arī ratificējusi Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108) ([10]).

(10) Ar 1998. gada Cilvēktiesību likumu Apvienotās Karalistes tiesību aktos ir iekļautas Eiropas Cilvēktiesību konvencijā paredzētās tiesības. Ar Cilvēktiesību likumu ikvienai personai ir piešķirtas pamattiesības un pamatbrīvības, kas paredzētas Eiropas Cilvēktiesību konvencijas 2.–12. pantā un 14. pantā, tās pirmā protokola 1., 2. un 3. pantā un tās trīspadsmitā protokola 1. pantā, ko skata kopā ar šīs konvencijas 16., 17. un 18. pantu. Tas ietver tiesības uz privātās un ģimenes dzīves neaizskaramību (un šo tiesību ietvaros tiesības uz datu aizsardzību) un tiesības uz lietas taisnīgu izskatīšanu ([11]). Konkrēti, saskaņā ar iepriekš minētās konvencijas 8. pantu publiskā iestāde (institūcija) var traucēt baudīt tiesības uz privātumu tikai gadījumos, kas ir paredzēti likumā un ir nepieciešami demokrātiskā sabiedrībā, lai aizsargātu valsts un sabiedrisko drošību vai valsts ekonomiskās labklājības intereses, lai nepieļautu nekārtības vai noziegumus, lai aizsargātu veselību vai tikumību vai lai aizstāvētu citu tiesības un brīvības.

(11) Saskaņā ar 1998. gada Cilvēktiesību likumu visām publisko iestāžu darbībām jābūt saderīgām ar konvencijā paredzētajām tiesībām ([12]). Turklāt primārie un sekundārie tiesību akti ir jāskata un jāpiemēro tā, lai tie būtu saderīgi ar konvencijā paredzētajām tiesībām ([13]).

2.2. **Apvienotās Karalistes datu aizsardzības regulējums**

(12) Apvienotā Karaliste 2020. gada 31. janvārī izstājās no Eiropas Savienības. Pamatojoties uz Līgumu par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes izstāšanos no Eiropas Savienības un Eiropas Atomenerģijas kopienas ([14]), Savienības tiesību aktu piemērošana Apvienotajā Karalistē turpinājās pārejas periodā līdz 2020. gada 31. decembrim. Pirms izstāšanās un pārejas periodā tiesisko regulējumu personas datu aizsardzībai Apvienotajā Karalistē veidoja attiecīgie ES tiesību akti (jo īpaši Eiropas Parlamenta un Padomes Regula (ES) 2016/679 un Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 ([15])) un valsts tiesību akti, jo īpaši 2018. gada Datu aizsardzības likums (turpmāk "2018. gada DAL") ([16]), kurā, ja to atļāva Regula (ES) 2016/679, bija paredzēti valsts noteikumi, kas precizēja un ierobežoja Regulas (ES) 2016/679 prasību piemērošanu, un ar kuru tika transponēta Direktīva (ES) 2016/680.

([10]) Konvencijas Nr. 108 principi sākotnēji tika iestrādāti Apvienotās Karalistes tiesību aktos ar 1984. gada Datu aizsardzības likumu, kas ir aizstāts ar 1998. gada DAL un pēc tam ar 2018. gada DAL (ko skata kopā ar Apvienotās Karalistes VDAR). Apvienotā Karaliste 2018. gadā ir parakstījusi arī Protokolu, ar ko groza Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi ("Konvencija Nr. 108+"), un pašlaik strādā pie konvencijas ratifikācijas.

([11]) Eiropas Cilvēktiesību konvencijas (ECTK) 6. un 8. pants (sk. arī 1998. gada Cilvēktiesību likuma 1. pielikumu).

([12]) 1998. gada Cilvēktiesību likuma 6. pants.

([13]) 1998. gada Cilvēktiesību likuma 3. pants.

([14]) Līgums par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes izstāšanos no Eiropas Savienības un Eiropas Atomenerģijas kopienas, 2019/C 384 I/01, XT/21054/2019/INIT (OV C 384I, 12.11.2019., 1. lpp.), pieejams vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=LV.

([15]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināls sodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.), pieejama vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:32016L0680&from=LV.

([16]) 2018. gada Datu aizsardzības likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(13) Veicot sagatavošanās pasākumus nolūkā izstāties no Eiropas Savienības, Apvienotās Karalistes valdība pieņēma 2018. gada Likumu par izstāšanos no Eiropas Savienības ([17]), ar ko Apvienotās Karalistes tiesību aktos ([18]) iekļāva tieši piemērojamus Savienības tiesību aktus. Šie tā dēvētie "saglabātie ES tiesību akti" ietver Regulu (ES) 2016/679 pilnā apjomā (ieskaitot tās apsvērumus) ([19]). Minētais likums paredz, ka Apvienotās Karalistes tiesām negrozītie saglabātie ES tiesību akti ir jāinterpretē saskaņā ar Eiropas Savienības Tiesas attiecīgo judikatūru un Savienības tiesību aktu vispārējiem principiem, kā tie piemērojami tieši pirms pārejas perioda beigām (attiecīgi "saglabātā ES judikatūra" un "saglabātie ES tiesību aktu vispārējie principi") ([20]).

(14) Saskaņā ar 2018. gada Likumu par izstāšanos no Eiropas Savienības Apvienotās Karalistes ministri ir pilnvaroti, izmantojot normatīvos aktus, pieņemt sekundāros tiesību aktus ar mērķi veikt saglabātajos Eiropas Savienības tiesību aktos nepieciešamos grozījumus, kas izriet no Apvienotās Karalistes izstāšanās no Eiropas Savienības. Šīs pilnvaras tika izmantotas, pieņemot 2019. gada Datu aizsardzības, privātuma un elektronisko sakaru (ar grozījumiem) (Izstāšanās no ES) noteikumus ("DAPES noteikumi") ([21]). Ar DAPES noteikumiem ir veikti grozījumi Regulā (ES) 2016/679, kas ir iestrādāta Apvienotās Karalistes tiesībās, pieņemot 2018. gada Likumu par izstāšanos no Eiropas Savienības, 2018. gada DAL un citus datu aizsardzības tiesību aktus, lai tie atbilstu vietējam kontekstam ([22]).

(15) Tādējādi personas datu aizsardzības tiesisko regulējumu Apvienotajā Karalistē pēc pārejas perioda veido:

— Apvienotās Karalistes VDAR, kas ir iestrādāta Apvienotās Karalistes tiesībās saskaņā ar 2018. gada Likumu par izstāšanos no Eiropas Savienības un grozīta ar DAPES noteikumiem ([23]), kā arī

— 2018. gada DAL ([24]), kas grozīts ar DAPES noteikumiem.

(16) Tā kā Apvienotās Karalistes VDAR pamatā ir ES tiesību akti, datu aizsardzības noteikumi Apvienotajā Karalistē daudzos aspektos ir ļoti līdzīgi attiecīgajiem Eiropas Savienībā piemērojamajiem noteikumiem.

(17) Papildus pilnvarām, kas ministram ir piešķirtas ar 2018. gada Likumu par izstāšanos no Eiropas Savienības, arī vairākos 2018. gada DAL noteikumos tam ir paredzētas pilnvaras pieņemt sekundāros tiesību aktus nolūkā grozīt atsevišķus likuma noteikumus vai pieņemt papildinošus vai papildu noteikumus ([25]). Ministrs līdz šim ir izmantojis

([17]) 2018. gada Likums par izstāšanos no Eiropas Savienības, pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/16/contents.

([18]) 2018. gada Likuma par izstāšanos no Eiropas Savienības mērķis un sekas ir tādas, ka visi tieši piemērojamie Savienības tiesību akti, kas bija iestrādāti Apvienotās Karalistes tiesību aktos pārejas perioda beigās, ir iestrādāti Apvienotās Karalistes tiesībās atbilstīgi ES tiesību aktiem tādā redakcijā, kas bija spēkā tieši pirms pārejos perioda beigām, sk. 2018. gada Likuma par izstāšanos no Eiropas Savienības 3. pantu.

([19]) 2018. gada Likuma par izstāšanos no Eiropas Savienības paskaidrojuma rakstā ir noteikts: "Gadījumos, kad tiesību akts saskaņā ar šo pantu tiek pārveidots, valsts tiesību aktā iekļauj paša tiesību akta tekstu. Tas ietver jebkura ES juridiskā instrumenta tekstu pilnībā (ieskaitot tā apsvērumus)." (2018. gada Likuma par izstāšanos no Eiropas Savienības paskaidrojuma raksta 83. punkts, pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf.) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju, ņemot vērā to, ka apsvērumi nav uzskatāmi par saistošām tiesību normām, tie nebija jāgroza tā, kā Regulas (ES) 2016/679 panti ir grozīti ar DAPES noteikumiem.

([20]) 2018. gada Likuma par izstāšanos no Eiropas Savienības 6. pants.

([21]) 2019. gada Datu aizsardzības, privātuma un elektronisko sakaru (ar grozījumiem) (Izstāšanās no ES) noteikumi, pieejami vietnē https://www.legislation.gov.uk/uksi/2019/419/contents/made, ar grozījumiem, kas izdarīti ar 2020. gada DAPES noteikumiem, pieejami vietnē https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([22]) Šiem Apvienotās Karalistes VDAR un 2018. gada DAL grozījumiem ir galvenokārt tehnisks raksturs, piemēram, ir svītrotas atsauces uz "dalībvalstīm" vai pielāgota terminoloģija, piemēram, atsauces uz Regulu (ES) 2016/679 ir aizstātas ar atsaucēm uz Apvienotās Karalistes VDAR. Dažos gadījumos izmaiņas bija vajadzīgas nolūkā atspoguļot to, ka noteikumi attiecas tikai uz vietējo kontekstu, piemēram, saistībā ar to, "kurš" pieņem "noteikumus par aizsardzības līmeņa pietiekamību" Apvienotās Karalistes datu aizsardzības tiesiskā regulējuma vajadzībām (sk. 2018. gada DAL 17.A pantu), proti, nevis Eiropas Komisija, bet ministrs.

([23]) Vispārīgā datu aizsardzības regula, *Keeling* pielikums, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) 2018. gada Datu aizsardzības likums, *Keeling* pielikums, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Šādas pilnvaras ir paredzētas, piemēram, 2018. gada DAL 16. pantā (pilnvaras īpašās, stingri noteiktās situācijās paredzēt papildu atbrīvojumus no konkrētu Apvienotās Karalistes VDAR noteikumu piemērošanas), 17.A pantā (pilnvaras pieņemt noteikumus par aizsardzības līmeņa pietiekamību), 212. un 213. pantā (pilnvaras sākt likumdošanas procesu un pieņemt pārejas noteikumus) un 211. pantā (pilnvaras veikt nebūtiskus un izrietošus grozījumus).

tikai 2018. gada DAL 137. pantā noteiktās pilnvaras, lai pieņemtu 2019. gada Datu aizsardzības (maksas un informācija) (grozījums) noteikumus, kuros ir izklāstīti apstākļi, kādos datu pārziņiem ir jāmaksā ikgadējs maksājums neatkarīgai Apvienotās Karalistes datu aizsardzības iestādei, proti, informācijas komisāram (IK).

(18) Papildu informācija par Apvienotās Karalistes datu aizsardzības tiesību aktiem ir sniegta prakses kodeksos un citos informācijas komisāra pieņemtos norādījumos. Lai gan, raugoties no oficiālā viedokļa, šie norādījumi nav juridiski saistoši, tiem ir interpretējošs spēks, un tajos ir izklāstīts, kā piemērojami datu aizsardzības tiesību akti un kā komisārs tos īsteno praksē. Konkrētāk, 2018. gada DAL 121.–125. pantā ir noteikts, ka komisāram jāsagatavo prakses kodeksi par datu apmaiņu, tiešo tirgvedību, vecumam atbilstošu noformējumu, datu aizsardzību un žurnālistiku.

(19) Tādējādi Apvienotās Karalistes tiesiskais regulējums, kas attiecas uz datu nosūtīšanu atbilstīgi šim lēmumam, pēc struktūras un galvenajiem elementiem ir ļoti līdzīgs tam, ko piemēro Eiropas Savienībā. Minētais ietver arī to, ka regulējums balstās ne tikai uz pienākumiem, kas noteikti valsts tiesību aktos, kurus ietekmējuši ES tiesību akti, bet arī uz starptautiskajās tiesībās nostiprinātajām saistībām, jo īpaši tādēļ, ka Apvienotā Karaliste ievēro ECTK un Konvenciju Nr. 108, kā arī pakļaujas Eiropas Cilvēktiesību tiesas jurisdikcijai. Tādējādi šie pienākumi, kas izriet no juridiski saistošiem starptautiskiem instrumentiem, jo īpaši personas datu aizsardzības jomā, ir īpaši svarīgs šajā lēmumā vērtētā tiesiskā regulējuma elements.

2.3. **Materiālā un teritoriālā piemērošanas joma**

(20) Apvienotās Karalistes VDAR, līdzīgi Regulai (ES) 2016/679, attiecas uz personas datu apstrādi, ko pilnībā vai daļēji veic ar automatizētiem līdzekļiem, vai citādu apstrādi, ja personas dati veido daļu no kartotēkas ([26]). Apvienotās Karalistes VDAR izmantotās jēdzienu "personas dati", "datu subjekts" un "apstrāde" definīcijas ir identiskas Regulā (ES) 2016/679 noteiktajām šo jēdzienu definīcijām ([27]). Turklāt Apvienotās Karalistes VDAR ir piemērojama tādu manuāli apstrādājamu nestrukturētu personas datu apstrādei ([28]), kas ir noteiktu Apvienotās Karalistes publisko iestāžu rīcībā ([29]), lai gan Apvienotās Karalistes VDAR paredzētie principi un tiesības, kas neattiecas uz šādiem personas datiem, saskaņā ar 2018. gada DAL 24. un 25. pantu nav piemērojami. Līdzīgi Regulā (ES) 2016/679 noteiktajam Apvienotās Karalistes VDAR nav piemērojama tādai personas datu apstrādei, ko persona veic tikai personiska vai mājsaimnieciska pasākuma gaitā ([30]).

(21) Apvienotās Karalistes VDAR darbības jomā ietilpst arī apstrāde, kas veikta, īstenojot darbību, uz kuru tieši pirmspārejas perioda beigām neattiecās Eiropas Savienības tiesību akti (piemēram, valsts drošība) ([31]) vai kura ietilpa Līguma par Eiropas Savienību 5. sadaļas 2. nodaļas darbības jomā (kopējās ārpolitikas un drošības politikas darbības) ([32]). Līdzīgi kā Eiropas Savienības sistēmas ietvaros, Apvienotās Karalistes VDAR nav piemērojama personas datu apstrādei, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu kriminālsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu (tā dēvētajā "tiesībaizsardzības nolūkā") (šādu personas datu apstrādi reglamentē 2018. gada DAL

([26]) Apvienotās Karalistes VDAR 2. panta 1. un 5. punkts.

([27]) Apvienotās Karalistes VDAR 4. panta 1. un 2. punkts.

([28]) Saskaņā ar 2. panta 5. punkta b) apakšpunktā sniegto definīciju personas datu manuāla nestrukturēta apstrāde ir tādu personas datu apstrāde, kas nav automatizēta vai strukturēta personas datu apstrāde.

([29]) Apvienotās Karalistes VDAR 2. panta 1.A punktā ir noteikts, ka regula ir piemērojama arī tādu personas datu manuālai nestrukturētai apstrādei, kas ir to publisko iestāžu rīcībā, uz kurām attiecas pienākums nodrošināt informācijas brīvību. Publiskās iestādes, uz kurām attiecas pienākums nodrošināt informācijas brīvību, ir visas publiskās iestādes, kā noteikts 2000. gada Informācijas brīvības likumā, vai visas Skotijas publiskās iestādes, kā noteikts 2002. gada Informācijas brīvības likumā (Skotija) (asp 13). 2018. gada DAL 21. panta 5. punkts.

([30]) Apvienotās Karalistes VDAR 2. panta 2. punkta a) apakšpunkts.

([31]) Ar valsts drošību saistītās darbības ietilpst Apvienotās Karalistes VDAR piemērošanas jomā tikai tad, ja tās tiesībaizsardzības nolūkā neveic kompetentā iestāde (šajā gadījumā attiecīgajām darbībām piemēro 2018. gada DAL 3. daļu) vai ja tās neveic izlūkdienests, kura darbības neietilpst Apvienotās Karalistes VDAR piemērošanas jomā un saskaņā ar Apvienotās Karalistes VDAR 2. panta 2. punkta c) apakšpunktu ir pakļautas 2018. gada DAL 4. daļai, vai ja tās neveic izlūkdienesta vārdā. Piemēram, policijas vienība drīkst veikt drošības pārbaudes attiecībā uz darbinieku nolūkā pārliecināties, vai viņam var atļaut piekļūt ar valsts drošību saistītiem materiāliem. Lai gan policija ir kompetentā iestāde tiesībaizsardzības nolūkā, attiecīgā apstrāde netiek veikta tiesībaizsardzības nolūkā, un būtu piemērojama Apvienotās Karalistes VDAR. Sk. Apvienotās Karalistes paskaidrojuma dokumentu aizsardzības līmeņa pietiekamības apspriešanai, H iedaļa "Valsts drošības datu aizsardzības un izmeklēšanas pilnvaru regulējums", 8. lpp., pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

([32]) Apvienotās Karalistes VDAR 2. panta 1. punkta a) un b) apakšpunkts.

3. daļa, līdzīgi kā Direktīvas (ES) 2016/680 gadījumā Eiropas Savienības tiesību ietvaros), vai izlūkdienestu (Drošības dienesta, Slepenās izlūkošanas dienesta un Valdības sakaru štāba) veiktai personas datu apstrādei, uz ko attiecas 2018. gada DAL 4. daļa ([33]).

(22) Apvienotās Karalistes VDAR teritoriālā piemērošanas joma ir aprakstīta Apvienotās Karalistes VDAR 3. pantā ([34]) un ietver personas datu apstrādi (neatkarīgi no tā, kur šī apstrāde tiek veikta), kas notiek saistībā ar darbībām, ko veic pārziņa vai apstrādātāja uzņēmējdarbības vietā Apvienotajā Karalistē, kā arī Apvienotajā Karalistē esošu datu subjektu personas datu apstrādi, ja apstrādes darbības ir saistītas ar preču vai pakalpojumu piedāvāšanu šādiem datu subjektiem vai viņu uzvedības novērošanu ([35]). Šis regulējums atspoguļo Regulas (ES) 2016/679 3. pantā izmantoto pieeju.

2.4. **Jēdzienu "personas dati", "pārzinis" un "apstrādātājs" definīcijas**

(23) Apvienotās Karalistes VDAR bez būtiskām izmaiņām ir saglabātas Regulā (ES) 2016/679 noteiktās jēdzienu "personas dati", "apstrāde", "pārzinis" un "apstrādātājs" definīcijas, kā arī jēdziena "pseidonimizācija" definīcija ([36]). Īpašas datu kategorijas Apvienotās Karalistes VDAR 9. panta 1. punktā ir definētas tāpat kā Regulā (ES) 2016/679 (personas dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, ģenētiskie dati, biometriskie dati, kas nepieciešami, lai veiktu fiziskas personas unikālu identifikāciju, veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju). 2018. gada DAL 205. pantā ir noteiktas jēdzienu "biometriskie dati" ([37]), "veselības dati" ([38]) un "ģenētiskie dati" ([39]) definīcijas.

2.5. **Garantijas, tiesības un pienākumi**

2.5.1. *Apstrādes likumīgums un godprātība*

(24) Personas dati ir jāapstrādā likumīgi un godprātīgi.

(25) Likumīguma, godprātības un pārredzamības principi un likumīgas apstrādes pamats Apvienotās Karalistes tiesību aktos ir garantēts ar Apvienotās Karalistes VDAR 5. panta 1. punkta a) apakšpunktu un 6. panta 1. punktu, kurā izklāstītās prasības ir identiskas ar attiecīgajiem noteikumiem Regulā (ES) 2016/679 ([40]). 2018. gada DAL 8. pants papildina 6. panta 1. punkta e) apakšpunktu, paredzot, ka Apvienotās Karalistes VDAR 6. panta 1. punkta e) apakšpunktā minētā personas datu apstrāde (kas ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs

([33]) Apvienotās Karalistes VDAR 2. panta 2. punkta b) un c) apakšpunkts.

([34]) Šāda teritoriālā piemērošanas joma attiecas arī uz personas datu apstrādi, kas ir minēta 2018. gada DAL 2. daļā, ar ko papildina Apvienotās Karalistes VDAR (207. panta 1.A punktu).

([35]) Tas jo īpaši nozīmē, ka 2018. gada DAL un tādējādi šis lēmums neattiecas uz Apvienotās Karalistes kroņa teritorijām (Džērsiju, Gērnsiju un Menas Salu) un Apvienotās Karalistes aizjūras teritorijām, piemēram, Folklenda (Malvinu) Salām un Gibraltāra teritoriju.

([36]) Apvienotās Karalistes VDAR 4. panta 1., 2., 5., 7. un 8. punkts.

([37]) "Biometriskie dati" ir personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati.

([38]) "Veselības dati" ir personas dati, kas saistīti ar personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu, un kas atspoguļo informāciju par tās veselības stāvokli.

([39]) "Ģenētiskie dati" ir personas dati, kas attiecas uz personas pārmantotajām vai iegūtajām ģenētiskajām pazīmēm, sniedz unikālu informāciju par minētās personas fizioloģiju vai veselību un kas izriet jo īpaši no attiecīgās personas bioloģiskā parauga analīzes.

([40]) Saskaņā ar Apvienotās Karalistes VDAR 6. panta 1. punktu apstrāde ir likumīga vienīgi tad un tiktāl, ciktāl: a) datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem; b) apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas; c) apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu; d) apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses; e) apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras; f) apstrāde ir vajadzīga pārziņa vai trešās personas leģitīmo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm, jo īpaši, ja datu subjekts ir bērns.

vai īstenojot pārzinim likumīgi piešķirtas oficiālas pilnvaras) ietver personas datu apstrādi, kas ir vajadzīga tiesas spriešanai, parlamenta palātu funkciju izpildei, tādas funkcijas izpildei, kuru persona ir pilnvarota veikt saskaņā ar likumdošanas instrumentu vai tiesību normu, valsts, valdības ministra vai valdības departamenta funkciju izpildei, vai darbību, kas atbalsta vai sekmē demokrātisku iesaistīšanos.

(26) Arī attiecībā uz piekrišanu (vienu no likumīgas apstrādes pamatiem) Apvienotās Karalistes VDAR ir saglabāti negrozīti Regulas (ES) 2016/679 7. pantā paredzētie nosacījumi, proti, pārzinim jāspēj uzskatāmi parādīt, ka datu subjekts ir piekritis savu personas datu apstrādei, ir jāiesniedz rakstisks piekrišanas pieprasījums, izmantojot skaidru un vienkāršu valodu, datu subjektam jābūt tiesībām jebkurā laikā atsaukt piekrišanu, un, novērtējot to, vai piekrišana ir dota brīvi, jāņem vērā tas, vai līguma izpilde ir atkarīga no piekrišanas tādai personas datu apstrādei, kura nav nepieciešama minētā līguma izpildei. Turklāt saskaņā ar Apvienotās Karalistes VDAR 8. pantu informācijas sabiedrības pakalpojumu nodrošināšanas kontekstā bērna sniegta piekrišana ir likumīga tikai tad, ja bērns ir vismaz 13 gadu vecs. Šis vecums atbilst Regulas (ES) 2016/679 8. pantā noteiktajai vecuma grupai.

2.5.2. *Īpašu kategoriju personas datu apstrāde*

(27) Būtu vajadzīgas īpašas garantijas gadījumos, kad tiek apstrādāti "īpašu kategoriju" dati.

(28) Apvienotās Karalistes VDAR un 2018. gada DAL ir paredzētas konkrētas prasības attiecībā uz īpašu kategoriju personas datu apstrādi. Šīs kategorijas ir noteiktas Apvienotās Karalistes VDAR 9. panta 1. punktā tādā pašā veidā kā Regulā (ES) 2016/679 (sk. iepriekš 23. apsvērumu). Saskaņā ar Apvienotās Karalistes VDAR 9. pantu īpašu kategoriju datu apstrāde principā ir aizliegta, izņemot gadījumus, kad ir piemērojami īpaši izņēmumi.

(29) Šie izņēmumi (uzskaitīti Apvienotās Karalistes VDAR 9. panta 2. un 3. punktā) pēc būtības neatšķiras no Regulas (ES) 2016/679 9. panta 2. un 3. punktā noteiktajiem izņēmumiem. Ja datu subjekts nav devis nepārprotamu piekrišanu šo personas datu apstrādei, īpašu kategoriju personas datu apstrāde ir atļauta tikai konkrētos un ierobežotos apstākļos. Vairumā gadījumu sensitīvu datu apstrādei jābūt nepieciešamai (jeb vajadzīgai) konkrētam attiecīgajos noteikumos paredzētam nolūkam (sk. 9. panta 2. punkta b), c), f), g), h), i) un j) apakšpunktu).

(30) Turklāt, ja Apvienotās Karalistes VDAR 9. panta 2. punktā minētajā izņēmumā noteikta prasība par likumā paredzētu pilnvarojumu vai sniegta atsauce uz sabiedrības interesēm, 2018. gada DAL 10. pantā un 1. pielikumā ir sīkāk izklāstīti nosacījumi, kas ir jāizpilda, lai varētu piemērot izņēmumu. Piemēram, saistībā ar sensitīvu datu apstrādi nolūkā aizsargāt "sabiedrības veselību" (Apvienotās Karalistes VDAR 9. panta 2. punkta i) apakšpunkts) 1. pielikuma 1. daļas 3. punkta b) apakšpunktā ir noteikts, ka papildus nepieciešamības pārbaudei šādu apstrādi veic "veselības aprūpes speciālists vai veselības aprūpes speciālista atbildībā", vai "cita persona, kurai ir jāievēro konfidencialitāte saskaņā ar likumdošanas instrumentu vai tiesību normu", tostarp saskaņā ar vispāratzītu anglosakšu tiesībās noteiktu konfidencialitātes ievērošanas pienākumu.

(31) Ja sensitīvus datus apstrādā būtisku sabiedrības interešu dēļ (Apvienotās Karalistes VDAR 9. panta 2. punkta g) apakšpunkts), 2018. gada DAL 1. pielikuma 2. daļā ir sniegts izsmeļošs tādu nolūku saraksts, kurus var uzskatīt par būtiskām sabiedrības interesēm, un attiecībā uz katru no šiem nolūkiem ir norādīti konkrēti papildu nosacījumi. Piemēram, organizāciju augstākā līmeņa darbinieku rasu un etniskās daudzveidības veicināšana ir atzīta par būtiskām sabiedrības interesēm. Uz sensitīvu datu apstrādi, kas veicama šajā konkrētajā nolūkā, attiecas sīki izstrādātas prasības, tostarp prasība, ka apstrāde ir jāveic tāda procesa ietvaros, kura mērķis ir noteikt darbam vadošos amatos piemērotas personas, ka apstrāde ir nepieciešama rasu un etniskās daudzveidības veicināšanai un ka šīs apstrādes rezultātā datu subjektam nevarētu tikt radīts būtisks kaitējums vai būtiska spriedze.

(32) 2018. gada DAL 11. panta 1. punktā ir paredzēti nosacījumi, kas attiecas uz personas datu apstrādi Apvienotās Karalistes VDAR 9. panta 3. punktā aprakstītajās situācijās saistībā ar slepenības ievērošanas pienākumu. Tie cita starpā attiecas uz situācijām, kad personas datu apstrādi veic veselības aprūpes speciālists vai veselības aprūpes speciālista atbildībā, vai sociālā darba speciālists, vai cita persona, kurai saskaņā ar likumdošanas instrumentu vai tiesību normu attiecīgajā situācijā ir jāievēro konfidencialitāte.

(33) Turklāt, lai izmantotu daudzus no Apvienotās Karalistes VDAR 9. panta 2. punktā uzskaitītajiem izņēmumiem, ir jānodrošina atbilstošas un īpašas garantijas. 2018. gada DAL 1. pielikumā paredzētie apstrādes nosacījumi paredz dažādas garantijas atkarībā no apstrādes rakstura un datu subjektu tiesībām un brīvībām radītā riska līmeņa. 1. pielikumā ir paredzēti nosacījumi attiecībā uz katru apstrādes situāciju.

(34) Lai nodrošinātu atbilstību konkrētam juridiskajam pamatam, dažos gadījumos 2018. gada DAL ir reglamentēti un ierobežoti sensitīvu datu veidi, kurus drīkst apstrādāt. Piemēram, 1. pielikuma 8. punktā ir atļauta sensitīvu datu apstrāde nolūkā veicināt iespēju vienlīdzību vai vienlīdzīgas attieksmes principa ievērošanu. Šo apstrādes nosacījumu var izmantot tikai tad, ja dati atklāj rases vai etnisko piederību, reliģisko vai filozofisko pārliecību, seksuālo orientāciju vai ja dati ir veselības dati.

(35) Dažos gadījumos 2018. gada DAL ir noteikti ierobežojumi attiecībā uz to, kāda veida pārziņi drīkst izmantot apstrādes nosacījumu. Piemēram, 1. pielikuma 23. punktā ir paredzēta sensitīvu datu apstrāde saistībā ar vēlētu pārstāvju sniegtām atbildēm sabiedrībai. Šo apstrādes nosacījumu var izmantot tikai tad, ja pārzinis ir ievēlētais pārstāvis vai rīkojas ievēlētā pārstāvja vārdā.

(36) Dažos citos gadījumos 2018. gada DAL ir noteikti ierobežojumi attiecībā uz datu subjektu kategorijām, kurām var piemērot apstrādes nosacījumu. Piemēram, 1. pielikuma 21. punktā ir reglamentēta sensitīvu datu apstrāde saistībā ar arodpensiju shēmām. Šo nosacījumu var izmantot tikai tad, ja attiecīgais datu subjekts ir shēmas dalībnieka māsa/brālis, vecāks, vecvecāks vai vecvecvecāks.

(37) Turklāt, izmantojot Apvienotās Karalistes VDAR 9. panta 2. punktā uzskaitītos izņēmumus, kas ir sīkāk izklāstīti 2018. gada DAL 10. pantā un 1. pielikumā, pārzinim vairumā gadījumu ir jāsagatavo "atbilstošs politikas dokuments". Tajā ir jāapraksta pārziņa procedūras, kuru mērķis ir nodrošināt atbilstību Apvienotās Karalistes VDAR 5. pantā noteiktajiem principiem. Tajā arī jānosaka politika attiecībā uz datu glabāšanu un dzēšanu, norādot iespējamo glabāšanas ilgumu. Pārziņiem attiecīgā gadījumā šis dokuments ir jāpārskata un jāatjaunina. Pārzinim šis politikas dokuments ir jāsaglabā sešus mēnešus pēc apstrādes beigām un pēc pieprasījuma jādara tas pieejams informācijas komisāram ([41]).

(38) Saskaņā ar 2018. gada DAL 1. pielikuma 41. punktu politikas dokumentam vienmēr jāpievieno apstrādes darbību padziļinātas uzskaites reģistrs. Šajā reģistrā ir jāatspoguļo politikas dokumentā iekļauto saistību izpilde, t. i., vai dati tiek dzēsti vai saglabāti saskaņā ar politiku. Ja politika nav ievērota, reģistrā ir jānorāda iemesli. Reģistrā arī jāapraksta tas, kā tiek nodrošināta apstrādes atbilstība Apvienotās Karalistes VDAR 6. pantam (apstrādes likumīgums), kā arī jānorāda, kurš no 2018. gada DAL 1. pielikumā uzskaitītajiem nosacījumiem ir piemērots konkrētajā situācijā.

(39) Visbeidzot, arī Apvienotās Karalistes VDAR tāpat kā Regulā (ES) 2016/679 ir paredzētas vispārējas garantijas attiecībā uz noteiktām īpašu kategoriju datu apstrādes darbībām. Apvienotās Karalistes VDAR 35. pantā ir noteikta prasība veikt novērtējumu par ietekmi uz datu aizsardzību, ja īpašas datu kategorijas tiek apstrādātas plašā mērogā. Saskaņā ar Apvienotās Karalistes VDAR 37. pantu gadījumā, ja pārziņa vai apstrādātāja pamatdarbības ietver īpašu kategoriju datu apstrādi plašā mērogā, pārzinim vai apstrādātājam ir jāieceļ datu aizsardzības speciālists.

(40) Saistībā ar personas datiem par sodāmību un pārkāpumiem Apvienotās Karalistes VDAR 10. pants ir identisks ar Regulas (ES) 2016/679 10. pantu. Tajā ir noteikts, ka apstrādāt personas datus par sodāmību un pārkāpumiem ir atļauts tikai oficiālas iestādes kontrolē vai tad, ja apstrādi atļauj valsts tiesību akti, paredzot atbilstošas garantijas datu subjektu tiesībām un brīvībām.

(41) Ja personas dati par sodāmību un pārkāpumiem netiek apstrādāti oficiālas iestādes kontrolē, 2018. gada DAL 10. panta 5. punktā ir noteikts, ka šādu apstrādi var veikt tikai konkrētos nolūkos / īpašās situācijās, kas ir norādītas 2018. gada DAL 1. pielikuma 1., 2. un 3. daļā, un ka uz šādu apstrādi attiecas konkrētas prasības, kas ir noteiktas saistībā ar katru no šiem nolūkiem/situācijām. Piemēram, datus par sodāmību drīkst apstrādāt bezpeļņas struktūras, ja apstrādi veic a) fonds, apvienība vai cita bezpeļņas struktūra, kas to dara ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi, veicot leģitīmas darbības un nodrošinot atbilstošas garantijas, un b) ar nosacījumu, i) ka apstrāde attiecas tikai uz šīs struktūras locekļiem vai bijušajiem locekļiem, vai personām, kas ar šo struktūru uztur regulārus sakarus saistībā ar tās nolūkiem, un ii) ka bez datu subjektu piekrišanas personas datus neizpauž ārpus minētās struktūras.

([41]) 2018. gada DAL 1. pielikuma 38.–40. punkts.

(42) Turklāt 2018. gada DAL 1. pielikuma 3. daļā ir paredzēti papildu apstākļi, kuros var izmantot datus par sodāmību un kuri atbilst Regulā (ES) 2016/679 9. panta 2. punktā un Apvienotās Karalistes VDAR noteiktajiem sensitīvu datu apstrādes juridiskajam pamatam (piemēram, datu subjekta dota piekrišana, personas vitālas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu, ja datu subjekts datus jau ir apzināti publiskojis, ja apstrāde ir nepieciešama, lai celtu, īstenotu vai aizstāvētu likumīgas prasības utt.).

2.5.3. *Nolūka ierobežojums, precizitāte, datu minimizēšana, glabāšanas ierobežojums un datu drošība*

(43) Personas dati būtu jāapstrādā konkrētā nolūkā, un pēc tam tos var izmantot, ciktāl tas nav pretrunā apstrādes nolūkam.

(44) Šis princips ir paredzēts Regulas (ES) 2016/679 5. panta 1. punkta b) apakšpunktā un bez izmaiņām ir saglabāts Apvienotās Karalistes VDAR 5. panta 1. punkta b) apakšpunktā. Apvienotās Karalistes VDAR 6. panta 4. punkta a)–e) apakšpunktā bez būtiskām izmaiņām ir saglabāti arī nosacījumi turpmākai saderīgai apstrādei saskaņā ar Regulas (ES) 2016/679 6. panta 4. punktu.

(45) Turklāt datiem būtu jābūt precīziem un nepieciešamības gadījumā atjauninātiem. Tiem vajadzētu būt arī adekvātiem, atbilstīgiem un nevajadzētu būt pārmērīgiem, ņemot vērā nolūkus, kādos tie tiek apstrādāti, un tie principā nebūtu jāglabā ilgāk nekā nepieciešams nolūkiem, kādos personas datus apstrādā.

(46) Šie datu minimizēšanas, precizitātes un glabāšanas ierobežojuma principi ir izklāstīti Regulas (ES) 2016/679 5. panta 1. punkta c)–e) apakšpunktā, un tie bez izmaiņām ir saglabāti Apvienotās Karalistes VDAR 5. panta 1. punkta c)–e) apakšpunktā.

(47) Personas dati arī būtu jāapstrādā tā, ka tiek nodrošināta to drošība, kas ietver aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu. Tālab uzņēmējiem būtu jāveic atbilstoši tehniskie vai organizatoriskie pasākumi, lai aizsargātu personas datus no iespējamiem apdraudējumiem. Šie pasākumi būtu jānovērtē, ņemot vērā faktisko situāciju un saistītās izmaksas.

(48) Datu drošība Apvienotās Karalistes tiesību aktos ir nostiprināta, paredzot konfidencialitātes un integritātes principu Apvienotās Karalistes VDAR 5. panta 1. punkta f) apakšpunktā, kā arī Apvienotās Karalistes VDAR 32. pantā par apstrādes drošību. Šie noteikumi ir identiski ar attiecīgajiem Regulas (ES) 2016/679 nosacījumiem. Turklāt saskaņā ar tādiem pašiem nosacījumiem, kādi ir paredzēti Regulas (ES) 2016/679 33. un 34. pantā, Apvienotās Karalistes VDAR ir noteikta prasība paziņot par personas datu aizsardzības pārkāpumu uzraudzības iestādei (Apvienotās Karalistes VDAR 33. pants) un informēt par personas datu aizsardzības pārkāpumu datu subjektu (Apvienotās Karalistes VDAR 34. pants).

2.5.4. *Pārredzamība*

(49) Datu subjektiem vajadzētu būt informētiem par viņu personas datu apstrādes galvenajām iezīmēm.

(50) To nodrošina Apvienotās Karalistes VDAR 13. un 14. pants, kurā papildus vispārējam pārredzamības principam ir paredzēti noteikumi par datu subjektam sniedzamo informāciju ([42]). Salīdzinājumā ar attiecīgajiem Regulas (ES) 2016/679 pantiem Apvienotās Karalistes VDAR šie noteikumi nav būtiski grozīti. Tomēr, tāpat kā Regulas (ES) 2016/679 gadījumā, uz šajos pantos paredzētajām pārredzamības prasībām attiecas vairāki 2018. gada DAL noteikti izņēmumi (sk. 55.–72. apsvērumu).

([42]) 13. panta 1. punkta f) apakšpunktā un 14. panta 1. punkta f) apakšpunktā atsauces uz Komisijas lēmumiem par aizsardzības līmeņa pietiekamību ir aizstātas ar atsaucēm uz līdzvērtīgu Apvienotās Karalistes instrumentu, t. i., 2018. gada DAL paredzētajiem noteikumiem par aizsardzības līmeņa pietiekamību. Turklāt 14. panta 5. punkta c) un d) apakšpunktā atsauces uz ES vai dalībvalstu tiesību aktiem ir aizstātas ar atsaucēm uz valsts tiesību aktiem (kā tādu valsts tiesību aktu piemērus, uz kuriem varētu attiekties 14. panta 5. punkta c) apakšpunkts, Apvienotā Karaliste ir minējusi 2013. gada Likuma par metāllūžņu pārdevējiem 7. pantu, kurā ir paredzēti noteikumi par metāllūžņu pārdošanas licenču reģistru, vai 2006. gada Uzņēmumu likuma 35. daļu, kurā ir paredzēti noteikumi par *Registrar of companies*). Līdzīgā kārtā tāda valsts tiesību akta piemērs, uz kuru varētu attiekties 14. panta 5. punkta d) apakšpunkts, varētu ietver tiesību aktus, kuros ir paredzēti noteikumi par profesionālo konfidencialitāti, vai darba līgumos noteiktas saistības, vai anglosakšu tiesībās noteiktu konfidencialitātes ievērošanas pienākumu (piemēram, veselības aprūpes speciālistu, cilvēkresursu speciālistu, sociālo darbinieku u. c. apstrādāti personas dati).

2.5.5. *Individuālās tiesības*

(51) Datu subjektiem būtu jābūt noteiktām tiesībām, kas ir īstenojamas attiecībā uz pārzini vai apstrādātāju, jo īpaši tiesībām piekļūt datiem, tiesībām iebilst pret apstrādi un tiesībām panākt datu labošanu vai dzēšanu. Tajā pašā laikā uz šīm tiesībām var attiekties ierobežojumi, ja tie ir nepieciešami un samērīgi, lai garantētu sabiedrisko drošību vai citu svarīgu vispārējo sabiedrības interešu mērķu īstenošanu.

2.5.5.1. Materiālās tiesības

(52) Apvienotās Karalistes VDAR nodrošina personām tādas pašas īstenojamas tiesības kā Regula (ES) 2016/679. Noteikumi, kuros ir paredzētas personu tiesības, ir saglabāti Apvienotās Karalistes VDAR bez būtiskām izmaiņām,

(53) Šie noteikumi ietver datu subjekta piekļuves tiesības (Apvienotās Karalistes VDAR 15. pants), tiesības uz labot (Apvienotās Karalistes VDAR 16. pants), tiesības uz dzēšanu (Apvienotās Karalistes VDAR 17. pants), tiesības uz apstrādes ierobežošanu (Apvienotās Karalistes VDAR 18. pants), pienākumu ziņot par personas datu labošanu vai dzēšanu, vai apstrādes ierobežošanu (Apvienotās Karalistes VDAR 19. pants), tiesības uz datu pārnesamību (Apvienotās Karalistes VDAR 20. pants), kā arī tiesības iebilst (Apvienotās Karalistes VDAR 21. pants) ([43]). Tiesības iebilst ietver arī Regulas (ES) 2016/679 21. panta 2. un 3. punktā minētās datu subjekta tiesības iebilst pret personas datu apstrādi tiešās tirgvedības vajadzībām. Turklāt saskaņā ar 2018. gada DAL 122. pantu informācijas komisāram ir jāsagatavo prakses kodekss saistībā ar tiešās tirgvedības veikšanu saskaņā ar datu aizsardzības tiesību aktu prasībām (un 2003. gada Noteikumiem par privātumu un elektroniskajiem sakariem (EK direktīva)), kā arī tādiem citiem norādījumiem labas prakses veicināšanai tiešās tirgvedības jomā, kurus komisārs uzskata par atbilstošiem. Informācijas komisāra birojs pašlaik izstrādā tiešās tirgvedības kodeksu ([44]).

(54) VDAR 22. pantā paredzētās datu subjekta tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu, bez būtiskām izmaiņām ir saglabātas arī Apvienotās Karalistes VDAR. Tomēr ir pievienots 3.A punkts nolūkā sniegt atsauci uz 2018. gada DAL 14. pantu, kurā ir izklāstītas datu subjektu tiesību, brīvību un leģitīmo interešu garantijas gadījumos, kad tiek veikta datu apstrāde atbilstīgi Apvienotās Karalistes VDAR 22. panta 2. punkta b) apakšpunktam. Tas attiecas tikai uz gadījumiem, kad šāda lēmuma pamatā ir atļauja vai prasība saskaņā ar Apvienotās Karalistes tiesību aktiem, un neattiecas uz gadījumiem, kad šāds lēmums ir nepieciešams saskaņā ar līgumu vai ir pieņemts, pamatojoties uz datu subjekta nepārprotamu piekrišanu. Ja ir piemērojams 2018. gada DAL 14. pants, pārzinim, tiklīdz tas ir praktiski iespējams, ir rakstiski jāpaziņo datu subjektam par to, ka lēmums ir pieņemts, pamatojoties tikai uz automatizētu apstrādi. Datu subjektam ir tiesības pieprasīt, lai pārzinis mēneša laikā pēc paziņojuma saņemšanas pārskatītu lēmumu vai pieņemtu jaunu lēmumu, kura pamatā nav tikai automatizēta apstrāde. Ministrs ir pilnvarots pieņemt papildu garantijas saistībā ar automatizētu lēmumu pieņemšanu. Šīs pilnvaras vēl nav izmantotas.

2.5.5.2. Individuālo tiesību ierobežojumi un citi noteikumi

(55) 2018. gada DAL ir paredzēti vairāki individuālo tiesību ierobežojumi, kas iederas Apvienotās Karalistes VDAR 23. pantā noteiktajā regulējumā. Šajā regulējumā nav iekļauti nekādi ierobežojumi attiecībā uz tiesībām iebilst pret tiešo tirgvedību, kā paredzēts Apvienotās Karalistes VDAR 21. panta 2. un 3. punktā, vai attiecībā uz tiesībām nebūt automatizētas lēmumu pieņemšanas subjektam, kā paredzēts Apvienotās Karalistes VDAR 22. pantā.

(56) Ierobežojumi ir izklāstīti 2018. gada DAL 2.–4. pielikumā. Apvienotās Karalistes iestādes ir skaidrojušas, ka to rīcību nosaka divi principi: konkrētības princips (detalizētas pieejas izmantošana, sadalot plašus ierobežojumus vairākos konkrētos noteikumos) un nosacījumu princips (katrs noteikums ir papildināts ar garantijām ierobežojumu vai nosacījumu veidā nolūkā nepieļaut ļaunprātīgu izmantošanu) ([45]).

([43]) 17. panta 1. punkta e) apakšpunktā un 17. panta 3. punkta b) apakšpunktā atsauces uz ES vai dalībvalstu tiesību aktiem ir aizstātas ar atsaucēm uz valsts tiesību aktiem (kā tādu valsts tiesību aktu piemērus, uz kuriem attiecas 17. panta 1. punkta e) apakšpunkts, Apvienotā Karaliste ir minējusi 2006. gada Noteikumus par izglītību (informācija par skolēniem) (Anglija), kuros noteikta prasība dzēst skolēnu vārdus un uzvārdus no skolas reģistriem pēc tam, kad viņi ir pametuši skolu, vai 1983. gada Likuma par medicīnu 34. F pantu, kurā ir paredzēti noteikumi par vārdu un uzvārdu dzēšanu no ģimenes ārstu reģistra un speciālistu reģistra.

([44]) Prakses kodeksa projekts ir pieejams vietnē https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf.

([45]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, E iedaļa "Ierobežojumi", 1. lpp., pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

(57) Apvienotās Karalistes VDAR 23. panta 1. punktā aprakstītie ierobežojumi ir izstrādāti nolūkā nodrošināt to piemērošanu tikai konkrētos apstākļos, ja šī piemērošana ir nepieciešama demokrātiskā sabiedrībā un ir samērīga ar minēto ierobežojumu leģitīmo mērķi. Turklāt saskaņā ar iedibināto judikatūru attiecībā uz ierobežojumu interpretāciju atbrīvojumu no datu aizsardzības režīma var piemērot tikai konkrētā gadījumā, ja šāda piemērošana ir nepieciešama un samērīga ([46]). Ir noteikts, ka nepieciešamības pārbaudei ir jābūt "stingrai, un tā paredz, ka jebkuram subjekta tiesību ierobežojumam ir jābūt samērīgam ar sabiedrības interešu apdraudējumu. Tādējādi pārbaude ietver klasisku samērīguma analīzi ([47])".

(58) Šo ierobežojumu mērķi atbilst Regulas (ES) 2016/679 23. pantā uzskaitīto ierobežojumu mērķim, izņemot ar valsts drošību un aizsardzību saistītos ierobežojumus, kas ir reglamentēti 2018. gada DAL 26. pantā, tomēr uz tiem attiecas tādas pašas nepieciešamības un samērīguma prasības (sk. 63.–66. apsvērumu).

(59) Daži no ierobežojumiem, piemēram, ierobežojumi saistībā ar noziegumu novēršanu vai atklāšanu, ierobežojumi saistībā ar likumpārkāpēju aizturēšanu vai saukšanu pie atbildības, kā arī ierobežojumi saistībā ar nodokļu vai maksājumu aprēķinu vai iekasēšanu ([48]), ļauj ierobežot visas individuālās tiesības un pārredzamības nodrošināšanas pienākumus (izņemot 21. panta 2. punktā un 22. pantā noteiktās tiesības). Pārējo ierobežojumu piemērošanas joma aptver tikai pārredzamības nodrošināšanas pienākumus un piekļuves tiesības, piemēram, ierobežojumus saistībā ar advokāta un klienta saziņas konfidencialitāti ([49]), ierobežojumus saistībā ar tiesībām uz atbrīvojumu no pienākuma sniegt informāciju, no kuras izrietētu pašapsūdzība ([50]), kā arī ierobežojumus saistībā ar uzņēmumu finansēm, jo īpaši iekšējās informācijas izmantošanas novēršanu ([51]). Daži ierobežojumi paredz iespēju ierobežot pārziņa pienākumu paziņot par personas datu aizsardzības pārkāpumu datu subjektam un apstrādes nolūka ierobežojuma, likumīguma, godprātības un pārredzamības principus ([52]).

(60) Atsevišķi ierobežojumi automātiski un pilnā apmērā attiecas uz noteiktiem personas datu apstrādes veidiem (piemēram, ja personas datus apstrādā nolūkā izvērtēt personas piemērotību amatam tiesu iestādē vai ja personas datus apstrādā tiesa, tribunāls vai persona, kas veic ar tiesu iestāžu darbu saistītus pienākumus, pārredzamības nodrošināšanas pienākumu un individuālo tiesību piemērošana ir izslēgta).

(61) Tomēr vairumā gadījumu 2018. gada DAL 2. pielikuma attiecīgajā punktā ir noteikts, ka ierobežojumi ir piemērojami tikai tad, ja / ciktāl noteikumu piemērošana "varētu kaitēt" šā ierobežojuma leģitīmā mērķa īstenošanai. Piemēram, Apvienotās Karalistes VDAR uzskaitītie noteikumi neattiecas uz personas datiem, kas apstrādāti nolūkā novērst vai atklāt noziegumus, aizturēt likumpārkāpējus vai saukt viņus pie atbildības vai aprēķināt vai iekasēt nodokļus vai maksājumus, "ciktāl šo noteikumu piemērošana varētu kaitēt" kādas iepriekš minētās darbības izpildei ([53]).

(62) Apvienotās Karalistes tiesas pastāvīgi ir interpretējušas standartu "varētu kaitēt" kā "ļoti būtisku un nopietnu kaitējuma iespēju noteiktajām sabiedrības interesēm" ([54]). Tādējādi ierobežojums, uz ko attiecas kaitējuma pārbaude, var tikt piemērots tikai tad un tiktāl, ja pastāv ļoti būtiska un nopietna iespēja, ka konkrētu tiesību piešķiršana kaitētu konkrētajām sabiedrības interesēm. Pārzinis ir atbildīgs par to, lai katrā gadījumā atsevišķi novērtētu, vai šie nosacījumi ir ievēroti ([55]).

(63) Papildus 2018. gada DAL 2. pielikumā paredzētajiem ierobežojumiem 2018. gada DAL 26. pantā ir paredzēts atbrīvojums, ko drīkst piemērot atsevišķiem Apvienotās Karalistes VDAR un 2018. gada DAL noteikumiem, ja šā atbrīvojuma piemērošana ir nepieciešama nolūkā garantēt valsts drošības vai aizsardzības mērķu īstenošanu. Šis atbrīvojums attiecas uz datu aizsardzības principiem (izņemot likumīguma principu), pārredzamības nodrošināšanas pienākumiem, datu subjekta tiesībām, pienākumu paziņot par personas datu aizsardzības pārkāpumu, noteikumiem par datu starptautisku nosūtīšanu, atsevišķiem informācijas komisāra pienākumiem un pilnvarām, kā arī noteikumiem par tiesiskās aizsardzības līdzekļiem, atbildību un sodiem, izņemot noteikumu par

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

([47]) *Guriev v Community Safety Development (United Kingdom) Ltd* [2016], EWHC 643 (QB), 43. punkts. Lai iegūtu informāciju par šo jautājumu, sk. arī *Lin v Commissioner of Police for the Metropolis* [2015], EWHC 2484 (QB), 80. punkts.

([48]) 2018. gada DAL 2. pielikuma 2. punkts.

([49]) 2018. gada DAL 2. pielikuma 19. punkts.

([50]) 2018. gada DAL 2. pielikuma 20. punkts.

([51]) 2018. gada DAL 2. pielikuma 21. punkts.

([52]) Piemēram, ierobežojumi attiecībā uz tiesībām saņemt paziņojumu par personas datu aizsardzības pārkāpumu ir atļauti tikai saistībā ar noziegumiem un nodokļiem (2018. gada DAL 2. pielikuma 2. punkts), parlamentārajām privilēģijām (2018. gada DAL 2. pielikuma 13. punkts), kā arī datu apstrādi žurnālistikas, akadēmiskos, mākslinieciskos un literāros nolūkos (2018. gada DAL 2. pielikuma 26. punkts).

([53]) 2018. gada DAL 2. pielikuma 2. punkts.

([54]) *R (Lord) v Secretary of State for the Home Department* [2003], EWHC 2073 (Admin), 100. punkts, un *Guriev v Community Safety Development (United Kingdom) Ltd* [2016], EWHC 643 (QB), 43. punkts.

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

vispārējiem nosacījumiem attiecībā uz administratīvo naudas sodu piemērošanu, kas ir paredzēts Apvienotās Karalistes VDAR 83. pantā, kā arī noteikumu par sodiem, kas ir iekļauts Apvienotās Karalistes VDAR 84. pantā. Turklāt ar 2018. gada DAL 28. pantu ir grozīta 9. panta 1. punkta piemērošanas kārtība nolūkā atļaut apstrādāt Apvienotās Karalistes VDAR 9. panta 1. punktā minētās īpašās datu kategorijas, ciktāl apstrādi veic, lai garantētu valsts drošības un aizsardzības mērķu īstenošanu, kā arī nodrošinot atbilstošas garantijas attiecībā uz datu subjekta tiesībām un brīvībām ([56]).

(64) Atbrīvojumu var piemērot tikai tad, ja un ciktāl tas ir nepieciešams nolūkā garantēt valsts drošību vai aizsardzību. Tāpat kā pārējo 2018. gada DAL paredzēto atbrīvojumu gadījumā, šis atbrīvojums pārzinim ir jāizvērtē un jāpiemēro katrā gadījumā atsevišķi. Turklāt visos atbrīvojuma piemērošanas gadījumos ir jāievēro cilvēktiesību standarti (kuru pamatā ir 1998. gada Cilvēktiesību likums), kas paredz, ka demokrātiskā sabiedrībā tiesību uz privātumu ierobežojumiem vienmēr jāatbilst nepieciešamības un samērīguma principiem ([57]).

(65) Šo atbrīvojuma interpretāciju apstiprina Informācijas komisāra birojs (IKB), kas ir izdevis detalizētus norādījumus par valsts drošības un aizsardzības atbrīvojuma piemērošanu, skaidri nosakot, ka pārzinim tas jāapsver un jāpiemēro katrā gadījumā atsevišķi ([58]). Konkrētāk, norādījumos uzsvērts, ka šis nav vispārējs atbrīvojums un ka tā piemērošanai nepietiek ar to, ka datus apstrādā valsts drošības vajadzībām. Turpretim pārzinim, kas to izmanto, jāapliecina, ka pastāv reāla iespēja negatīvi ietekmēt valsts drošību, un, ja nepieciešams, pārzinim jāsniedz IKB pierādījumi tam, kādēļ šis atbrīvojums izmantots. Norādījumos iekļauts kontrolsaraksts un vairāki piemēri, kas sīkāk precizē nosacījumus, saskaņā ar kādiem šo atbrīvojumu var piemērot.

(66) Tāpēc fakts, ka datus apstrādā valsts drošības vai aizsardzības nolūkos, pats par sevi nav pietiekams pamatojums atbrīvojuma piemērošanai. Pārzinim ir jāņem vērā faktiskās sekas valsts drošības jomā, kas izrietētu, ja tam būtu jāievēro konkrētā datu aizsardzības prasība. Atbrīvojumu var piemēroti tikai tiem konkrētajiem noteikumiem, kas ir paredzēti kā tādi, kas rada risku, un tas ir jāpiemēro pēc iespējas ierobežotākā veidā ([59]).

(67) Šo pieeju ir apstiprinājis Informācijas tribunāls ([60]). Lietā *Baker v Secretary of State for the Home Department* (*"Baker v Secretary of State"*) tika nolemts, ka piemērot atbrīvojumu sakarā ar valsts drošību kā vispārēju atbrīvojumu izlūkdienestiem iesniegtiem piekļuves pieprasījumiem ir nelikumīgi. Tika noteikts, ka atbrīvojums ir piemērojams katrā gadījumā atsevišķi, izvērtējot katru pieprasījumu pēc būtības un ņemot vērā personu tiesības uz privātās dzīves neaizskaramību ([61]).

([56]) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju gadījumos, kad apstrādi veic valsts drošības kontekstā, pārziņi apstrādei parasti piemēro uzlabotas garantijas un drošības pasākumus, ņemot vērā apstrādes sensitīvo raksturu. Tas, kādas garantijas ir piemērotas, ir atkarīgs no veiktās apstrādes radītajiem riskiem. Tās varētu ietvert ierobežojumus attiecībā uz piekļuvi datiem, nosakot, ka tiem var piekļūt tikai pilnvarotas personas ar atbilstošu drošības pielaidi, stingrus ierobežojumus attiecībā uz datu apmaiņu, kā arī augsta drošības standarta piemērošanu uzglabāšanas un apstrādes procedūrām.

([57]) Sk. arī *Guriev v Community Safety Development (United Kingdom) Ltd* [2016], EWHC 643 (QB), 45. punkts; *Lin v Commissioner of the Police for the Metropolis* [2015], EWHC 2484 (QB), 80. punkts.

([58]) Sk. IKB norādījumus par valsts drošības un aizsardzības atbrīvojumu, pieejami vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/.

([59]) Saskaņā ar Apvienotās Karalistes iestāžu sniegtu piemēru, ja persona, kas tiek turēta aizdomās par terorismu un par kuru MI5 aktīvi veic izmeklēšanu, Iekšlietu ministrijai iesniegtu piekļuves pieprasījumu (piemēram, tāpēc, ka šai personai ir domstarpības ar Iekšlietu ministriju ar imigrāciju saistītos jautājumos), jebkuri dati, kurus MI5 būtu sniedzis Iekšlietu ministrijai saistībā ar notiekošo izmeklēšanu un kuri varētu radīt kaitējumu saistībā ar sensitīviem avotiem, metodēm un paņēmieniem un/vai palielināt personas radītos draudus, būtu jāaizsargā pret izpaušanu datu subjektam. Domājams, ka šādā situācijā prasības 26. pantā noteiktā atbrīvojuma piemērošanai būtu izpildītas un valsts drošības garantēšanas nolūkā būtu jāpiemēro atbrīvojums no pienākuma izpaust informāciju. Tomēr, ja Iekšlietu ministrijas rīcībā būtu arī ar MI5 izmeklēšanu nesaistīti šīs personas dati un šo informāciju būtu iespējams sniegt, neradot kaitējuma risku valsts drošībai, izvērtējot informācijas izpaušanu attiecīgajai personai, atbrīvojums sakarā ar valsts drošību nebūtu piemērojams. IKB pašlaik izstrādā norādījumus par to, kādu pieeju pārziņi varētu piemērot 26. pantā paredzētā atbrīvojuma izmantošanai. Paredzams, ka šie norādījumi tiks publicēti 2021. gada marta beigās.

([60]) Informācijas tribunāls tika izveidots ar datu aizsardzību saistītu pārsūdzību izskatīšanai saskaņā ar 1984. gada Datu aizsardzības likumu. Apvienotās Karalistes tribunālu sistēmas struktūras reformas ietvaros Informācijas tribunāls 2010. gadā kļuva par daļu no pirmā līmeņa tribunāla Vispārējās regulatīvās palātas.

([61]) Sk. *Baker v Secretary of State for the Home Department* [2001], UKIT NSA2 (*"Baker v Secretary of State"*).

2.5.6. *Ierobežojumi saistībā ar personas datiem, ko apstrādā žurnālistikas, mākslinieciskos, akadēmiskos un literāros nolūkos, kā arī arhivēšanas un pētniecības nolūkos*

(68) Apvienotās Karalistes VDAR 85. panta 2. punktā ir atļauts noteikums, kas paredz, ka žurnālistikas, mākslinieciskos, akadēmiskos un literāros nolūkos veiktai personas datu apstrādei var piemērot atbrīvojumu no vairākiem Apvienotās Karalistes VDAR noteikumiem. 2018. gada DAL 2. pielikuma 5. daļā ir noteikti atbrīvojumi attiecībā uz apstrādi, ko veic šādos nolūkos. Tajā ir paredzēti atbrīvojumi no datu aizsardzības principu piemērošanas (izņemot integritātes un konfidencialitātes principu), apstrādes juridiskais pamats (tostarp īpašas datu kategorijas, dati par sodāmību utt.), piekrišanas nosacījumi, pārredzamības nodrošināšanas pienākumi, datu subjektu tiesības un pienākums paziņot par datu aizsardzības pārkāpumu, prasība apspriesties ar informācijas komisāru pirms tādas datu apstrādes, kas ir saistīta ar augstu risku, kā arī noteikumi par datu starptautisku nosūtīšanu ([62]). Šajā sakarā Apvienotās Karalistes VDAR būtiski neatkāpjas no Regulas (ES) 2016/679, kuras 85. pantā arī ir paredzēta iespēja piemērot atbrīvojumu no vairāku šīs regulas prasību piemērošanas žurnālistikas nolūkos veiktai apstrādei vai akadēmiskās, mākslinieciskās vai literārās izpausmes nolūkos veiktai apstrādei. 2018. gada DAL noteikumi, jo īpaši 2. pielikuma 5. daļa, ir saderīgi ar Apvienotās Karalistes VDAR.

(69) Saskaņā ar Apvienotās Karalistes VDAR 85. pantu veicamā galvenā līdzsvara pārbaude ir saistīta ar to, vai 68. apsvērumā minētais atbrīvojums no datu aizsardzības noteikumiem ir "nepieciešams nolūkā panākt līdzsvaru starp tiesībām uz personas datu aizsardzību un vārda un informācijas brīvību" ([63]). Saskaņā ar 2018. gada DAL 2. pielikuma 26. punkta 2. un 3. apakšpunktu Apvienotā Karaliste nolūkā panākt šo līdzsvaru piemēro "pamatota pieņēmuma" pārbaudi. Lai atbrīvojums būtu pamatots, pārzinim ir pamatoti jāpieņem, ka i) publicēšana ir sabiedrības interesēs; ii) attiecīgā VDAR noteikuma piemērošana būtu nesaderīga ar žurnālistikas, akadēmiskiem, mākslinieciskiem un literāriem nolūkiem. Kā apstiprināts judikatūrā ([64]), "pamatota pieņēmuma" pārbaude ietver gan subjektīvu, gan objektīvu komponentu: nepietiek ar to, ka pārzinis apliecina, ka saskaņā ar viņa ieskatu noteikumu ievērošana rada pretrunu. Viņa pieņēmumam ir jābūt pamatotam, t. i., tam varētu piekrist saprātīga persona, kura pārzina attiecīgos faktus. Tāpēc, formulējot savu nostāju, pārzinim ir jāievēro pienācīga rūpība, lai varētu uzskatāmi parādīt nostājas pamatotību. Saskaņā ar Apvienotās Karalistes iestāžu sniegtajiem skaidrojumiem "pamatota pieņēmuma" pārbaude ir jāveic attiecībā uz katru atbrīvojumu atsevišķi ([65]). Ja nosacījumi ir izpildīti, atbrīvojumu atbilstīgi Apvienotās Karalistes tiesību aktiem uzskata par nepieciešamu un samērīgu.

(70) Saskaņā ar 2018. gada DAL 124. pantu IKB ir jāsagatavo prakses kodekss par datu aizsardzību un žurnālistiku. Norit darbs pie šā kodeksa izstrādes. Saskaņā ar 1998. gada Datu aizsardzības likumu ir publicēti norādījumi par šo jautājumu, un tajos jo īpaši uzsvērts, ka, lai izmantotu šo atbrīvojumu, nav pietiekami tikai norādīt, ka konkrēto noteikumu ievērošana apgrūtinātu ar žurnālistiku saistītas darbības, un ir jāsniedz skaidrs arguments

([62]) Sk. Apvienotās Karalistes VDAR 85. pantu un 2018. gada DAL 2. pielikuma 5. daļas 26. punkta 9. apakšpunktu.

([63]) Saskaņā ar 2018. gada DAL 2. pielikuma 5. daļas 26. punkta 2. apakšpunktu izņēmums attiecas uz personas datu apstrādi, ko veic īpašos nolūkos (žurnālistikas, akadēmiskos, mākslinieciskos un literāros nolūkos), ja apstrādi veic persona, kuras mērķis ir publicēt žurnālistikas, akadēmiska, mākslinieciska vai literāra rakstura materiālu, un ja pārzinis pamatoti pieņem, ka publicētais materiāls kalpotu sabiedrības interesēm. Nosakot, vai publikācija kalpotu sabiedrības interesēm, pārzinim ir jāņem vērā sabiedrības interešu īpašā nozīme vārda un informācijas brīvības jomā. Turklāt pārzinim ir jāņem vērā ar attiecīgo publikāciju saistītie prakses kodeksi vai pamatnostādnes (*the BBC Editorial Guidelines, Ofcom Broadcasting Code*, kā arī *Editors' Code of Practice*). Lai piemērotu atbrīvojumu, pārzinim ir pamatoti jāpieņem, ka attiecīgā noteikuma ievērošana nebūtu saderīga ar īpašo nolūku (2018. gada DAL 2. pielikuma 26. punkta 3. apakšpunkts).

([64]) Lietā *NT1 v Google* [2018], EWHC 799 (QB), pieņemtā sprieduma 102. punktā ir aplūkotas diskusijas par to, vai datu pārziņa pieņēmums, ka publikācija bija sabiedrības interesēs un ka attiecīgo noteikumu ievērošana bija nesaderīga ar īpašajiem nolūkiem, bija pamatots. Tiesa norādīja, ka 1998. gada Datu aizsardzības likuma 32. panta 1. punkta b) un c) apakšpunkts ietver subjektīvu un objektīvu elementu: datu pārzinim ir jāapliecina, ka viņš uzskata, ka publikācija kalpo sabiedrības interesēm un ka viņa uzskats ir objektīvi pamatots; viņam ir jāapliecina, ka saskaņā ar viņa subjektīvo ieskatu to noteikumu ievērošana, attiecībā uz kuriem viņš vēlas piemērot atbrīvojumu, būtu nesaderīga ar attiecīgo īpašo nolūku.

([65]) "Pamatota pieņēmuma" pārbaudes piemērošanas piemērs ir iekļauts IKB lēmumā piemērot sodu uzņēmumam *True Visions Productions*, kas tika pieņemts saskaņā ar 1998. gada Datu aizsardzības likumu. IKB piekrita, ka saskaņā ar mediju pārziņa subjektīvo ieskatu pirmā datu aizsardzības principa (godprātība un likumīgums) ievērošana nebija saderīga ar žurnālistikas nolūkiem. Tomēr IKB nepiekrita, ka šis uzskats bija objektīvi pamatots. IKB lēmums ir pieejams vietnē https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf.

par to, ka šis noteikums rada šķērsli atbildīgai žurnālistikas darba veikšanai ([66]). Arī Apvienotās Karalistes telesakaru regulators OFCOM un BBC savās redakcionālajās pamatnostādnēs ir publicējuši norādījumus par sabiedrības interešu pārbaudes piemērošanu un sabiedrības interešu un ar privātumu saistīto personas interešu līdzsvarošanu ([67]). Pamatnostādnēs jo īpaši sniegti tādas informācijas piemēri, kuru var uzskatīt par saistītu ar sabiedrības interesēm, kā arī paskaidrots, ka ir jāspēj uzskatāmi parādīt, ka sabiedrības intereses konkrētās lietas apstākļos ir svarīgākas par tiesībām uz privātumu.

(71) Līdzīgi VDAR 89. pantā paredzētajām prasībām, personas datu apstrādei arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos arī var piemērot atbrīvojumu no vairākiem Apvienotās Karalistes VDAR noteikumiem ([68]). Pētniecības un statistikas kontekstā atbrīvojumi ir iespējami attiecībā uz Apvienotās Karalistes VDAR noteikumiem saistībā ar apstrādes apstiprināšanu un piekļuvi datiem un garantijām attiecībā uz datu nosūtīšanu trešām valstīm, tiesībām labot, apstrādes ierobežošanu un iebilšanu pret apstrādi. Saistībā ar arhivēšanu sabiedrības interesēs atbrīvojumu iespējams piemērot arī attiecībā uz pienākumu ziņot par personas datu labošanu vai dzēšanu, apstrādes ierobežošanu un tiesībām uz datu pārnesamību.

(72) Saskaņā ar 2018. gada DAL 2. pielikuma 27. panta 1. punktu un 28. panta 1. punktu atbrīvojumi no uzskaitīto Apvienotās Karalistes VDAR noteikumu piemērošanas ir iespējami tad, ja šo noteikumu piemērošana "liegtu īstenot vai būtiski traucētu īstenot" attiecīgos nolūkus ([69]).

(73) Tā kā iepriekš minētajiem atbrīvojumiem ir būtiska nozīme individuālo tiesību efektīvā izmantošanā, jebkādas attiecīgas norises saistībā ar to interpretāciju un piemērošanu praksē (papildus norisēm saistībā ar efektīvas imigrācijas kontroles nodrošināšanu, kā skaidrots 6. apsvērumā), ietverot judikatūras un IKB norādījumu un izpildes panākšanas darbību jebkādu turpmāku attīstību, tiks ņemtas vērā šā lēmuma pastāvīgās uzraudzības kontekstā ([70]).

2.5.7. *Tālākas nosūtīšanas ierobežojumi*

(74) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus nosūta no Eiropas Savienības pārziņiem vai apstrādātājiem Apvienotajā Karalistē, nedrīkst samazināt šādu datu tālāka nosūtīšana saņēmējiem trešā valstī. Šāda "tālāka nosūtīšana", kas no Apvienotas Karalistes pārziņa vai apstrādātāja skatpunkta ir starptautiska nosūtīšana no Apvienotās Karalistes, būtu jāatļauj tikai tad, ja uz nākamo saņēmēju ārpus Apvienotās Karalistes attiecina noteikumus, kuri nodrošina aizsardzības līmeni, kas ir līdzīgs Apvienotās Karalistes tiesību sistēmas garantētajam. Šā iemesla dēļ Apvienotās Karalistes VDAR un 2018. gada DAL noteikumu piemērošana personas datu starptautiskai nosūtīšanai ir būtisks faktors nolūkā nodrošināt aizsardzības nepārtrauktību tādu personas datu gadījumā, ko atbilstīgi šim lēmumam nosūta no Eiropas Savienības uz Apvienoto Karalisti.

([66]) Saskaņā ar norādījumiem organizācijām jāspēj paskaidrot, kāpēc attiecīgo 1998. gada Datu aizsardzības likuma noteikumu ievērošana ir nesaderīga ar žurnālistikas nolūkiem. Konkrētāk, pārziņiem ir jālīdzsvaro negatīvā ietekme, ko noteikumu ievērošana radītu uz žurnālistiku, ar šo noteikumu neievērošanas radīto kaitējumu datu subjekta tiesībām. Ja žurnālists var saprātīgi sasniegt savus redakcionālos mērķus, ievērojot DAL standarta noteikumus, viņam tas ir jādara. Organizācijām ir jāspēj pamatot ierobežojumu izmantošanu attiecībā uz katru noteikumu, ko tās nav ievērojušas. "Data protection and journalism: a guide for the media", pieejami vietnē https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf.

([67]) Sabiedrības interešu piemēri cita starpā ir noziegumu atklāšana vai konstatēšana, sabiedrības veselības vai drošības aizsardzība, personu vai organizāciju sniegtu maldinošu apgalvojumu atklāšana vai tādas nekompetences atklāšana, kas skar sabiedrību. Sk. *OFCOM* norādījumus, pieejami vietnē https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf, kā arī *BBC* redakcionālās pamatnostādnes, pieejamas vietnē https://www.bbc.com/editorialguidelines/guidelines/privacy.

([68]) Sk. Apvienotās Karalistes VDAR 89. pantu un 2018. gada DAL 2. pielikuma 6. daļas 27. punkta 2. apakšpunktu un 28. punkta 2. apakšpunktu.

([69]) Uz to attiecas prasība, ka personas dati ir jāapstrādā saskaņā ar Apvienotās Karalistes VDAR 89. panta 1. punktu, ko papildina 2018. gada DAL 19. pants.

([70]) Sk. 281.–287. apsvērumu.

(75) Kārtība attiecībā uz personas datu starptautisko nosūtīšanu no Apvienotās Karalistes ir izklāstīta Apvienotās Karalistes VDAR 44.–49. pantā, un to papildina 2018. gada DAL. Šī kārtība būtībā ir identiska Regulas (ES) 2016/679 V nodaļā izklāstītajiem noteikumiem ([71]). Personas datus uz trešo valsti vai starptautisku organizāciju var nosūtīt, tikai pamatojoties uz noteikumiem par aizsardzības līmeņa pietiekamību (Apvienotās Karalistes ekvivalents Regulā (ES) 2016/679 paredzētajam lēmumam par aizsardzības līmeņa pietiekamību), vai, ja šādu noteikumu par aizsardzības līmeņa pietiekamību nav, tikai tad, ja pārzinis vai apstrādātājs ir sniedzis atbilstošas garantijas saskaņā ar Apvienotās Karalistes VDAR 46. pantu. Ja noteikumu par aizsardzības līmeņa pietiekamību vai atbilstošu garantiju nav, datus var nosūtīt, tikai pamatojoties uz Apvienotās Karalistes VDAR 49. pantā paredzētajām atkāpēm.

(76) Ministra izstrādātajos noteikumos par aizsardzības līmeņa pietiekamību var noteikt, ka trešā valsts (vai tās teritorija vai sektors), starptautiska organizācija vai šādas valsts, teritorijas, sektora vai organizācijas apraksts ([72]) nodrošina pietiekamu personas datu aizsardzības līmeni. Izvērtējot aizsardzības līmeņa pietiekamību, ministram ir jāņem vērā tieši tie paši elementi, kas ir jāizvērtē Komisijai saskaņā ar Regulas (ES) 2016/679 45. panta 2. punkta a)–c) apakšpunktu, ko skaidro kopsakarā ar Regulas (ES) 2016/679 104. apsvērumu un saglabāto ES judikatūru. Tas nozīmē, ka, novērtējot, vai trešā valsts nodrošina pietiekamu aizsardzības līmeni, attiecīgais standarts paredzēs, ka jānovērtē, vai attiecīgā trešā valsts garantē tādu aizsardzības līmeni, kurš "pēc būtības ir līdzvērtīgs" Apvienotajā Karalistē nodrošinātajam.

(77) Saistībā ar procedūru uz noteikumiem par aizsardzības līmeņa pietiekamību attiecas 2018. gada DAL 182. pantā paredzētās "vispārējās" prasības procedūrai. Saskaņā ar šo procedūru ministram, ierosinot pieņemt Apvienotās Karalistes noteikumus par aizsardzības līmeņa pietiekamību, ir jāapspriežas ar informācijas komisāru ([73]). Pēc tam, kad ministrs ir pieņēmis šos noteikumus, tos iesniedz parlamentam un tiem piemēro "noraidošas rezolūcijas" procedūru, saskaņā ar kuru abas parlamenta palātas var pārbaudīt noteikumus un 40 dienu laikā pieņemt priekšlikumu par noteikumu atcelšanu ([74]).

(78) Saskaņā ar 2018. gada DAL 17.B panta 1. punktu noteikumi par aizsardzības līmeņa pietiekamību jāpārskata ne retāk kā reizi četros gados un ministram pastāvīgi jāuzrauga norises trešās valstīs un starptautiskajās organizācijās, kas varētu ietekmēt lēmumus pieņemt noteikumus par aizsardzības līmeņa pietiekamību vai šādu noteikumu grozīšanu vai atcelšanu. Ja ministrs uzzina, ka norādītā valsts vai organizācija vairs nenodrošina pietiekamu personas datu aizsardzības līmeni, viņam, ciktāl nepieciešams, jāgroza vai jāatceļ noteikumi un jāuzsāk apspriešanās ar attiecīgo trešo valsti vai starptautisko organizāciju, lai novērstu aizsardzības līmeņa nepietiekamību. Šie procesuālie aspekti arī atspoguļo attiecīgās prasības, kas ir paredzētas Regulā (ES) 2016/679.

([71]) Izņemot Regulas (ES) 2016/679 48. pantu, ko Apvienotā Karaliste ir izvēlējusies neiekļaut Apvienotās Karalistes VDAR. Šajā saistībā, pirmkārt, būtu jāatceras, ka standarts, kuru uzskata par tādu, kas nodrošina pietiekamu aizsardzības līmeni, ir "līdzvērtības pēc būtības" standarts, nevis identitāte, kā precizējusi EST (*Schrems I*, 73.–74. punkts) un atzinusi EDAK (Pietiekamības atsauces, 3. lpp.). Tāpēc, kā Pietiekamības atsaucēs skaidro EDAK, mērķis nav Eiropas tiesību aktu precīzs atspoguļojums, bet gan šo tiesību aktu būtisko prasību un pamatprasību noteikšana. Šajā ziņā ir būtiski norādīt, ka, lai gan Apvienotās Karalistes tiesiskā kārtība oficiāli nesatur 48. pantam identisku noteikumu, to pašu ietekmi garantē citas tiesību normas un principi, t. i., ka, reaģējot uz trešās valsts tiesas vai administratīvas iestādes pieprasījumu pēc personas datiem, šos personas datus var nosūtīt uz minēto trešo valsti tikai tad, ja ir noslēgts starptautisks nolīgums, balstoties uz kuru attiecīgās trešās valsts tiesas spriedums vai administratīvais lēmums tiek atzīts vai izpildīts Apvienotajā Karalistē, vai ja nosūtīšanas pamatā ir kāds no Apvienotās Karalistes VDAR V nodaļā minētajiem nosūtīšanas mehānismiem. Konkrētāk, lai izpildītu ārvalstu tiesas pieņemtu spriedumu, tiesām Apvienotajā Karalistē ir jāspēj norādīt anglosakšu tiesības vai likumu, ar ko ir atļauta šāda sprieduma izpilde. Tomēr ne anglosakšu tiesības (sk. *Adams and Others / Cape Industries Plc.*, [1990] 2 W.L.R. 657), ne likumi neparedz tādu ārvalstu tiesas pieņemtu spriedumu izpildi, kuros pieprasīta datu nosūtīšana bez spēkā esoša starptautiska nolīguma. Rezultātā datu pieprasījumi saskaņā ar Apvienotās Karalistes tiesību aktiem nav izpildāmi, ja nav šāda starptautiska nolīguma. Turklāt jebkāda personas datu nosūtīšana uz trešām valstīm – arī pēc pieprasījuma no ārvalstu tiesas vai administratīvas iestādes – ir pakļauta Apvienotās Karalistes VDAR V nodaļā noteiktajiem ierobežojumiem, kas ir identiski attiecīgajiem Regulas (ES) 2016/679 noteikumiem, tāpēc uz nosūtīšanu jāattiecina kāds no nosūtīšanas pamatojumiem, kas pieejami V nodaļā atbilstīgi konkrētajiem nosacījumiem, kuri saskaņā ar šo nodaļu uz to attiecas.

([72]) Apvienotās Karalistes iestādes ir paskaidrojušas, ka valsts vai starptautiskas organizācijas apraksts attiecas uz situāciju, kad ir nepieciešams konkrēti un daļēji noteikt pietiekamību saistībā ar mērķtiecīgiem ierobežojumiem (piemēram, noteikumi par aizsardzības līmeņa pietiekamību tikai attiecībā uz noteiktiem datu nosūtīšanas veidiem).

([73]) Sk. Digitalizācijas, kultūras, mediju un sporta ministrijas valsts sekretāra un Informācijas komisāra biroja saprašanās memorandu *Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments*, pieejams vietnē https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([74]) Ja tiks nobalsots par šādu priekšlikumu, noteikumiem vairs nebūs turpmāka juridiska spēka.

(79) Ja nav spēkā noteikumi par aizsardzības līmeņa pietiekamību, datu starptautisku nosūtīšanu var veikt tad, ja pārzinis vai apstrādātājs ir nodrošinājis **atbilstošas garantijas** saskaņā ar Apvienotās Karalistes VDAR 46. pantu. Šīs garantijas ir līdzīgas Regulas (ES) 2016/679 46. pantā paredzētajām garantijām. Tās ietver starp publiskajām iestādēm vai struktūrām juridiski saistošus un tiesiski īstenojamus instrumentus, saistošus uzņēmuma noteikumus ([75]), standarta datu aizsardzības klauzulas, apstiprinātus rīcības kodeksus, apstiprinātus sertifikācijas mehānismus, kā arī – saskaņā ar informācijas komisāra atļauju – līguma klauzulas starp pārziņiem (vai apstrādātājiem) vai administratīvās vienošanās starp publiskām iestādēm. Tomēr noteikumi no procesuālā viedokļa ir grozīti, lai darbotos Apvienotās Karalistes sistēmā, proti, standarta datu aizsardzības klauzulas var pieņemt ministrs (17.C pants) vai informācijas komisārs (119.A pants) atbilstīgi 2018. gada DAL.

(80) Ja lēmuma par aizsardzības līmeņa pietiekamību vai atbilstošu garantiju nav, datus var nosūtīt, tikai pamatojoties uz Apvienotās Karalistes VDAR 49. pantā paredzētajām atkāpēm ([76]). Salīdzinājumā ar attiecīgajiem Regulas (ES) 2016/679 noteikumiem Apvienotās Karalistes VDAR šīs atkāpes nav būtiski grozītas. Saskaņā ar Apvienotās Karalistes VDAR, tāpat kā Regulas (ES) 2016/679 gadījumā, atsevišķas atkāpes var piemērot tikai tad, ja nosūtīšana ir gadījuma rakstura ([77]). Turklāt IKB norādījumos par datu starptautisku nosūtīšanu precizēts: "Jums būtu jāizmanto šīs atkāpes kā faktiski "izņēmumi" no vispārējā noteikuma, kas paredz, ka jums nevajadzētu nosūtīt ierobežotas aprites datus, izņemot gadījumus, ja uz tiem attiecas lēmums par aizsardzības līmeņa pietiekamību vai ir spēkā atbilstošas garantijas" ([78]). Attiecībā uz datu nosūtīšanu, kas ir nepieciešama, ja ir svarīgi iemesli sabiedrības interesēs (49. panta 1. punkta d) apakšpunkts), ministrs var paredzēt noteikumus, kuros precizē apstākļus, kādos personas datu nosūtīšana uz trešo valsti vai starptautisko organizāciju nav nepieciešama svarīgu iemeslu dēļ sabiedrības interesēs. Ministrs, pieņemot noteikumus, arī var ierobežot noteiktas kategorijas personas datu nosūtīšanu uz trešo valsti vai starptautisko organizāciju, ja, pamatojoties uz noteikumiem par aizsardzības līmeņa pietiekamību, datus nedrīkst nosūtīt un ja ministrs uzskata, ka ierobežojums ir nepieciešams svarīgu iemeslu dēļ sabiedrības interesēs. Līdz šim šādi noteikumi nav pieņemti.

(81) Šis regulējums par datu starptautisku nosūtīšanu kļuva piemērojams pārejas perioda beigās ([79]). Tomēr 2018. gada DAL 21. pielikuma 4. punktā (ieviests ar DAPES noteikumiem) ir paredzēts, ka pēc pārejas perioda beigām konkrētu personas datu nosūtīšanu uzskata par tādu, kas ir pamatota ar noteikumiem par aizsardzības līmeņa pietiekamību. Šāda nosūtīšana ietver datu nosūtīšanu uz EEZ valsti, Gibraltāra teritoriju, Savienības iestādi, struktūru, biroju vai aģentūru, kas ir izveidota ar ES līgumu vai uz tā pamata, un uz trešām valstīm, par kurām pārejas perioda beigās ir pieņemts ES lēmums par aizsardzības līmeņa pietiekamību. Tādēļ nosūtīšana uz šīm valstīm var turpināties tā, kā tā notika pirms Apvienotās Karalistes izstāšanās no ES. Pārejas

([75]) Apvienotās Karalistes VDAR ir saglabāti Regulas (ES) 2016/679 47. panta noteikumi, grozot tos tikai tiktāl, ciktāl nepieciešams, lai pielāgotu noteikumus valsts kontekstam, piemēram, atsauces uz kompetento uzraudzības iestādi aizstājot ar atsaucēm uz informācijas komisāru, no 1. punkta dzēšot atsauci uz konsekvences mehānismu, kā arī dzēšot visu 3. punktu.

([76]) Saskaņā ar Apvienotās Karalistes VDAR 49. pantu datus drīkst nosūtīt, ja ir izpildīts kāds no turpmāk izklāstītajiem nosacījumiem: a) datu subjekts ir skaidri piekritis ierosinātajai nosūtīšanai pēc tam, kad ir ticis informēts par iespējamiem riskiem, ko šāda nosūtīšana var radīt datu subjektam lēmuma par aizsardzības līmeņa pietiekamību un atbilstošu garantiju trūkuma dēļ; b) nosūtīšana ir vajadzīga, lai izpildītu līgumu starp datu subjektu un pārzini vai īstenotu pasākumus pirms līguma noslēgšanas, ko veic pēc datu subjekta pieprasījuma; c) nosūtīšana ir vajadzīga līguma noslēgšanai starp pārzini un citu fizisku vai juridisku personu datu subjekta interesēs vai šāda līguma izpildei; d) nosūtīšana ir nepieciešama, ja ir svarīgi iemesli sabiedrības interesēs; e) nosūtīšana ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības; f) nosūtīšana ir vajadzīga, lai aizsargātu datu subjekta vai citu personu vitālas (īpaši svarīgas) intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu; g) nosūtīšanu izdara no reģistra, kurš saskaņā ar valsts tiesību aktiem ir paredzēts, lai sniegtu informāciju sabiedrībai, un kuru var izmantot vai nu plaša sabiedrība, vai jebkura persona, kas var uzskatāmi parādīt, ka tai ir leģitīmas intereses, taču vienīgi tiktāl, ciktāl konkrētajā gadījumā tiek pildīti valsts tiesību aktos paredzētie izmantošanas nosacījumi. Ja nav piemērojams neviens no iepriekš minētajiem nosacījumiem, datus var nosūtīt tikai tad, ja nosūtīšana neatkārtojas, attiecas vienīgi uz ierobežotu skaitu datu subjektu, ir vajadzīga pārziņa pārliecinošām leģitīmām interesēm, attiecībā uz kurām datu subjekta intereses vai tiesības un brīvības nav svarīgākas, un pārzinis ir novērtējis visus apstākļus saistībā ar datu nosūtīšanu un, pamatojoties uz minēto novērtējumu, ir sniedzis atbilstošas garantijas attiecībā uz personas datu aizsardzību.

([77]) Apvienotās Karalistes VDAR 111. apsvērumā ir noteikts, ka datus saistībā ar līgumu vai likumīgu prasību var nosūtīt tikai tad, ja nosūtīšana ir gadījuma rakstura.

([78]) IKB norādījumi par datu starptautisku nosūtīšanu, pieejami vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7.

([79]) Laikposmā, kas nepārsniedz sešus mēnešus un beidzas ne vēlāk kā 2021. gada 30. jūnijā, šī jaunā regulējuma piemērojamība ir jāinterpretē, ņemot vērā 782. pantu Tirdzniecības un sadarbības nolīgumā starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses (OV L 444/14, 31.12.2020.) ("ES un Apvienotās Karalistes TSN"), pieejams vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:22020A1231(01)&from=LV.

perioda beigās ministram četru gadu laikā (proti, līdz 2024. gada decembra beigām) ir jāpārskata minētie konstatējumi par aizsardzības līmeņa pietiekamību. Kā paskaidrojušas Apvienotās Karalistes iestādes, lai gan ministram šāda pārskatīšana ir jāveic līdz 2024. gada decembra beigām, pārejas noteikumi neietver noteikumu par spēka zaudēšanu, tādēļ attiecīgie pārejas noteikumi automātiski nezaudēs spēku, ja pārskatīšana līdz 2024. gada decembra beigām netiks pabeigta.

(82) Visbeidzot, attiecībā uz Apvienotās Karalistes starptautiskās nosūtīšanas kārtības turpmāko attīstību – līdz ar jaunu noteikumu par aizsardzības līmeņa pietiekamību pieņemšanu, starptautisku nolīgumu noslēgšanu vai citu nosūtīšanas mehānismu attīstību – Komisija cieši uzraudzīs situāciju, vērtēs, vai dažādos nosūtīšanas mehānismus izmanto tā, ka tie nodrošina aizsardzības nepārtrauktību, un, ja nepieciešams, īstenos attiecīgus pasākumus, kuru mērķis būs novērst iespējamo negatīvo ietekmi uz šādu nepārtrauktību (sk. 278.–287. apsvērumu). Tā kā ES un Apvienotās Karalistes noteikumi par starptautisko nosūtīšanu ir līdzīgi, paredzams, ka problemātisku novirzīšanos varētu arī novērst, sadarbojoties, apmainoties ar informāciju un pieredzi, tai skaitā starp IKB un EDAK.

2.5.8. *Pārskatatbildība*

(83) Saskaņā ar pārskatatbildības principu vienībām, kas apstrādā datus, ir jāievieš atbilstoši tehniskie un organizatoriskie pasākumi, lai tās efektīvi izpildītu savus datu aizsardzības pienākumus, un jāspēj pierādīt šādu izpildi, jo īpaši kompetentajai uzraudzības iestādei.

(84) Regulā (ES) 2016/679 noteiktais pārskatatbildības princips ir saglabāts Apvienotās Karalistes VDAR 5. panta 2. punktā bez būtiskām izmaiņām, un tas pats attiecas uz 24. pantu par pārziņa atbildību, 25. pantu par datu integrētu aizsardzību un datu aizsardzību pēc noklusējuma, kā arī 30. pantu par apstrādes darbību reģistrēšanu. Ir saglabāts arī 35. un 36. pants attiecībā uz novērtējumu par ietekmi uz datu aizsardzību un iepriekšēju apspriešanos ar uzraudzības iestādi. Apvienotās Karalistes VDAR bez būtiskām izmaiņām ir saglabāts Regulas (ES) 2016/679 37.–39. pants par datu aizsardzības speciālista iecelšanu un uzdevumiem. Apvienotās Karalistes VDAR ir saglabāti arī Regulas (ES) 2016/679 40. un 42. panta noteikumi par rīcības kodeksiem un sertifikāciju ([80]).

2.6. **Pārraudzība un izpilde**

2.6.1. *Neatkarīga pārraudzība*

(85) Lai nodrošinātu, ka arī praksē tiek garantēts pietiekams datu aizsardzības līmenis, vajadzētu būt izveidotai neatkarīgai uzraudzības iestādei, kurai uzticētas pilnvaras uzraudzīt un nodrošināt datu aizsardzības noteikumu izpildi. Šai iestādei tās uzdevumi būtu jāveic un pilnvaras jāīsteno pilnīgi neatkarīgi un objektīvi.

(86) Apvienotajā Karalistē pārraudzību un izpildes nodrošināšanu attiecībā uz atbilstību Apvienotās Karalistes VDAR un 2018. gada DAL veic informācijas komisārs. Informācijas komisārs ir "individuāls komersants": atsevišķs tiesību subjekts, ko veido viena persona. Informācijas komisāra darbā to atbalsta birojs. 2020. gada 31. martā informācijas komisāra birojā bija 768 pastāvīgie darbinieki ([81]). Informācijas komisāru atbalsta Digitalizācijas, kultūras, mediju un sporta ministrija ([82]).

(87) Komisāra neatkarība ir skaidri noteikta Apvienotās Karalistes VDAR 52. pantā, kura saturs bez būtiskām izmaiņām atspoguļo VDAR 52. panta 1.–3. punktā paredzēto. Komisāram, veicot uzdevumus un īstenojot savas pilnvaras saskaņā ar Apvienotās Karalistes VDAR, ir jārīkojas pilnīgi neatkarīgi, attiecībā uz šiem uzdevumiem un pilnvarām

([80]) Vajadzības gadījumā šīs atsauces ir aizstātas ar atsaucēm uz Apvienotās Karalistes iestādēm. Piemēram, saskaņā ar 2018. gada DAL 17. pantu informācijas komisārs vai Apvienotās Karalistes valsts akreditācijas struktūra var akreditēt personu, kas atbilst Apvienotās Karalistes VDAR 43. pantā paredzētajām prasībām, lai tā uzraudzītu atbilstību sertifikācijai.

([81]) Informācijas komisāra gada pārskats un finanšu pārskati par 2019.–2020. gadu, pieejami vietnē https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([82]) Attiecības starp abām pusēm regulē pārvaldības nolīgums. Konkrēti, *DCMS* kā atbalstošās ministrijas galvenie pienākumi ir šādi: nodrošināt, lai informācijas komisāram tiktu piešķirts atbilstošs finansējums un resursi; pārstāvēt informācijas komisāra intereses parlamentā un citās valdības ministrijās; nodrošināt, ka ir ieviests stabils valsts datu aizsardzības regulējums; sniegt informācijas komisāra birojam norādījumus un atbalstu korporatīvajos jautājumos, piemēram, par nekustamo īpašumu, nomu un iepirkumiem (2018.–2021. gada pārvaldības nolīgums, pieejams vietnē https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

ir jābūt brīvam no tiešas vai netiešas ārējas ietekmes, un viņš nedrīkst lūgt un ne no viena pieņemt nekādus norādījumus. Komisāram ir arī jāatturas no jebkādas darbības, kas nav savienojama ar viņa pienākumiem, un, esot amatā, viņš nedrīkst uzņemties nekādu nesavienojamu algotu vai nealgotu darbu.

(88) Nosacījumi informācijas komisāra iecelšanai un atbrīvošanai no amata ir izklāstīti 2018. gada DAL 12. pielikumā. Informācijas komisāru ieceļ Viņas Majestāte, pēc valdības ieteikuma, pamatojoties uz godīgu un atklātu konkursu. Kandidātam ir jāpiemīt atbilstošai kvalifikācijai, prasmēm un kompetencei. Saskaņā ar Pārvaldības kodeksu par valsts amatpersonu iecelšanu amatā ([83]) padomdevēja novērtēšanas komisija izveido to kandidātu sarakstu, kurus var iecelt amatā. Pirms digitalizācijas, kultūras, mediju un sporta ministrs pieņem galīgo lēmumu, attiecīgajai parlamenta komitejai ir jāveic pirmsiecelšanas pārbaude. Komitejas nostāja tiek publiskota ([84]).

(89) Informācijas komisāra amata pilnvaru termiņš ir līdz septiņiem gadiem. Personu informācijas komisāra amatā var iecelt tikai vienu reizi. Informācijas komisāru no amata var atbrīvot Viņas Majestāte pēc tam, kad abas parlamenta palātas ir izdarījušas uzrunu ([85]). Nevienai no parlamenta palātām nevar iesniegt pieprasījumu par informācijas komisāra atbrīvošanu no amata, ja vien ministrs nav iesniedzis ziņojumu, kurā minēts, ka viņš ir pārliecināts, ka informācijas komisārs ir vainojams nopietnā pārkāpumā un/vai komisārs vairs neatbilst komisāra funkciju veikšanai nepieciešamajiem nosacījumiem ([86]).

(90) Informācijas komisāram ir trīs finansējuma avoti: i) pārziņu maksājumi par datu aizsardzību, kuri noteikti ar ministra izdotiem noteikumiem ([87]) (2018. gada Datu aizsardzības (maksas un informācija) noteikumi) un veido 85–90 % no biroja gada budžeta ([88]); ii) dotācijas, ko informācijas komisāram izmaksā valdība (dotācijas galvenokārt izmanto, lai finansētu informācijas komisāra darbības izmaksas, kas nav saistītas ar datu aizsardzību ([89])); un iii) maksa par pakalpojumiem ([90]). Pašlaik šādas maksas netiek iekasētas.

(91) Informācijas komisāra vispārīgās funkcijas saistībā ar to personas datu apstrādi, uz kuriem attiecas Apvienotās Karalistes VDAR, ir noteiktas Apvienotās Karalistes VDAR 57. pantā, kas atspoguļo attiecīgās prasības Regulā (ES) 2016/679. Informācijas komisāra funkcijās ietilpst uzraudzība un Apvienotās Karalistes VDAR piemērošana, sabiedrības informētības veicināšana, datu subjektu iesniegto sūdzību apstrāde, izmeklēšana utt. 2018. gada DAL 115. pantā ir noteiktas komisāra vispārīgās funkcijas, tostarp pienākums sniegt parlamentam, valdībai un citām iestādēm un struktūrām ieteikumus par likumdošanas un administratīviem pasākumiem saistībā ar personas tiesību un brīvību aizsardzību attiecībā uz personas datu apstrādi, kā arī pilnvaras pēc komisāra paša

([83]) Pārvaldības kodekss par valsts amatpersonu iecelšanu amatā, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) Pārstāvju palātas Kultūras, mediju un sporta komitejas 2015.–2016. gada sesijas otrais ziņojums, pieejams vietnē https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([85]) "Uzruna" ir parlamentam iesniegts priekšlikums, kura mērķis ir iepazīstināt monarhu ar parlamenta viedokli par kādu konkrētu jautājumu.

([86]) 2018. gada DAL 12. pielikuma 3.3. punkts.

([87]) 2018. gada DAL 137. pants, sk. 17. apsvērumu.

([88]) 2018. gada DAL 137. un 138. pantā ir ietvertas vairākas garantijas, lai nodrošinātu, ka maksas tiek noteiktas atbilstošā līmenī. Konkrēti, 137. panta 4. punktā ir uzskaitīti aspekti, kas ministram ir jāņem vērā, izstrādājot noteikumus par summu, ko maksā dažādas organizācijas. 2018. gada DAL 138. panta 1. punktā un 182. pantā ir ietverta arī juridiska prasība ministram pirms noteikumu pieņemšanas apspriesties ar informācijas komisāru un citiem to personu pārstāvjiem, kuras varētu ietekmēt noteikumi, lai varētu ņemt vērā to viedokļus. Turklāt saskaņā ar 2018. gada DAL 138. panta 2. punktu informācijas komisāram ir jāpārrauga Maksas noteikumu darbība, un viņš var iesniegt ministram priekšlikumus par grozījumiem, kas jāveic noteikumos. Visbeidzot, izņemot gadījumus, kad noteikumi pieņemti tikai tādēļ, lai ņemtu vērā mazumtirdzniecības cenu indeksa pieaugumu (tādā gadījumā uz tiem attiecas noraidošas rezolūcijas procedūra), uz noteikumiem attiecas apstiprinošas rezolūcijas procedūra, un tos nevar pieņemt, kamēr tie nav apstiprināti ar katras parlamenta palātas rezolūciju.

([89]) Pārvaldības nolīgumā ir precizēts, ka "ministrs var veikt maksājumus IK no parlamenta piešķirtajiem līdzekļiem saskaņā ar 2018. gada DAL 12. pielikuma 9. punktu. Pēc apspriešanās ar IK *DCMS* izmaksā IK attiecīgas summas (dotācijas) IKB administratīvo izmaksu segšanai un IK funkciju izpildei vairāku konkrētu uzdevumu, tostarp informācijas brīvības, sakarā" (2018.–2021. gada pārvaldības nolīgums, 1.12. punkts, sk. 82. zemsvītras piezīmi).

([90]) Sk. 2018. gada DAL 134. pantu.

iniciatīvas vai pēc pieprasījuma sniegt parlamentam, valdībai vai citām iestādēm un struktūrām, kā arī sabiedrībai atzinumus par jebkādiem ar personas datu aizsardzību saistītiem jautājumiem. Lai saglabātu tiesu iestāžu neatkarību, informācijas komisāram nav atļauts veikt savas funkcijas saistībā ar personas datu apstrādi, ko veic persona, kas pilda ar tiesu iestāžu darbu saistītus pienākumus, vai tiesa vai tribunāls, kad tas rīkojas atbilstīgi savai kompetencei. Tiesu iestāžu pārraudzību veic specializētas struktūras (sk. 99.–103. apsvērumu).

2.6.2. *Izpildes panākšana, ieskaitot sankcijas*

(92) Informācijas komisāra pilnvaras ir noteiktas Apvienotās Karalistes VDAR 58. pantā, kas nav būtiski grozīts salīdzinājumā ar attiecīgo pantu Regulā (ES) 2016/679. 2018. gada DAL ir paredzēti papildu noteikumi par šo pilnvaru izmantošanu. Konkrēti, komisāram ir pilnvaras: a) uzdot pārzinim un apstrādātājam (konkrētos gadījumos – jebkurai citai personai) sniegt nepieciešamo informāciju ar informatīvu paziņojumu ("informatīvais paziņojums") ([91]); b) veikt izmeklēšanu un revīzijas, sniedzot novērtējuma paziņojumu, kurā var pieprasīt pārzinim vai apstrādātājam, lai tas atļauj komisāram iekļūt konkrētās telpās, apskatīt vai pārbaudīt dokumentus vai iekārtas, iztaujāt personas, kas pārziņa vārdā apstrādā personas datus ("novērtējuma paziņojums") ([92]); c) citādi iegūt piekļuvi pārziņu un apstrādātāju dokumentiem un iekļūt to telpās saskaņā ar 2018. gada DAL 154. pantu ("iekļūšanas un pārbaudes pilnvaras"); d) īstenot korektīvās pilnvaras, tostarp izsakot brīdinājumus un rājienus, vai dot rīkojumus ar izpildes paziņojumu, ar kuru pārziņiem/apstrādātājiem pieprasa veikt konkrētas darbības vai atturēties no to veikšanas, tostarp sniegt rīkojumu pārzinim vai apstrādātājam veikt jebkuru Apvienotās Karalistes VDAR 58. panta 2. punkta c)–g) apakšpunktā un j) apakšpunktā noteikto darbību ("izpildes paziņojums") ([93]); e) uzlikt administratīvos naudas sodus soda paziņojuma veidā ("soda paziņojums") ([94]). Administratīvos naudas sodus var uzlikt arī tad, ja publiska iestāde nav izpildījusi Apvienotās Karalistes VDAR noteikumus ([95]).

(93) IKB regulatīvās rīcības politikā ir izklāstīti apstākļi, kādos birojs izdod attiecīgi informatīvu, novērtējuma, izpildes un soda paziņojumu ([96]). Izpildes paziņojumā, ko nosūta, reaģējot uz pārziņa vai apstrādātāja pārkāpumu, var noteikt tikai tādas prasības, kuras komisārs uzskata par piemērotām pārkāpuma novēršanai. Izpildes un soda paziņojumus pārzinim vai apstrādātājam var nosūtīt saistībā ar Apvienotās Karalistes VDAR II nodaļas (apstrādes principi), 12.–22. panta (datu subjekta tiesības), 25.–39. panta (pārziņu un apstrādātāju pienākumi) un 44.–49. panta (datu starptautiska nosūtīšana) pārkāpumiem. Izpildes paziņojumu var nosūtīt arī tad, ja pārzinis nav izpildījis prasību veikt maksājumu, kas paredzēta saskaņā ar 2018. gada DAL 137. pantu izstrādātajos noteikumos. Turklāt izpildes paziņojumu var nosūtīt 41. pantā minētajai uzraudzības iestādei vai sertifikācijas pakalpojumu sniedzējam, ja tas nepilda pienākumus, kas tam noteikti Apvienotās Karalistes VDAR. Soda paziņojumu var nosūtīt arī personai, kas nav izpildījusi informatīvajā paziņojumā, novērtējuma paziņojumā vai izpildes paziņojumā noteiktās prasības.

(94) Soda paziņojumā personai tiek prasīts samaksāt informācijas komisāram paziņojumā norādīto summu. Nosakot, vai personai ir jāpiemēro sods, un nosakot soda apmēru, informācijas komisāram jāņem vērā Apvienotās Karalistes VDAR 83. panta 1. un 2. punktā uzskaitītie aspekti, kas ir identiski attiecīgajiem noteikumiem Regulā (ES) 2016/679 ([97]). Saskaņā ar 83. panta 4. un 5. punktu maksimālās administratīvo naudas sodu summas, ko var piemērot par iepriekš minētajos noteikumos paredzēto pienākumu nepildīšanu, ir attiecīgi 8700 000 GBP vai 17 500 000 GBP. Ja persona ir uzņēmums, informācijas komisārs naudas sodus var piemērot, arī iekasējot

([91]) 2018. gada DAL 142. pants (atbilstīgi 2018. gada DAL 143. pantā paredzētajiem ierobežojumiem).
([92]) 2018. gada DAL 146. pants (atbilstīgi 2018. gada DAL 147. pantā paredzētajiem ierobežojumiem).
([93]) 2018. gada DAL 149.–151. pants (atbilstīgi 2018. gada DAL 152. pantā paredzētajiem ierobežojumiem).
([94]) 2018. gada DAL 155. pants un Apvienotās Karalistes VDAR 83. pants.
([95]) Tas izriet no 2018. gada DAL 155. panta 1. punkta, ko skata kopā ar 2018. gada DAL 149. panta 2. un 5. punktu, un no 2018. gada DAL 156. panta 4. punkta, kas ierobežo soda paziņojumu izdošanu tikai attiecībā uz valsts īpašumu pilnvarniekiem un karaliskās ģimenes saimniecības pārziņiem saskaņā ar 2018. gada DAL 209. panta 4. punktu.
([96]) Regulatīvās rīcības politika, pieejama vietnē https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([97]) Ieskaitot pārkāpuma raksturu un smagumu (ņemot vērā attiecīgās apstrādes raksturu, apmēru un nolūkus, kā arī ietekmēto datu subjektu skaitu un tiem nodarītā kaitējuma apmēru), to, vai pārkāpums izdarīts tīši vai neuzmanības dēļ, jebkādu pārziņa rīcību, lai mazinātu kaitējumu, kas nodarīts datu subjektiem, pārziņa vai apstrādātāja atbildības līmeni (ņemot vērā pārziņa vai apstrādātāja veiktos tehniskos un organizatoriskos pasākumus), jebkādus attiecīgus pārziņa vai apstrādātāja iepriekšējus pārkāpumus, sadarbības pakāpi ar komisāru, to, kādu kategoriju personas datus ietekmējis pārkāpums, jebkādu citu pastiprinošu vai mīkstinošu apstākli, kas piemērojams lietas apstākļiem, piemēram, no pārkāpuma tieši vai netieši gūti finansiālie labumi vai novērsti zaudējumi.

procentuālu daļu no tā gada apgrozījuma pasaulē, ja tā ir lielāka par iepriekš minētajiem naudas sodiem. Tāpat kā attiecīgajos Regulas (ES) 2016/679 noteikumos, šīs summas attiecīgi 83. panta 4. punktā un 83. panta 5. punktā ir noteiktas 2 % un 4 % apmērā. Personai, kas nav izpildījusi informatīvajā paziņojumā, novērtējuma paziņojumā vai izpildes paziņojumā noteiktās prasības, soda paziņojumā var noteikt naudas sodu, kas nepārsniedz 17 500 000 GBP, vai, ja persona ir uzņēmums, 4 % no gada apgrozījuma pasaulē.

(95) Apvienotās Karalistes VDAR kopā ar 2018. gada DAL ir stiprinājusi arī pārējās informācijas komisāra pilnvaras. Piemēram, komisārs, izmantojot novērtējuma paziņojumus, tagad var veikt obligātas revīzijas saistībā ar visiem pārziņiem un apstrādātājiem, turpretī saskaņā ar iepriekšējo tiesisko regulējumu, 1998. gada Datu aizsardzības likumu, komisāram bija pilnvaras tikai attiecībā uz centrālo valdību un veselības organizācijām, bet pārējos gadījumos bija jāsaņem attiecīgo struktūru piekrišana.

(96) Kopš Regulas (ES) 2016/679 pieņemšanas IKB gadā apstrādā aptuveni 40 000 datu subjektu sūdzību ([98]), kā arī papildus tam veic aptuveni 2000 *ex officio* izmeklēšanu ([99]). Lielākā daļa sūdzību ir saistītas ar tiesībām uz piekļuvi datiem un uz datu izpaušanu. Pēc izmeklēšanas veikšanas komisārs veic izpildes pasākumus virknē sektoru. Konkrētāk, saskaņā ar informācijas komisāra jaunāko gada pārskatu (2019.–2020. gads) ([100]) komisārs pārskata periodā nosūtīja 54 informatīvos paziņojumus, 8 novērtējuma paziņojumus, 7 izpildes paziņojumus, 4 brīdinājumus, 8 apsūdzības un 15 soda paziņojumus ([101]).

(97) Tas ietver vairākus lielus naudas sodus, kas tika piemēroti saskaņā ar Regulu (ES) 2016/679 un 2018. gada DAL. Konkrēti, informācijas komisārs 2020. gada oktobrī par datu aizsardzības pārkāpumu, kas ietekmēja vairāk nekā 400 000 klientu, britu aviokompānijai piemēroja naudas sodu 20 miljonu GBP apmērā. Par nespēju nodrošināt miljoniem klientu personas datu drošību 2020. gada oktobra beigās naudas sods 18,4 miljonu GBP apmērā tika piemērots starptautiskai viesnīcu ķēdei, un 2020. gada novembrī britu pakalpojumu sniedzējam, kas tiešsaistē pārdod pasākumu biļetes, tika piemērots naudas sods 1,25 miljonu GBP apmērā, jo šis pakalpojumu sniedzējs pārkāpa klientu maksājumu informācijas aizsardzības prasības ([102]).

(98) Papildus 92. apsvērumā aprakstītajām informācijas komisāra izpildes pilnvarām daži datu aizsardzības tiesību aktu pārkāpumi ir noziedzīgi nodarījumi, tāpēc par tiem var piemērot kriminālsodus (2018. gada DAL 196. pants). Tas attiecas, piemēram, uz apzinātu vai bezatbildīgu personas datu iegūšanu vai izpaušanu bez pārziņa piekrišanas, panākšanu, ka personas dati tiek izpausti citai personai bez pārziņa piekrišanas ([103]), informācijas, kas ir anonimizēti personas dati, atkārtotu identificēšanu, ja tai nav piekritis par personas datu anonimizēšanu atbildīgais pārzinis ([104]), komisāra pilnvaru īstenošanas apzinātu kavēšanu saistībā ar personas datu pārbaudi saskaņā ar starptautiskajām saistībām ([105]), nepatiesu ziņu sniegšanu, atbildot uz informatīvu paziņojumu, vai informācijas iznīcināšanu saistībā ar informatīviem un novērtējuma paziņojumiem ([106]).

([98]) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju informācijas komisāra 2019.–2020. gada pārskatā aplūkotajā periodā aptuveni 25 % gadījumu netika konstatēts pārkāpums, aptuveni 29 % gadījumu datu subjekts tika aicināts pirmo reizi vērsties ar sūdzību pie datu pārziņa, sagaidīt datu pārziņa atbildi vai turpināt dialogu ar datu pārzini, aptuveni 17 % gadījumu netika konstatēts pārkāpums, bet datu pārzinim tika sniegti ieteikumi, aptuveni 25 % gadījumu informācijas komisārs konstatēja pārkāpumu un sniedza datu pārzinim ieteikumus vai prasīja tam veikt noteiktas darbības, aptuveni 3 % gadījumu tika konstatēts, ka sūdzība neietilpst Regulas (ES) 2016/679 darbības jomā, un aptuveni 1 % gadījumu lietas tika pārsūtītas citai datu aizsardzības iestādei Eiropas Datu aizsardzības kolēģijas ietvaros.

([99]) IKB var sākt šīs izmeklēšanas, pamatojoties uz informāciju, kas ir saņemta no dažādiem avotiem, tostarp pamatojoties uz paziņojumiem par personas datu aizsardzības pārkāpumiem, citu Apvienotās Karalistes publisko iestāžu vai ārvalstu datu aizsardzības iestāžu iesniegumiem, kā arī personu vai pilsoniskās sabiedrības organizāciju sūdzībām.

([100]) Informācijas komisāra gada pārskats un finanšu pārskati par 2019.–2020. gadu (sk. 81. zemsvītras piezīmi).

([101]) Saskaņā ar iepriekšējo gada pārskatu, kas aptvēra 2018.–2019. gadu, informācijas komisārs atbilstīgi 1998. gada DAL pārskata periodā izsūtīja 22 soda paziņojumus par kopējo summu 3010 610 GBP, tostarp par diviem naudas sodiem 500 000 GBP apmērā (1998. gada DAL atļautā maksimālā nauda soda summa). Pēc tam, kad kļuva zināma ar *Cambridge Analytica* saistītā informācija, informācijas komisārs 2018. gadā veica izmeklēšanu par datu analītikas izmantošanu politiskiem mērķiem. Izmeklēšanas rezultātā tika sagatavots ziņojums par politiku, ieteikumu kopums, *Facebook* tika piemērots naudas sods 500 000 GBP apmērā, un Kanādas datu brokerim *Aggregate IQ* tika nosūtīts izpildes paziņojums, kurā uzņēmumam tika sniegts rīkojums dzēst tā rīcībā esošos Apvienotās Karalistes pilsoņu un rezidentu personas datus (sk. informācijas komisāra gada pārskatu un finanšu pārskatus par 2018.–2019. gadu, pieejami vietnē https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf).

([102]) Kopsavilkumu par veiktajām izpildes darbībām sk. IKB tīmekļa vietnē, pieejams vietnē https://ico.org.uk/action-weve-taken/enforcement/.

([103]) 2018. gada DAL 170. pants.

([104]) 2018. gada DAL 171. pants.

([105]) 2018. gada DAL 119. pants.

([106]) 2018. gada DAL 144. un 148. pants.

2.6.3. *Tiesu iestāžu pārraudzība*

(99) Tiesu un tiesu iestāžu veiktās personas datu apstrādes pārraudzība ir divējāda. Ja tiesu iestādes amatpersona vai tiesa neīsteno tiesu varu, pārraudzību nodrošina informācijas komisārs. Ja pārzinis īsteno tiesu varu, IKB nevar īstenot pārraudzību ([107]), un pārraudzību veic īpašas struktūras. Tas atspoguļo Regulā (ES) 2016/679 (55. panta 3. punktā) izmantoto pieeju.

(100) Konkrēti, otrajā scenārijā šādu pārraudzību pār Anglijas un Velsas tiesām un Anglijas un Velsas pirmā un augstākā līmeņa tribunāliem nodrošina Tiesu datu aizsardzības kolēģija ([108]). Turklāt lords augstais tiesnesis un tribunālu galvenais tiesnesis ir izdevuši Paziņojumu par privātumu ([109]), kurā izklāstīts, kā Anglijas un Velsas tiesas apstrādā personas datus tiesas funkciju veikšanai. Līdzīgu paziņojumu ir izdevušas Ziemeļīrijas ([110]) un Skotijas ([111]) tiesu iestādes.

(101) Turklāt Ziemeļīrijas lords augstais tiesnesis ir iecēlis Augstās tiesas tiesnesi par datu uzraudzības tiesnesi (DUT) Ziemeļīrijā ([112]). Tas ir arī izdevis norādījumus Ziemeļīrijas tiesu iestādēm par to, kā rīkoties datu nozaudēšanas vai iespējamas nozaudēšanas gadījumā un kā risināt ar to saistītos jautājumus ([113]).

(102) Skotijā lords priekšsēdētājs ir iecēlis datu uzraudzības tiesnesi, kas izmeklē visas sūdzības datu aizsardzības jomā. Tas ir noteikts saskaņā ar tiesu iestāžu sūdzību izskatīšanas noteikumiem, kas atbilst Anglijā un Velsā spēkā esošajiem noteikumiem ([114]).

(103) Visbeidzot, Augstākajā tiesā datu aizsardzības pārraudzībai ir iecelts viens no Augstākās tiesas tiesnešiem.

2.6.4. *Tiesiskās aizsardzības līdzekļi*

(104) Lai nodrošinātu pietiekamu aizsardzību un jo īpaši individuālo tiesību īstenošanu, datu subjektam vajadzētu būt pieejamai efektīvai tiesību aizsardzībai administratīvā kārtā vai tiesā, tostarp kompensācijai par kaitējumu.

([107]) 2018. gada DAL 117. pants.

([108]) Kolēģija ir atbildīga par norādījumu došanu tiesu iestādēm un mācību rīkošanu. Tā arī izskata datu subjektu sūdzības par personas datu apstrādi, ko veikušas tiesas, tribunāli un personas, kuras īsteno tiesu varu. Kolēģijas mērķis ir nodrošināt, lai pastāvētu veids, kā atrisināt jebkuru sūdzību. Ja sūdzības iesniedzējs nav apmierināts ar kolēģijas lēmumu un iesniedz papildu pierādījumus, kolēģija var pārskatīt savu lēmumu. Lai gan pati kolēģija nepiemēro finansiālas sankcijas, ja tā uzskata, ka ir noticis pietiekami nopietns 2018. gada DAL pārkāpums, tā var nodot lietu Tiesu rīcības izmeklēšanas birojam (*JCIO*), lai tas izmeklētu sūdzību. Ja sūdzība tiek apmierināta, lorda kanclera un lorda augstā tiesneša (vai vecākā tiesneša, kas ir pilnvarots rīkoties viņa vārdā) ziņā ir lemt par to, kādi pasākumi būtu jāveic pret amatā esošo personu. Sarindojot pēc smaguma pakāpes, tie var ietvert: oficiālu ieteikumu, oficiālu brīdinājumu, rājienu un galu galā atcelšanu no amata. Ja persona nav apmierināta ar to, kā *JCIO* ir izmeklējis sūdzību, tā var iesniegt sūdzību tiesnešu iecelšanas un rīcības ombudam (sk. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudam ir pilnvaras lūgt *JCIO* atkārtoti izmeklēt sūdzību, un tas var ierosināt izmaksāt kompensāciju sūdzības iesniedzējam, ja ir iemesls domāt, ka tam administratīvas kļūmes dēļ ir nodarīts kaitējums.

([109]) Lorda augstā tiesneša un tribunālu galvenā tiesneša paziņojums par privātumu ir pieejams vietnē https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([110]) Ziemeļīrijas lorda augstā tiesneša paziņojums par privātumu ir pieejams vietnē https://judiciaryni.uk/data-privacy.

([111]) Skotijas tiesu un tribunālu paziņojums par privātumu ir pieejams vietnē https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([112]) DUT sniedz norādījumus tiesu iestādēm un izmeklē pārkāpumus un/vai sūdzības attiecībā uz personas datu apstrādi, ko veic tiesas vai privātpersonas, kuras darbojas kā tiesu iestādes.

([113]) Ja sūdzību vai pārkāpumu uzskata par nopietnu, to nosūta tiesu sūdzību inspektoram turpmākai izmeklēšanai saskaņā ar Ziemeļīrijas lorda augstā tiesneša Sūdzību prakses kodeksu. Šādas sūdzības rezultāts varētu būt: tālāku darbību neveikšana, ieteikumi, apmācība vai mentorēšana, neoficiāls brīdinājums, oficiāls brīdinājums, galīgais brīdinājums, prakses ierobežošana vai nodošana likumā paredzētajam tribunālam. Ziemeļīrijas lorda augstā tiesneša izdotais Sūdzību prakses kodekss ir pieejams vietnē https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([114]) Jebkuru pamatotu sūdzību izskata datu uzraudzības tiesnesis, un tā tiek nodota lordam priekšsēdētājam, kuram ir tiesības sniegt ieteikumus, izteikt oficiālu brīdinājumu vai rājienu, ja viņš to uzskata par nepieciešamu (līdzvērtīgi noteikumi ir spēkā attiecībā uz tribunāla locekļiem un ir pieejami vietnē https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

(105) Pirmkārt, datu subjektam ir tiesības iesniegt sūdzību informācijas komisāram, ja datu subjekts uzskata, ka saistībā ar viņa personas datiem ir pārkāpta Apvienotās Karalistes VDAR ([115]). Apvienotās Karalistes VDAR bez būtiskām izmaiņām ir saglabāti Regulas (ES) 2016/679 77. pantā paredzētie noteikumi par šīm tiesībām. Tas pats attiecas uz 57. panta 1. punkta f) apakšpunktu un 2. punktu, kurā izklāstīti komisāra pienākumi saistībā ar sūdzību izskatīšanu. Kā aprakstīts iepriekš 92.–98. apsvērumā, informācijas komisārs ir pilnvarots novērtēt pārziņa un apstrādātāja atbilstību Apvienotās Karalistes VDAR un 2018. gada DAL, neatbilstības gadījumā pieprasīt tiem veikt nepieciešamos pasākumus vai atturēties no to veikšanas un uzlikt naudas sodu.

(106) Otrkārt, Apvienotās Karalistes VDAR un 2018. gada DAL ir paredzētas tiesības uz tiesisko aizsardzību pret informācijas komisāru. Saskaņā ar Apvienotās Karalistes VDAR 78. panta 1. punktu personai ir tiesības uz efektīvu tiesisko aizsardzību tiesā pret komisāra pieņemtu juridiski saistošu lēmumu, kas skar minētās personas. Veicot pārskatīšanu tiesā, tiesnesis izskata prasībā apstrīdēto lēmumu un izvērtē, vai informācijas komisārs ir rīkojies likumīgi. Turklāt saskaņā ar Apvienotās Karalistes VDAR 78. panta 2. punktu, ja komisārs nav atbilstoši izskatījis datu subjekta iesniegto sūdzību, ([116]) sūdzības iesniedzējs var izmantot tiesisko aizsardzību tiesā. Tas var vērsties pirmā līmeņa tribunālā, lai tas uzdotu komisāram veikt atbilstošus pasākumus sakarā ar sūdzību vai informēt sūdzības iesniedzēju par sūdzības virzību ([117]). Turklāt jebkura persona, kas no komisāra ir saņēmusi kādu no iepriekš minētajiem paziņojumiem (informatīvu, novērtējuma, izpildes vai soda paziņojumu), var to pārsūdzēt pirmā līmeņa tribunālā ([118]). Ja tribunāls uzskata, ka komisāra lēmums neatbilst tiesību aktiem vai ka informācijas komisāram vajadzēja citādi izmantot savu rīcības brīvību, tribunālam ir jāatļauj pārsūdzība vai jānosaka aizstājējs paziņojums vai lēmums, ko informācijas komisārs būtu varējis izdot vai pieņemt.

(107) Treškārt, personas var tieši panākt tiesisko aizsardzību pret kontrolieriem un apstrādātājiem tiesā saskaņā ar Apvienotās Karalistes VDAR 79. pantu un 2018. gada DAL 167. pantu. Ja pēc datu subjekta pieteikuma tiesa ir pārliecinājusies, ka ir pārkāptas datu subjekta tiesības, ko paredz datu aizsardzības tiesību akti, tiesa var uzdot pārzinim, kas apstrādā datus, vai apstrādātājam, kas rīkojas minētā pārziņa vārdā, veikt rīkojumā noteiktos pasākumus vai atturēties no rīkojumā noteikto pasākumu veikšanas.

(108) Turklāt saskaņā ar Apvienotās Karalistes VDAR 82. pantu un 2018. gada DAL 168. pantu jebkurai personai, kurai Apvienotās Karalistes VDAR pārkāpuma rezultātā ir nodarīts materiāls vai nemateriāls kaitējums, ir tiesības no pārziņa vai apstrādātāja saņemt kompensāciju par tai nodarīto kaitējumu. Apvienotās Karalistes VDAR 82. panta 1.–5. punktā izklāstītie noteikumi par kompensāciju un atbildību ir identiski ar attiecīgajiem noteikumiem Regulā (ES) 2016/679. Saskaņā ar 2018. gada DAL 168. pantu nemateriāls kaitējums ietver arī spriedzi. Saskaņā ar Apvienotās Karalistes VDAR 80. pantu datu subjektam ir arī tiesības pilnvarot pārstāvības struktūru vai organizāciju, lai tā datu subjekta vārdā iesniegtu sūdzību komisāram (saskaņā ar Apvienotās Karalistes VDAR 77. pantu) un datu subjekta vārdā izmantotu Apvienotās Karalistes VDAR 78. pantā minētās tiesības (tiesības uz efektīvu tiesisko aizsardzību tiesā pret komisāru), 79. pantā minētās tiesības (tiesības uz efektīvu tiesisko aizsardzību tiesā pret pārzini vai apstrādātāju) un 82. pantā minētās tiesības (tiesības uz kompensāciju un atbildību).

(109) Ceturtkārt, kā arī papildus iepriekš aprakstītajām tiesiskās aizsardzības iespējām jebkura persona, kas uzskata, ka publiskās iestādes ir pārkāpušas tās tiesības, tostarp tiesības uz privātumu un datu aizsardzību, var saņemt kompensāciju Apvienotās Karalistes tiesās saskaņā ar 1998. gada Cilvēktiesību likumu ([119]). Persona, kas apgalvo, ka publiska iestāde ir rīkojusies (vai plāno rīkoties) veidā, kas nav savienojams ar konvencijā paredzētajām tiesībām un līdz ar to ir prettiesisks saskaņā ar 1998. gada Cilvēktiesību likuma 6. panta 1. punktu, var celt prasību pret iestādi attiecīgajā tiesā vai tribunālā vai paļauties uz attiecīgajām tiesībām jebkurā tiesvedībā, ja attiecīgā persona ir (vai būtu) cietusi no nelikumīgas darbības.

(110) Ja tiesa konstatē, ka kāda publiskas iestādes darbība ir nelikumīga, tā var apmierināt šādu prasību vai atzīt tiesiskās aizsardzības līdzekli, vai savu pilnvaru ietvaros izdot rīkojumu, ko tā uzskata par taisnīgu un piemērotu ([120]). Tiesa var arī pasludināt primāra tiesību akta normu par nesaderīgu ar konvencijā garantētajām tiesībām.

([115]) Apvienotās Karalistes VDAR 77. pants.

([116]) 2018. gada DAL 166. pants jo īpaši attiecas uz šādām situācijām: a) komisārs neveic atbilstošus pasākumus, lai atbildētu uz sūdzību, b) komisārs nesniedz sūdzības iesniedzējam informāciju par sūdzības virzību vai par sūdzības iznākumu, līdz pagājis trīs mēnešu periods, kas sākas no brīža, kad komisārs saņēmis sūdzību, vai c) ja komisārs sūdzības izskatīšanu šajā periodā nav pabeidzis – nesniedz sūdzības iesniedzējam šādu informāciju turpmākajā trīs mēnešu periodā.

([117]) Apvienotās Karalistes VDAR 78. panta 2. punkts un 2018. gada DAL 166. pants.

([118]) Apvienotās Karalistes VDAR 78. panta 1. punkts un 2018. gada DAL 162. pants.

([119]) 1998. gada Cilvēktiesību likuma 7. panta 1. punkts. Saskaņā ar 7. panta 7. punktu persona ir cietusi no nelikumīgas darbības tikai tad, ja tā būtu upuris atbilstīgi Eiropas Cilvēktiesību konvencijas 34. pantam gadījumā, ja Eiropas Cilvēktiesību tiesā būtu iesniegta prasība saistībā ar šo darbību.

([120]) 1998. gada Cilvēktiesību likuma 8. panta 1. punkts.

(111) Visbeidzot, pēc valsts tiesiskās aizsardzības līdzekļu izsmelšanas persona var saņemt kompensāciju, vēršoties Eiropas Cilvēktiesību tiesā par Eiropas Cilvēktiesību konvencijā garantēto tiesību pārkāpumiem.

3. APVIENOTĀS KARALISTES PUBLISKO IESTĀŽU PIEKĻUVE PERSONAS DATIEM, KO NOSŪTA NO EIROPAS SAVIENĪBAS, UN ŠĀDU DATU IZMANTOŠANA

(112) Komisija arī izvērtēja Apvienotās Karalistes tiesisko regulējumu tādu personas datu vākšanai un turpmākai izmantošanai, ko Apvienotās Karalistes publiskās iestādes nosūtīja Apvienotās Karalistes uzņēmējiem sabiedrības interesēs, jo īpaši krimināltiesību aktu piemērošanas un valsts drošības nolūkos (turpmāk tekstā – "valdības piekļuve"). Novērtējot, vai nosacījumi, ar kādiem valdības piekļuve datiem, kas saskaņā ar šo lēmumu nosūtīti uz Apvienoto Karalisti, atbilstu "līdzvērtības pēc būtības" pārbaudei saskaņā ar Regulas (ES) 2016/679 45. panta 1. punktu, kā to interpretējusi Eiropas Savienības Tiesa, ņemot vērā Pamattiesību hartu, Komisija jo īpaši ņēma vērā turpmāk minētos kritērijus.

(113) Pirmkārt, jebkuriem ierobežojumiem, kas skar tiesības uz personas datu aizsardzību, ir jābūt paredzētiem tiesību aktos, un juridiskajam pamatam, kas pieļauj šādu tiesību ierobežojumu, pašam jānosaka attiecīgo tiesību izmantošanas ierobežojuma tvērums ([121]).

(114) Otrkārt, lai nodrošinātu atbilstību samērīguma prasībai, saskaņā ar kuru atkāpes no personas datu aizsardzības un to ierobežojumi piemērojami tikai tiktāl, ciktāl tas ir absolūti nepieciešams (noteikti vajadzīgs) demokrātiskā sabiedrībā, lai sasniegtu konkrētus vispārējas nozīmes mērķus, kas ir līdzvērtīgi Savienībā atzītajiem, attiecīgās trešās valsts tiesību aktos, kas pieļauj ierobežojumu, jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgo pasākumu darbības jomu un piemērošanu, un jānosaka minimāli aizsardzības pasākumi, lai personām, kuru dati ir nosūtīti, būtu pietiekamas garantijas efektīvai viņu personas datu aizsardzībai pret ļaunprātīgas izmantošanas risku ([122]). Tiesību aktos jo īpaši jānorāda, kādos apstākļos un ar kādiem nosacījumiem var īstenot pasākumu ([123]), kas nodrošina šādu datu apstrādi, kā arī piemērot šādu prasību izpildei neatkarīgu pārraudzību ([124]).

(115) Treškārt, šiem tiesību aktiem jābūt juridiski saistošiem saskaņā ar valsts tiesību aktiem, un šīm juridiskajām prasībām jābūt saistošām iestādēm, kā arī to izpildei jābūt panākamai tiesās pret attiecīgās trešās valsts iestādēm ([125]). Datu subjektiem jo īpaši jābūt iespējai celt prasību neatkarīgā un objektīvā tiesā, lai gūtu piekļuvi saviem personas datiem vai panāktu šādu datu labošanu vai dzēšanu ([126]).

3.1. Vispārējais tiesiskais regulējums

(116) Publiskajām iestādēm piešķirto pilnvaru ietvaros, valdības piekļuve Apvienotajā Karalistē jāīsteno, pilnībā ievērojot tiesību aktos noteikto. Apvienotā Karaliste ir ratificējusi Eiropas Cilvēktiesību konvenciju (sk. 9. apsvērumu), un visām Apvienotās Karalistes publiskajām iestādēm ir jārīkojas saskaņā ar šo konvenciju ([127]). Konvencijas 8. pantā noteikts, ka jebkuram privātās dzīves neaizskaramības ierobežojumam ir jāatbilst tiesību aktiem, jāatbilst vienam no 8. panta 2. punktā noteiktajiem mērķiem un jābūt samērīgam, ņemot vērā šo mērķi. Konvencijas 8. pantā arī noteikts, ka ierobežojumam ir jābūt paredzamam, t. i., tam jābūt skaidram, pieejamam likumīgajam pamatam, un tiesību aktos jābūt paredzētām atbilstošām garantijām, lai novērstu ļaunprātīgu izmantošanu.

(117) Turklāt Eiropas Cilvēktiesību tiesa savā judikatūrā ir precizējusi, ka jebkuram ierobežojumam, kas skar tiesības uz privātumu un datu aizsardzību, būtu jāpiemēro efektīva, neatkarīga un objektīva pārraudzības sistēma, kuru nodrošina vai nu tiesnesis, vai arī cita neatkarīga struktūra ([128]) (piemēram, administratīva iestāde vai parlamenta struktūra).

([121]) Sk. spriedumu lietā *Schrems II*, 174.–175. punkts, un šeit minēto judikatūru. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. spriedumu lietā C-623/17 *Privacy International*, ECLI:EU:C:2020:790, 65. punkts; un apvienotajās lietās C-511/18, C-512/18 un C-520/18, *La Quadrature du Net and Others*, ECLI:EU:C:2020:791, 175. punkts.

([122]) Sk. spriedumu lietā *Schrems II*, 176.un 181. punkts, un šeit minēto judikatūru. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. arī spriedumu lietā *Privacy International*, 68. punkts; un *La Quadrature du Net and Others*, 132. punkts.

([123]) Sk. spriedumu lietā *Schrems II*, 176. punkts. Attiecībā uz dalībvalstu publisko iestāžu piekļuvi sk. arī spriedumu lietā *Privacy International*, 68. punkts; un *La Quadrature du Net and Others*, 132. punkts.

([124]) Sk. spriedumu lietā *Schrems II*, 179. punkts.

([125]) Sk. spriedumu lietā *Schrems II*, 181.–182. punkts.

([126]) Sk. spriedumu lietā *Schrems I*, 95. punkts, un *Schrems II*, 194. punkts. Šajā sakarā EST ir īpaši uzsvērusi, ka Pamattiesību hartas 47. panta ievērošana, garantējot tiesības uz efektīvu tiesisko aizsardzību neatkarīgā un objektīvā tiesā, "atbilst arī Eiropas Savienībā prasītajam aizsardzības līmenim un tā ievērošana Komisijai ir jākonstatē, pirms tā pieņem lēmumu par aizsardzības līmeņa pietiekamību saskaņā ar Regulas (ES) 2016/679 45. panta 1. punktu" (*Schrems II*, 186. punkts).

([127]) 1998. gada Cilvēktiesību likuma 6. pants.

([128]) Eiropas Cilvēktiesību tiesa, *Klass and others v Germany*, prasības pieteikuma Nr. 5029/71, 17.–51. punkts.

(118) Turklāt personām ir jānodrošina efektīvs tiesiskās aizsardzības līdzeklis, un Eiropas Cilvēktiesību tiesa ir paskaidrojusi, ka tiesiskās aizsardzības līdzeklis jāpiedāvā neatkarīgai un objektīvai struktūrai, kura pieņēmusi savu reglamentu un kuras locekļiem ir jābūt augstam amatam vai ieņēmušiem augstu amatu tiesu iestādē vai jābūt pieredzējušiem juristiem, un ka nedrīkst būt pierādīšanas pienākums, lai tajā iesniegtu pieteikumu. Uzņemoties privātpersonu sūdzību izskatīšanu, neatkarīgai un objektīvai struktūrai būtu jābūt pieejai visai attiecīgajai informācijai, tostarp slēgtiem materiāliem. Visbeidzot, tai vajadzētu būt pilnvarām novērst neatbilstību ([129]).

(119) 2018. gadā Apvienotā Karaliste arī ratificējusi Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108) un parakstīja Protokolu, ar kuru groza Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108+) ([130]). Konvencijas Nr. 108 9. pantā paredzēts, ka atkāpes no vispārējiem datu aizsardzības principiem (5. pants "Datu kvalitāte"), noteikumiem, kas reglamentē īpašas datu kategorijas (6. pants "Īpašas datu kategorijas") un datu subjekta tiesības (8. pants "Datu subjekta papildu garantijas"), ir pieļaujamas tikai tad, ja šādas atkāpes ir paredzētas Puses tiesību aktos un ir nepieciešams pasākums demokrātiskā sabiedrībā valsts drošības, sabiedriskās drošības, valsts monetāro interešu aizsardzības vai noziedzīgu nodarījumu apkarošanas interesēs vai arī datu subjekta vai citu personu tiesību un brīvību aizsardzībai ([131]).

(120) Tāpēc, pateicoties dalībai Eiropas Padomē, Eiropas Cilvēktiesību konvencijas ievērošanai un pakļaujoties Eiropas Cilvēktiesību tiesas jurisdikcijai, uz Apvienoto Karalisti attiecas vairāki starptautiskajos tiesību aktos noteikti pienākumi, kas nosaka tās valdības piekļuves sistēmu, pamatojoties uz principiem, garantijām un individuālām tiesībām, kas līdzīgas ES tiesību aktos garantētajām un dalībvalstīm piemērojamajām. Kā uzsvērts 19. apsvērumā, pastāvīga šādu instrumentu ievērošana ir īpaši svarīgs novērtējuma elements, uz kura balstīts šis lēmums.

(121) Turklāt īpašas datu aizsardzības garantijas un tiesības garantē 2018. gada DAL gadījumos, kad datus apstrādā publiskās iestādes, tostarp tiesībaizsardzības iestādes un valsts drošības struktūras.

(122) Konkrēti, personas datu apstrādes režīms krimināltiesību aktu piemērošanas kontekstā ir noteikts 2018. gada DAL 3. daļā, kas tika ieviesta nolūkā transponēt Direktīvu (ES) 2016/680. 2018. gada DAL 3. daļu piemēro personas datu apstrādei, kuru veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu ([132]).

(123) Jēdziens "kompetentā iestāde" ir definēts DAL 30. pantā kā persona, kas minēta 2018. gada DAL 7. pielikumā, kā arī jebkāda cita persona, ciktāl tai ir likumā noteiktas funkcijas jebkādiem tiesībaizsardzības nolūkiem ([133]). Kā skaidrots turpmāk (sk. 139. apsvērumu), noteiktas kompetentās iestādes (piemēram, Valsts noziedzības apkarošanas aģentūra) saskaņā ar konkrētiem nosacījumiem var izmantot pilnvaras, kas paredzētas 2016. gada Izmeklēšanas pilnvaru likumā (2016. gada IPL). Šajā gadījumā papildus 2018. gada DAL 3. daļā minētajām garantijām piemēros 2016. gada IPL minētās garantijas. Izlūkdienesti (Slepenās izlūkošanas dienests, Drošības dienests un Valdības sakaru štābs) nav kompetentās iestādes ([134]) 2018. gada DAL 3. daļas nozīmē, tāpēc tajā minētie noteikumi uz šo izlūkdienestu darbību neattiecas. 2018. gada DAL konkrēta daļa (4. daļa) ir veltīta izlūkdienestu veiktai personas datu apstrādei (plašāku informāciju sk. 125. apsvērumā).

([129]) Eiropas Cilvēktiesību tiesa, *Kennedy v the United Kingdom*, prasības pieteikuma Nr. 26839/05, ("*Kennedy*"), 167. un 190. punkts.

([130]) Plašāku informāciju par Eiropas Cilvēktiesību konvenciju un tās iekļaušanu Apvienotās Karalistes tiesību aktos, pieņemot 1998. gada Cilvēktiesību likumu, kā arī par Konvenciju Nr. 108, sk. 9. apsvērumu.

([131]) Līdzīgi saskaņā ar Konvencijas Nr. 108+ 11. pantu dažu konvencijas īpašo tiesību un pienākumu ierobežojumi valsts drošības nolūkā vai nolūkā novērst, izmeklēt noziedzīgus nodarījumus un saukt pie atbildības par tiem, kā arī izpildīt krimināLsodus ir pieļaujami tikai tad, ja šāds ierobežojums ir paredzēts tiesību aktos, respektē pamattiesību un pamatbrīvību būtību un ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā. Apstrādes darbībām valsts drošības un aizsardzības nolūkā arī piemēro neatkarīgu un efektīvu izvērtējumu un uzraudzību saskaņā ar attiecīgās konvencijas Puses valsts tiesību aktiem.

([132]) 2018. gada DAL 31. pants.

([133]) Kompetentās iestādes, kas minētas 7. pielikumā, ietver ne vien policijas spēkus, bet arī visas Apvienotās Karalistes valdības ministrijas, kā arī citas iestādes, kurām ir izmeklēšanas funkcijas (piemēram, Viņas Majestātes ieņēmumu un muitas komisārs, Valsts noziedzības apkarošanas aģentūra, Velsas ieņēmumu pārvalde, Konkurences un tirgu iestāde vai Viņas Majestātes Zemes reģistrs), prokuratūras aģentūras, citas krimināltiesību aģentūras un citas personas vai organizācijas, kas veic tiesībaizsardzības darbības (to skaitā 2018. gada DAL 7. pielikumā uzskaitīti prokuratūru direktori, Ziemeļīrijas Prokuratūras direktors vai Informācijas komisija).

([134]) 2018. gada DAL 30. panta 2. punkts.

(124) Līdzīgi kā Direktīvā (ES) 2016/680, arī 2018. gada DAL 3. daļā ir noteikti likumīguma un godprātības ([135]), nolūka ierobežošanas ([136]), datu minimizēšanas ([137]), precizitātes ([138]), glabāšanas ierobežojuma ([139]) un drošības ([140]) principi. Tiesību akti uzliek īpašus pārredzamības nodrošināšanas pienākumus ([141]) un nodrošina personām tiesības piekļūt ([142]), panākt savu datu labošanu un dzēšanu ([143]), kā arī tiesības nebūt automatizētas lēmumu pieņemšanas subjektam ([144]). Kompetentajām iestādēm ir arī jāievieš integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma, jānodrošina apstrādes darbību uzskaite un attiecībā uz dažām apstrādes darbībām jāveic novērtējumi par ietekmi uz datu aizsardzību un iepriekš jākonsultējas ar informācijas komisāru ([145]). Saskaņā ar 2018. gada DAL 56. pantu tām ir jāpierāda atbilstība. Turklāt tām ir jāievieš atbilstoši pasākumi apstrādes drošības nodrošināšanai ([146]), un datu aizsardzības pārkāpuma gadījumā tām ir jāuzņemas īpašas saistības, tostarp pienākums ziņot par šādiem pārkāpumiem informācijas komisāram un datu subjektiem ([147]). Tāpat kā paredzēts Direktīvā (ES) 2016/680, uz pārzini (ja vien tā nav tiesa vai cita tiesu iestāde, kas darbojas kā tiesnesis) ir attiecināma prasība iecelt datu aizsardzības speciālistu (DAS) ([148]), kurš palīdz pārzinim izpildīt tā pienākumus, kā arī uzrauga šo atbilstību ([149]). Turklāt tiesību aktos ir noteiktas konkrētas prasības personas datu starptautiskai nosūtīšanai tiesībaizsardzības nolūkā uz trešām valstīm vai starptautiskām organizācijām, lai nodrošinātu aizsardzības nepārtrauktību ([150]). Šī lēmuma pieņemšanas dienā Komisija ir pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, pamatojoties uz Direktīvas (ES) 2016/680 36. panta 3. punktu, konstatējot, ka datu aizsardzības režīms, kas piemērojams Apvienotās Karalistes kriminālizmeklēšanas iestāžu veiktajai apstrādei, nodrošina aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs Direktīvā (ES) 2016/680 garantētajam.

(125) 2018. gada DAL 4. daļu piemēro visu veidu apstrādei, ko veic izlūkdienesti vai kas tiek veikta to vārdā. Tajā ir noteikti galvenie datu aizsardzības principi (likumīgums, godprātība un pārredzamība ([151]); nolūka ierobežojums ([152]); datu minimizēšana ([153]); precizitāte ([154]); glabāšanas ierobežojums ([155]) un drošība ([156])), kā arī paredzēti nosacījumi īpašu kategoriju datu apstrādei ([157]), datu subjekta tiesības ([158]), prasība par

([135]) 2018. gada DAL 35. pants.
([136]) 2018. gada DAL 36. pants.
([137]) 2018. gada DAL 37. pants.
([138]) 2018. gada DAL 38. pants.
([139]) 2018. gada DAL 39. pants.
([140]) 2018. gada DAL 40. pants.
([141]) 2018. gada DAL 44. pants.
([142]) 2018. gada DAL 45. pants.
([143]) 2018. gada DAL 46. un 47. pants.
([144]) 2018. gada DAL 49. un 50. pants.
([145]) 2018. gada DAL 56.–65. pants.
([146]) 2018. gada DAL 66. pants.
([147]) 2018. gada DAL 67.–68. pants.
([148]) 2018. gada DAL 69.-71. pants.
([149]) 2018. gada DAL 67.–68. pants.
([150]) 2018. gada DAL 3. daļas 5. nodaļa.
([151]) Saskaņā ar 2018. gada DAL 86. panta 6. punktu, lai noteiktu apstrādes godprātību un pārredzamību, ir jāņem vērā to iegūšanas metode. Šajā ziņā godprātības un pārredzamības prasība ir izpildīta, ja dati tiek iegūti no personas, kam ar likumu ir atļauts vai noteikts pienākums tos sniegt.
([152]) Saskaņā ar 2018. gada DAL 87. pantu apstrādes nolūkiem jābūt konkrētiem, skaidriem un leģitīmiem. Datus nedrīkst apstrādāt ar to vākšanas nolūku nesaderīgā veidā. Saskaņā ar 2018. gada DAL 87. panta 3. punktu personas datu turpmāku saderīgu apstrādi var atļaut tikai tad, ja pārzinim ar tiesību aktu ir atļauts apstrādāt datus šādā nolūkā un apstrāde ir nepieciešama un samērīga ar šādu nolūku. Apstrādi uzskata par saderīgu, ja apstrāde tiek veikta arhivēšanas nolūkā sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkā vai statistikas nolūkā, kā arī tai piemēro atbilstošas garantijas (2018. gada DAL 87. panta 4. punkts).
([153]) Personas datiem jābūt adekvātiem, atbilstīgiem un ne pārmērīgiem (2018. gada DAL 88. pants).
([154]) Personas datiem jābūt precīziem un atjauninātiem (2018. gada DAL 89. pants).
([155]) Personas datus nedrīkst glabāt ilgāk, nekā nepieciešams (2018. gada DAL 90. pants).
([156]) Sestais datu aizsardzības princips paredz, ka personas dati ir jāapstrādā tā, lai apstrāde ietvertu atbilstošu drošības pasākumu veikšanu attiecībā uz riskiem, kas rodas, apstrādājot personas datus. Riski ietver (ne tikai) nejaušu vai neatļautu piekļuvi personas datiem vai to iznīcināšanu, nozaudēšanu, izmantošanu, grozīšanu vai izpaušanu (2018. gada DAL 91. pants). 107. pantā ir arī noteikts, ka 1) katram pārzinim jāievieš atbilstoši drošības pasākumi, kas ir piemēroti personas datu apstrādes riskiem, un 2) automatizētas apstrādes gadījumā katrs pārzinis un katrs apstrādātājs īsteno preventīvus vai mīkstinošus pasākumus, pamatojoties uz riska novērtējumu.
([157]) 2018. gada DAL 86. panta 2. punkta b) apakšpunkts un 10. pielikums.
([158]) 2018. gada DAL 4. daļas 3. nodaļa, jo īpaši tiesības: piekļūt datiem, labot un dzēst tos, iebilst pret apstrādi un nebūt automatizētas lēmumu pieņemšanas subjektam, iejaukties automatizētā lēmumu pieņemšanā un tikt informētam par lēmumu pieņemšanu. Turklāt pārzinim jāsniedz datu subjektam informācija par tā personas datu apstrādi. Kā skaidrots IKB norādījumos par izlūkdienestu veiktu apstrādi, personas var izmantot visas savas tiesības (arī uz labošanas pieprasījumu), iesniedzot sūdzību IKB vai prasību tiesā (sk. IKB norādījumus par izlūkdienestu veiktu apstrādi, pieejami vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

datu integrētu aizsardzību ([159]) un reglamentēta personas datu starptautiska nosūtīšana ([160]). IKB nesen izdevis detalizētus norādījumus par izlūkošanas aģentūru veiktu apstrādi saskaņā ar 2018. gada DAL 4. daļu ([161]).

(126) Tajā pašā laikā 2018. gada DAL 110. pantā ir paredzēts atbrīvojums no 2018. gada DAL 4. daļas konkrētiem noteikumiem ([162]), ja šāds atbrīvojums ir nepieciešams, lai aizsargātu valsts drošību. Šo atbrīvojumu var izmantot, pamatojoties uz katra gadījuma atsevišķu analīzi ([163]). Kā paskaidrojušas Apvienotās Karalistes iestādes un ko apstiprina Apvienotās Karalistes judikatūra, "pārzinim ir jāņem vērā faktiskās sekas attiecībā uz valsts drošību vai aizsardzību, ja tam bija jāievēro konkrētais datu aizsardzības noteikums un ja tas varēja saprātīgi ievērot parasto noteikumu, neietekmējot valsts drošību vai aizsardzību" ([164]). IKB pārrauga, vai atbrīvojums ir izmantots pareizi ([165]).

(127) Turklāt attiecībā uz iespēju " valsts drošības" aizsardzības nolūkā ierobežot iepriekš minēto noteikumu piemērošanu, saskaņā ar 2018. gada DAL 111. pantu pārzinis var pieprasīt Ministru kabineta ministra vai ģenerālprokurora parakstītu apliecinājumu, ka šādu tiesību ierobežojums ir nepieciešams un samērīgs pasākums valsts drošības aizsardzībai ([166]).

(128) Apvienotās Karalistes valdība ir izdevusi norādījumus, lai palīdzētu pārziņiem izlemt, vai pieteikties valsts drošības sertifikātam saskaņā ar 2018. gada DAL, kuros īpaši uzsvērts, ka jebkādiem datu subjektu tiesību ierobežojumiem valsts drošības aizsardzības nolūkā jābūt samērīgiem un nepieciešamiem ([167]). Visi valsts drošības sertifikāti jāpublicē IKB tīmekļa vietnē ([168]).

([159]) 2018. gada DAL 103. pants.

([160]) 2018. gada DAL 109. pants. Personas datu nosūtīšana starptautiskām organizācijām vai valstīm ārpus Apvienotās Karalistes ir iespējama, ja šāda nosūtīšana ir nepieciešams un samērīgs pasākums, ko veic likumā noteikto pārziņa funkciju izpildei vai citiem nolūkiem, kas paredzēti konkrētos 1989. gada Drošības dienestu likuma un 1994. gada Izlūkdienestu likuma pantos.

([161]) IKB norādījumi, sk. 158. zemsvītras piezīmi.
2018. gada DAL 30. pants un 2018. gada DAL 7. pielikums.

([162]) 2018. gada DAL 110. panta 2. punktā ir uzskaitīti noteikumi, kuriem ir atļauts piemērot atbrīvojumu. Tie ietver datu aizsardzības principus (izņemot likumīguma principu), datu subjekta tiesības, pienākumu informēt informācijas komisāru par datu aizsardzības pārkāpumu, informācijas komisāra pārbaudes pilnvaras saskaņā ar starptautiskajām saistībām, noteiktas informācijas komisāra izpildes pilnvaras, noteikumus, kas paredz, ka noteikti datu aizsardzības pārkāpumi ir kriminālī sodāmi, un noteikumus, kas attiecas uz īpašiem apstrādes nolūkiem, piemēram, žurnālistikas, akadēmiskiem vai mākslas nolūkiem.

([163]) *Baker v Secretary of State*, sk.61. zemsvītras piezīmi.

([164]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, H iedaļa "Valsts drošības datu aizsardzības un izmeklēšanas pilnvaru regulējums", 15.–16. lpp. (sk. 31. zemsvītras piezīmi). Sk. arī *Baker v Secretary of State* (sk. 61. zemsvītras piezīmi), kurā tiesa atcēla iekšlietu ministra izdoto valsts drošības sertifikātu un apstiprināja izņēmuma piemērošanu sakarā ar valsts drošību, ņemot vērā, ka nebija iemesla paredzēt vispārēju izņēmumu attiecībā uz pienākumu atbildēt uz piekļuves pieprasījumiem un ka šāda izņēmuma atļaušana visās situācijās bez katra gadījuma atsevišķas analīzes pārsniedza to, kas ir nepieciešams un samērīgs valsts drošības aizsardzībai.

([165]) Sk. IKB un Apvienotās Karalistes izlūkdienestu kopienas saprašanās memorandu, saskaņā ar kuru "IKB, saņemot sūdzību no datu subjekta, vēlas pārliecināties, ka jautājums ir izskatīts pareizi un attiecīgā gadījumā – ka jebkāds atbrīvojums ir piemērots pienācīgi". Saprašanās memorands starp informācijas komisāra biroju un Apvienotās Karalistes izlūkdienestu kopienu, 16. punkts, pieejams vietnē https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) Ar 2018. gada DAL ir atcelta iespēja izdod sertifikātus saskaņā ar 1998. gada Datu aizsardzības likuma 28. panta 2. punktu. Tomēr iespēja izdot "vecos sertifikātus" joprojām pastāv, jo ir iespējams īstenot vēsturisku apstrīdēšanu saskaņā ar 1998. gada likumu (sk. 2018. gada DAL 20. pielikuma 5. daļas 17. punktu). Taču šī iespēja šķiet ļoti reta un tiks piemērota tikai ierobežotos gadījumos, piemēram, ja datu subjekts apstrīd atbrīvojuma sakarā ar valsts drošību izmantošanu saistībā ar apstrādi, kuru publiska iestāde veikusi saskaņā ar 1998. gada likumu. Jānorāda, ka šādos gadījumos pilnībā piemēro 1998. gada DAL 28. pantu, tādējādi ietverot datu subjekta iespēju apstrīdēt sertifikātu tiesā.

([167]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem saskaņā ar 2018. gada Datu aizsardzības likumu, pieejami vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Saskaņā ar Apvienotās Karalistes iestāžu sniegto skaidrojumu, lai gan sertifikāts ir pārliecinošs pierādījums tam, ka attiecībā uz sertifikātā aprakstītajiem datiem vai apstrādi ir piemērojams atbrīvojums, tas neatceļ prasību pārzinim katrā gadījumā atsevišķi lemt, vai ir nepieciešams atsaukties uz atbrīvojumu.

([168]) Saskaņā ar 2018. gada DAL 130. pantu IKB var nolemt nepublicēt sertifikāta tekstu vai daļu no tā, ja tas būtu pretrunā valsts drošības vai sabiedrības interesēm vai varētu apdraudēt kādas personas drošību. Šādos gadījumos IKB tomēr publicē informāciju par to, ka sertifikāts ir izdots.

(129) Sertifikātam jābūt izdotam uz laiku, kas nepārsniedz piecus gadus, un izpildvarai tas regulāri jāpārskata ([169]). Sertifikātā norāda personas datus vai personas datu kategorijas, kam piemēro atbrīvojumu, kā arī 2018. gada DAL noteikumus, uz kuriem attiecas atbrīvojums ([170]).

(130) Ir svarīgi norādīt, ka valsts drošības sertifikāti neparedz papildu pamatu datu aizsardzības tiesību ierobežošanai valsts drošības iemeslu dēļ. Citiem vārdiem – pārzinis vai apstrādātājs var paļauties uz sertifikātu tikai tad, ja tas ir secinājis, ka ir nepieciešams atsaukties uz atbrīvojumu sakarā ar valsts drošību, kas, kā paskaidrots iepriekš, jāpiemēro katrā gadījumā atsevišķi ([171]). Pat tad, ja uz konkrēto jautājumu attiecas valsts drošības sertifikāts, IKB var izmeklēt, vai konkrētajā gadījumā paļaušanās uz atbrīvojumu sakarā ar valsts drošību ir bijusi pamatota ([172]).

(131) Jebkura persona, kuru tieši ietekmē sertifikāta izsniegšana, var pārsūdzēt sertifikātu ([173]) Augstākajā tribunālā ([174]) vai, ja sertifikātā dati identificēti ar vispārīgu aprakstu, apstrīdēt sertifikāta piemērošanu konkrētiem datiem ([175]). Tribunāls pārskata lēmumu izdot sertifikātu un lemj, vai sertifikāta izdošanai ir bijis pamatots iemesls ([176]). Tas var vērtēt dažādus jautājumus, tostarp nepieciešamību, samērīgumu un likumīgumu, ņemot vērā ietekmi uz datu subjektu tiesībām un līdzsvarojot tās ar nepieciešamību aizsargāt valsts drošību. Tādējādi tribunāls var noteikt, ka sertifikāts neattiecas uz konkrētiem personas datiem, kas ir pārsūdzības priekšmets ([177]).

(132) Atšķirīgs iespējamo ierobežojumu kopums saskaņā ar 2018. gada DAL 11. pielikumu attiecas uz dažiem 2018. gada DAL 4. daļas noteikumiem ([178]), ar ko aizsargā citus svarīgus vispārēju sabiedrības interešu vai aizsargātu interešu mērķus, piemēram, parlamentārās privilēģijas, advokāta un klienta saziņas konfidencialitāti, tiesvedības norisi vai bruņoto spēku kaujas efektivitāti ([179]). Atbrīvojumi šo noteikumu piemērošanā tiek paredzēti attiecībā uz noteiktām informācijas kategorijām ("balstīti uz kategoriju") vai tiktāl, ciktāl šo noteikumu piemērošana varētu kaitēt aizsargātajām interesēm ("balstīti uz aizskārumu") ([180]). Uz atbrīvojumiem, kas balstīti uz aizskārumu, var atsaukties tikai tiktāl, ciktāl norādītā datu aizsardzības noteikuma piemērošana varētu kaitēt konkrētajām interesēm. Tāpēc

([169]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, 15. punkts, sk. 167. zemsvītras piezīmi.

([170]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, 5. punkts, sk.167. zemsvītras piezīmi.

([171]) Sk. 164. zemsvītras piezīmi.

([172]) Saskaņā ar 2018. gada DAL 102. pantu pārzinim ir jāspēj pierādīt, ka tas ir ievērojis 2018. gada DAL. Tas nozīmē, ka izlūkdienestam būtu jāpierāda IKB, ka, paļaujoties uz atbrīvojumu, tas ir apsvēris konkrētā gadījuma īpašos apstākļus. IKB arī publicē valsts drošības sertifikātu reģistru, kas ir pieejams vietnē https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([173]) 2018. gada DAL 111. panta 3. punkts.

([174]) Augstākais tribunāls ir tiesa, kuras kompetencē ir izskatīt apelācijas sūdzības par zemāku administratīvo tribunālu pieņemtajiem lēmumiem, un tam ir īpaši piekritīgas tiešas sūdzības par noteiktu valsts iestāžu lēmumiem.

([175]) 2018. gada DAL 111. panta 5. punkts.

([176]) Lietā *Baker v Secretary of State* (sk. 61. zemsvītras piezīmi) Informācijas tribunāls atcēla iekšlietu ministra izdoto valsts drošības sertifikātu, ņemot vērā, ka nebija iemesla paredzēt vispārēju izņēmumu attiecībā uz pienākumu atbildēt uz piekļuves pieprasījumiem un ka šāda izņēmuma atļaušana visās situācijās bez katra gadījuma atsevišķas analīzes pārsniedza to, kas ir nepieciešams un samērīgs valsts drošības aizsardzībai.

([177]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, 25. punkts, sk. 167. zemsvītras piezīmi.

([178]) Minētais ietver: i) 4. daļas datu aizsardzības principus, izņemot apstrādes likumīguma prasību saskaņā ar pirmo principu un to, ka apstrādei jāatbilst vienam no 9. un 10. pielikumā izklāstītajiem attiecīgajiem nosacījumiem; ii) datu subjektu tiesības; un iii) pienākumus saistībā ar ziņošanu IKB par pārkāpumiem.

([179]) 2018. gada DAL 4. daļa paredz tiesisko regulējumu, ko piemēro visu veidu personas datu apstrādei, kuru veic izlūkošanas aģentūras (un ne tikai valsts drošības uzdevumu izpildei). Tādējādi 4. daļu piemēro, ja izlūkošanas aģentūras apstrādā datus, piemēram, cilvēkresursu vadības nolūkā, tiesvedības kontekstā vai publiskā iepirkuma kontekstā. Šajos citos kontekstos galvenokārt paredzēts piemērot 11. pielikumā minētos ierobežojumus. Piemēram, ja notiek tiesvedība ar darbinieku, var piemērot ierobežojumu tiesvedības nolūkā, publiskā iepirkuma kontekstā – ierobežojumu sarunu nolūkā utt. Tas ir atspoguļots IKB norādījumos par izlūkdienestu veiktu apstrādi, kuros kā 11. pielikuma ierobežojumu piemērošanas piemērs minētas sarunas par izlīgumu starp izlūkošanas aģentūru un bijušo darbinieku, kas iesniedzis ar nodarbinātību saistītu prasību (sk. 161. zemsvītras piezīmi). Būtu arī jānorāda, ka tādi paši ierobežojumi ir pieejami citām publiskajām iestādēm saskaņā ar 2018. gada DAL 2. pielikuma 2. daļu.

([180]) Saskaņā ar Apvienotās Karalistes paskaidrojuma dokumentu "uz kategoriju balstīti" ir šādi atbrīvojumi: i) informācija par valsts goda apbalvojumu un titulu piešķiršanu; ii) advokāta un klienta saziņas konfidencialitāte; iii) konfidenciālas atsauksmes par darbu, mācībām vai izglītību; un iv) eksāmenu jautājumi un atzīmes. Izņēmumi, kas ir "balstīti uz aizskārumu", attiecas uz šādiem jautājumiem: i) noziedzības novēršanu vai atklāšanu; likumpārkāpēju aizturēšanu un saukšanu pie atbildības; ii) parlamentārajām privilēģijām; iii) tiesvedību; iv) valsts bruņoto spēku kaujas efektivitāti; v) Apvienotās Karalistes ekonomisko labklājību; vi) sarunām ar datu subjektu; vii) zinātniskās vai vēstures pētniecības vai statistikas nolūkiem; viii) arhivēšanu sabiedrības interesēs. Sk. Apvienotās Karalistes paskaidrojuma dokumentu aizsardzības līmeņa pietiekamības apspriešanai, H iedaļa "Valsts drošība", 13. lpp., sk. 31. zemsvītras piezīmi.

atbrīvojuma izmantošana vienmēr ir jāpamato, atsaucoties uz attiecīgo aizskārumu, kas varētu rasties konkrētajā gadījumā. Uz kategoriju balstītus atbrīvojumus var izmantot tikai attiecībā uz konkrētu, precīzi definētu informācijas kategoriju, kurai piešķirts atbrīvojums. To nolūks un sekas ir līdzīgi vairākiem Apvienotās Karalistes VDAR izņēmumiem (saskaņā ar 2018. gada DAL 2. pielikumu), kas savukārt atspoguļo VDAR 23. pantā paredzētos izņēmumus.

(133) No iepriekš minētā izriet, ka saskaņā ar piemērojamajām Apvienotās Karalistes tiesību normām, kā tās interpretē arī tiesas un Informācijas komisija, ir paredzēti nosacījumi, lai nodrošinātu, ka šie atbrīvojumi un ierobežojumi nepārsniedz tos, kas ir nepieciešami un samērīgi valsts drošības aizsardzībai.

3.2. **Apvienotās Karalistes publisko iestāžu piekļuve datiem un datu izmantošana krimināltiesību aktu piemērošanas nolūkā**

(134) Apvienotās Karalistes tiesību aktos ir noteikti vairāki ierobežojumi piekļuvei personas datiem un to izmantošanai krimināltiesību aktu piemērošanas nolūkā, kā arī šajā jomā ir paredzēti pārraudzības un tiesiskās aizsardzības mehānismi, kas atbilst šā lēmuma 113.–115. apsvērumos minētajām prasībām. Apstākļi, kādos var notikt šāda piekļuve, un garantijas, kas piemērojamas šo pilnvaru izmantošanai, sīki izvērtēti nākamajās iedaļās.

3.2.1. *Juridiskais pamats un piemērojamie ierobežojumi/garantijas*

(135) Saskaņā ar 2018. gada DAL 35. pantā garantēto likumīguma principu personas datu apstrāde jebkurā tiesībaizsardzības nolūkā ir likumīga tikai tad, ja tā ir pamatota ar tiesību aktu un vai nu datu subjekts ir devis piekrišanu apstrādei šajā nolūkā ([181]), vai apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko šim nolūkam veic kompetentā iestāde.

3.2.1.1. Kratīšanas orderi un pierādījumu sniegšanas orderi

(136) Apvienotās Karalistes tiesiskajā regulējumā personas datu vākšana no uzņēmējiem, tostarp tiem, kuri apstrādā datus, kas saskaņā ar šo lēmumu par aizsardzības līmeņa pietiekamību tiek nosūtīti no ES, krimināltiesību aktu piemērošanas nolūkos ir atļauta, pamatojoties uz kratīšanas orderiem ([182]) un pierādījumu sniegšanas orderiem ([183]).

(137) Kratīšanas orderus parasti izsniedz tiesa pēc izmeklēšanas ierēdņa pieteikuma. Tie ļauj ierēdnim ieiet telpās nolūkā meklēt materiālu vai personas, kas saistītas ar viņa izmeklēšanu un izņemt jebko, attiecībā uz ko ir atļauta kratīšana, tostarp jebkādus būtiskos dokumentus vai materiālus, kas satur personas datus ([184]). Ar pierādījumu sniegšanas orderi, ko izsniedz arī tiesa, tajā

([181]) Piekrišanas izmantošana nešķiet atbilstoša aizsardzības līmeņa pietiekamības jomā, jo nosūtīšanas situācijā Apvienotās Karalistes tiesībaizsardzības iestāde, pamatojoties uz piekrišanu, datus no ES datu subjekta nebūs vākusi tieši.

([182]) Attiecīgo juridisko pamatu sk. 8. un turpmākajos pantos 1984. gada Likumā par policiju un pierādījumiem krimināllietās (LPPK) (Anglijai un Velsai), 10. un turpmākajos pantos 1989. gada Rīkojumā par policiju un pierādījumiem krimināllietās (Ziemeļīrijai), savukārt Skotijai tas rodams anglosakšu tiesībās (sk. 2016. gada Skotijas Krimināltiesību likuma 46. pantu) un Krimināllikuma (konsolidētais) 23.B pantā (Skotija). Kratīšanas orderiem, kas izdoti pēc aresta, juridiskais pamats ir 1984. gada LPPK 18. pantā (Anglijai un Velsai), 20. un turpmākajos pantos 1989. gada Rīkojumā par policiju un pierādījumiem krimināllietās (Ziemeļīrijai), savukārt Skotijai tas rodams anglosakšu tiesībās (sk. 2016. gada Skotijas Krimināltiesību likuma 46. pantu). Apvienotās Karalistes iestādes paskaidroja, ka kratīšanas orderus izsniedz tiesa pēc izmeklēšanas ierēdņa pieteikuma. Tie ļauj ierēdnim ieiet telpās nolūkā meklēt materiālu vai personas, kas saistītas ar viņa izmeklēšanu; ordera izpildei nereti nepieciešama policijas konstebla palīdzība.

([183]) Ja izmeklēšana attiecas uz nelikumīgi iegūtu līdzekļu legalizāciju (tostarp konfiskāciju un civilām piedziņas procedūrām), atbilstošais juridiskais pamats pierādījumu sniegšanas ordera pieteikumam ir 345. un turpmākie panti Anglijai, Velsai un Ziemeļīrijai un 380. un turpmākie panti Skotijai 2002. gada Likumā par nelikumīgi iegūtiem līdzekļiem. Ja izmeklēšana skar citus jautājumus, nevis nelikumīgi iegūtu līdzekļu legalizāciju, pieteikumu pierādījumu sniegšanas orderim var iesniegt saskaņā ar 1984. gada LPPK 9. pantu un 1. pielikumu Anglijai un Velsai, kā arī 10. un nākamajiem pantiem 1989. gada Rīkojumā par policiju un pierādījumiem krimināllietās (Ziemeļīrija) Ziemeļīrijai. Skotijai to iegūst saskaņā ar anglosakšu tiesībām (sk. 2016. gada Skotijas Krimināltiesību likuma 46. pantu) un Krimināllikuma (konsolidētais) 23.B pantu (Skotija). Apvienotās Karalistes iestādes paskaidroja, ka ar pierādījumu sniegšanas orderi tajā norādītajai personai jāuzrāda vai jāpiešķir piekļuve materiālam, kas ir viņu rīcībā vai kontrolē (sk. 1984. gada LPPK 1. pielikuma 4. punktu).

([184]) Piemēram, 1984. gada LPPK 8. un 18. pantā ir paredzētas pilnvaras konfiscēt un paturēt jebko, attiecībā uz ko atļauts veikt kratīšanu.

norādītajai personai jāuzrāda vai jāpiešķir piekļuve materiālam, kas ir tās rīcībā vai kontrolē. Pieteikuma iesniedzējam ir jāpamato tiesai, kāpēc orderis ir nepieciešams, kā arī kāpēc tas ir sabiedrības interesēs. Ir vairākas likumā noteiktās pilnvaras, kas ļauj izdot kratīšanas orderus un pierādījumu sniegšanas orderus. Katram noteikumam ir savs likumā noteikto nosacījumu kopums, kas jāievēro, lai izdotu kratīšanas orderi ([185]) vai pierādījumu sniegšanas orderi ([186]).

(138) Pierādījumu sniegšanas orderus un kratīšanas orderus var pārskatīt tiesā ([187]). Attiecībā uz garantijām jānorāda, ka visas kriminālizmeklēšanas iestādes, uz kurām attiecas 2018. gada DAL 3. daļas darbības joma, var piekļūt personas datiem (kas ir apstrādes veids) tikai atbilstīgi 2018. gada DAL noteiktajiem principiem un prasībām (sk. iepriekš 122. un 124. apsvērumu). Tāpēc jebkuras tiesībaizsardzības iestādes pieprasījumam būtu jāatbilst principam, saskaņā ar kuru

([185]) Piemēram, LPPK 8. un 18. pants attiecīgi regulē miertiesneša pilnvaras izdot kratīšanas orderi un policista pilnvaras veikt kratīšanu īpašumā. Pirmajā gadījumā (8. pants) pirms ordera izdošanas miertiesnesim vispirms ir jāpārliecinās, ka ir pamatots iemesls uzskatīt, ka: i) ir izdarīts apsūdzams noziedzīgs nodarījums; ii) telpās ir materiāls, kuram, iespējams, ir būtiska vērtība (vai nu atsevišķi, vai kopā ar citiem materiāliem) noziedzīgā nodarījuma izmeklēšanai; iii) materiāls, iespējams, ir būtisks pierādījums; iv) tas (pilnībā vai daļēji) nesastāv no priekšmetiem, uz kuriem attiecas advokāta un klienta saziņas konfidencialitāte, izslēgta materiāla vai īpašas procedūras materiāla; un v) nebūtu iespējams iekļūt telpās bez ordera. Otrajā gadījumā 18. pants ļauj policistam pārmeklēt tādas personas telpas, kas aizturēta par apsūdzamu noziedzīgu nodarījumu, meklējot tādus materiālus, uz ko neattiecas advokāta un klienta saziņas konfidencialitāte, ja viņam ir pamatotas aizdomas, ka telpās ir pierādījumi, kas attiecas uz šo noziedzīgo nodarījumu vai citu līdzīgu vai saistītu apsūdzamu noziedzīgu nodarījumu. Šāda kratīšana attiecināma tikai uz šī materiāla atklāšanu, un tā rakstiski jāapstiprina vismaz inspektora pakāpes policistam, izņemot gadījumus, kad tas nepieciešams noziedzīga nodarījuma izmeklēšanai. Tādā gadījumā vismaz inspektora pakāpes policists ir jāinformē pēc iespējas ātrāk pēc tās veikšanas. Jāreģistrē kratīšanas pamatojums un meklēto pierādījumu veids. Turklāt 1984. gada LPPK 15. un 16. pantā paredzētas likumā noteiktās garantijas, kas jāievēro, lūdzot izsniegt kratīšanas orderi. 15. pantā noteiktas prasības, kas piemērojamas kratīšanas ordera iegūšanai (tostarp konstebla iesniegtā pieteikuma saturam un tam, ka orderī cita starpā jānorāda tiesību akts, saskaņā ar kuru tas izdots, un pēc iespējas jāidentificē meklējamie priekšmeti un personas, kā arī telpas, kurās veicama kratīšana). 16. pantā ir noteikts, kā jāveic kratīšana saskaņā ar orderi (piemēram: 16. panta 5. punktā noteikts, ka policistam, kurš izpilda orderi, jāizsniedz ordera kopija to telpu iemītniekam, kurās veic kratīšanu; 16. panta 11. punktā noteikts, ka orderis pēc izpildes tiek saglabāts 12 mēnešus; 16. panta 12. punktā paredzētas telpu iemītnieka tiesības šajā periodā pārbaudīt orderi, ja viņš to vēlas). Šie panti palīdz nodrošināt atbilstību ECTK 8. pantam (sk., piemēram, lietu *Kent Pharmaceuticals v Director of the Serious Fraud Office* [2002], EWHC 3023 (QB), 30. punkts, *Lord Woolf CJ*). Ja šīs garantijas netiek ievērotas, kratīšana var tikt pasludināta par nelikumīgu (starp piemēriem minamas lietas *R (Brook) v Preston Crown Court* [2018], EWHC 2024 (Admin), [2018] ACD 95; *R (Superior Import / Export Ltd) v Revenue and Customs Commissioners* [2017], EWHC 3172 (Admin), [2018] *Lloyd's Rep FC* 115; un *R (F) v Blackfriars Crown Court* [2014], EWHC 1541 (Admin)). 1984. gada LPPK 15. un 16. pantu papildina LPPK B kodekss – prakses kodekss, kas regulē policijas pilnvaru izmantošanu telpu kratīšanā.

([186]) Piemēram, izsniedzot pierādījumu sniegšanas orderi saskaņā ar 2002. gada Likumu par nelikumīgi iegūtiem līdzekļiem, papildus tam, ka ir nepieciešams pamatots iemesls, lai atbilstu Likuma par nelikumīgi iegūtiem līdzekļiem 346. panta 2. punktā izklāstītajiem nosacījumiem, ir jābūt pamatotam iemeslam uzskatīt, ka norādītais materiāls ir personas rīcībā vai kontrolē un ka materiālam, iespējams, ir būtiska vērtība. Turklāt vēl viena prasība, izdodot pierādījumu sniegšanas orderi, ir tāda, ka ir jābūt pamatotam iemeslam uzskatīt, ka sniedzamā materiāla vai tā pieejamības nodrošināšana ir sabiedrības interesēs, ņemot vērā a) iespējamo ieguvumu izmeklēšanai, iegūstot materiālu; un b) apstākļus, kādos persona, kura pieteikumā norādīta kā tā, kuras rīcībā vai kontrolē ir materiāls, tur šo informāciju. Tāpat tiesai, kas izskata pieteikumu pierādījumu sniegšanas orderim saskaņā ar 1984. gada LPPK 1. pielikumu, ir jāpārliecinās, ka ir izpildīti īpaši nosacījumi. Jo īpaši LPPK 1. pielikumā ir noteikti divi atsevišķi alternatīvi nosacījumu kopumi, no kuriem vienam ir jābūt izpildītam, pirms tiesnesis var izdot pierādījumu sniegšanas orderi. Pirmajā kopumā tiesnesim jābūt pamatotam iemeslam uzskatīt, ka i) ir izdarīts apsūdzams noziedzīgs nodarījums; ii) telpās meklējamais materiāls (pilnībā vai daļēji) sastāv no īpašas procedūras, bet ne izslēgta materiāla; iii) tam, visticamāk, pašam par sevi vai kopā ar citiem materiāliem būs būtiska vērtība izmeklēšanai; iv) un ka tas, iespējams, ir būtisks pierādījums; v) ir mēģināts izmantot citas materiāla iegūšanas metodes vai arī šīs metodes nav mēģinātas, jo tās noteikti būtu nesekmīgas; un vi) ņemot vērā izmeklēšanas ieguvumu un apstākļus, saskaņā ar kādiem materiāls personai ir īpašumā, sabiedrības interesēs ir, lai materiāls tiktu izsniegts vai tiktu nodrošināta piekļuve tam. Otrā nosacījumu kopuma prasības: i) telpās ir materiāls, kuru veido īpašas procedūras vai izslēgts materiāls; ii) ja nebūtu aizliegta kratīšana, pamatojoties uz tiesību aktiem, kas pieņemti pirms LPPK, attiecībā uz īpašas procedūras, izslēgtu vai ar advokāta un klienta saziņas konfidencialitāti aizsargātu materiālu, kratīšanas orderis šim materiālam varētu tikt izdots; un iii) būtu bijis pareizi to darīt.

([187]) Pārskatīšana tiesā ir juridiska procedūra, ar kuru valsts pārvaldes struktūru lēmumus var apstrīdēt Augstajā tiesā. Tiesas "pārskata" apstrīdēto lēmumu un lemj, vai ir pamatoti, ka lēmums ir juridiski kļūdains, ņemot vērā publisko tiesību koncepcijas/principus. Galvenie iemesli pārskatīšanai tiesā ir prettiesiskums, iracionalitāte, procesuālā neatbilstība, tiesiskā paļāvība un cilvēktiesības. Pēc sekmīgas pārskatīšanas tiesā tiesa var izdot rīkojumus par virkni tiesiskās aizsardzības līdzekļu, no kuriem visizplatītākais ir atcelšanas rīkojums (ar ko atceļ vai atsauc sākotnējo lēmumu, proti, lēmumu par kratīšanas ordera izdošanu), dažos gadījumos tas var ietvert arī finansiālas kompensācijas piešķiršanu. Papildu informācija par pārskatīšanu tiesā Apvienotajā Karalistē ir pieejama valdības juridiskā departamenta publikācijā "Judge Over Your Shoulder - a guide to good decision-making", kas pieejama vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

apstrādes nolūkiem jābūt konkrētiem, skaidriem un leģitīmiem ([188]) un kompetentās iestādes apstrādātiem personas datiem ir jābūt atbilstīgiem šim nolūkam un tie nedrīkst būt pārmērīgi ([189]).

3.2.1.2. Izmeklēšanas pilnvaras tiesībaizsardzības nolūkā

(139) Lai novērstu vai atklātu smagus noziegumus ([190]), dažas tiesībaizsardzības iestādes, piemēram, Valsts noziedzības apkarošanas aģentūra vai Policijas priekšnieks ([191]), var izmantot 2016. gada IPL paredzētās mērķētas izmeklēšanas pilnvaras. Šajā gadījumā papildus 2018. gada DAL 3. daļā minētajām garantijām piemēros 2016. gada IPL minētās garantijas. Konkrētās izmeklēšanas pilnvaras, kuras šīs tiesībaizsardzības iestādes var izmantot ir šādas: mērķēta pārtveršana (2016. gada IPL 2. daļa), saziņas datu iegūšana (2016. gada IPL 3. daļa), saziņas datu glabāšana (2016. gada IPL 4. daļa) un mērķēta iejaukšanās iekārtās (2016. gada IPL 5. daļa). Pārtveršana attiecas uz saziņas satura iegūšanu ([192]), savukārt saziņas datu iegūšana un glabāšana ir vērsta nevis uz saziņas satura iegūšanu, bet gan uz saziņas "kas", "kad", "kur" un "kā". Tas, piemēram, aptver saziņas laiku un ilgumu, saziņas ierosinātāja un saņēmēja tālruņa numuru vai e-pasta adresi un dažreiz to ierīču atrašanās vietu, no kurām tika veikta saziņa, tālruņa pakalpojumu abonentu vai detalizētu rēķinu ([193]). Iejaukšanās iekārtās ir metožu kopums, ko izmanto, lai iegūtu dažādus datus no iekārtām, tostarp datoriem, planšetdatoriem un viedtālruņiem, kā arī kabeļiem, vadiem un atmiņas ierīcēm ([194]).

(140) Mērķētas pārtveršanas pilnvaras var izmantot arī tad, ja tās "ir nepieciešamas, lai īstenotu ES savstarpējās palīdzības instrumenta vai starptautiska savstarpējās palīdzības nolīguma noteikumus" (tā dēvētais "savstarpējās palīdzības orderis" ([195])). Savstarpējās palīdzības orderi tiek izdoti tikai saistībā ar pārtveršanu, nevis saziņas datu ieguves vai iejaukšanās iekārtās nolūkos. Šīs mērķētās pilnvaras reglamentē 2016. gada Izmeklēšanas pilnvaru likums (2016. gada IPL) ([196]), kas kopā ar 2000. gada Izmeklēšanas pilnvaru regulēšanas likumu (IPRL) Anglijai, Velsai un Ziemeļīrijai un 2000. gada Izmeklēšanas pilnvaru likumu (Skotija) (IPLS) attiecībā uz Skotiju paredz juridisko pamatu un nosaka piemērojamos ierobežojumus un garantijas šādu pilnvaru izmantošanai. 2016. gada IPL paredzēts arī režīms masveida izmeklēšanas pilnvaru izmantošanai, kaut arī tiesībaizsardzības iestādēm tās nav pieejamas (tās var izmantot tikai izlūkošanas aģentūras) ([197]).

([188]) Apvienotās Karalistes 2018. gada DAL 36. panta 1. punkts.

([189]) Apvienotās Karalistes 2018. gada DAL 37. pants.

([190]) 2016. gada IPL 263. panta 1. punktā paredzēts, ka "smags noziegums" ir noziedzīgs nodarījums, par kuru pamatoti var gaidīt, ka pieaugušajam, kuram iepriekš nav bijis notiesājošs spriedums, tiks piespriesta brīvības atņemšana uz laiku līdz 3 gadiem vai vairāk, vai uzvedība ir saistīta ar vardarbības izmantošanu, rada ievērojamu finansiālu labumu vai to izdara personas grupā. Turklāt, lai iegūtu saziņas datus atbilstīgi 2016. gada IPL 4. daļai, 87. panta 10.B punkts paredz, ka "smags noziegums" ir noziegums, par kuru var piespriest 12 mēnešu vai ilgāku brīvības atņemšanu, vai noziedzīgs nodarījums, kuru izdarījusi persona, kas nav fiziska persona, vai kura neatņemama sastāvdaļa ir ziņojuma nosūtīšana vai personas privātuma pārkāpums.

([191]) Konkrētāk, mērķētas pārtveršanas orderim var pieteikties šādas tiesībaizsardzības iestādes: Valsts noziedzības apkarošanas aģentūras ģenerāldirektors, Metropoles policijas komisārs, Ziemeļīrijas Policijas dienesta galvenais konstebls, Skotijas Policijas dienesta galvenais konstebls, Viņas Majestātes ieņēmumu un muitas komisārs, Aizsardzības izlūkdienesta vadītājs un persona, kas ir valsts vai teritorija ārpus Apvienotās Karalistes kompetentā iestāde ES savstarpējās palīdzības instrumenta vai starptautiska savstarpējās palīdzības nolīguma vajadzībām (2016. gada IPL 18. panta 1. punkts).

([192]) Sk. 2016. gada IPL 4. pantu.

([193]) Sk. 2016. gada IPL 261. panta 5. punktu un Saziņas datu masveida iegūšanas prakses kodeksu, kas pieejams šajā vietnē: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, 2.9. punkts.

([194]) Prakses kodekss par iejaukšanos iekārtās, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, 2.2. punkts.

([195]) Savstarpējās palīdzības orderis pilnvaro Apvienotās Karalistes iestādi sniegt palīdzību iestādei ārpus Apvienotās Karalistes teritorijas pārtveršanas nolūkā un nolūkā pārtverto materiālu izpaust šādai iestādei saskaņā ar starptautisko savstarpējās palīdzības instrumentu (2016. gada IPL 15. panta 4. punkts).

([196]) 2016. gada Izmeklēšanas pilnvaru likums (IPL) (sk.: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) aizstāja atšķirīgus likumus attiecībā uz saziņas pārtveršanu, iejaukšanos iekārtās un saziņas datu iegūšanu, jo īpaši 2000. gada IPRL I daļu, kas iepriekš sniedza vispārējo tiesisko regulējumu izmeklēšanas pilnvaru izmantošanai tiesībaizsardzības un valsts drošības iestādēm.

([197]) 2016. gada IPL 138. panta 1. punkts, 158. panta 1. punkts, 178. panta 1. punkts, 199. panta 1. punkts.

(141) Lai izmantotu šīs pilnvaras, iestādēm jāsaņem kompetentas iestādes ([198]) izdots orderis ([199]), kuru apstiprinājis neatkarīgs tieslietu komisārs ([200]) (tā dēvētā "divkāršās drošības" procedūra). Šāda ordera iegūšanai veic nepieciešamības un samērīguma pārbaudi ([201]). Tā kā šīs 2016. gada IPL paredzētās mērķētas izmeklēšanas pilnvaras ir tādas pašas kā valsts drošības dienestiem pieejamās, šādām pilnvarām piemērojamie nosacījumi, ierobežojumi un garantijas ir sīki izklāstīti iedaļā par Apvienotās Karalistes publisko iestāžu piekļuvi personas datiem un to izmantošanu valsts drošības nolūkos (sk. 177. un turpmākos apsvērumus).

3.2.2. *Savāktās informācijas turpmāka izmantošana*

(142) Tiesībaizsardzības iestādes datu apmaiņai ar citu iestādi nolūkiem, kas atšķiras no tiem, kuriem tie sākotnēji tika vākti (tā sauktā "tālākā apmaiņa"), piemēro noteiktus nosacījumus.

(143) Līdzīgi Direktīvas (ES) 2016/680 4. panta 2. punktā paredzētajam 2018. gada DAL 36. panta 3. punkts ļauj personas datus, ko kompetentā iestāde vākusi tiesībaizsardzības nolūkā turpināt apstrādāt (vai nu sākotnējam pārzinim vai citam pārzinim) jebkuram citam tiesībaizsardzības nolūkam, ar nosacījumu, ka pārzinis ar tiesību aktu ir pilnvarots apstrādāt datus šim citam nolūkam un apstrāde ir nepieciešama un samērīga attiecībā uz šo nolūku ([202]). Šajā gadījumā visas 2018. gada DAL 3. daļā paredzētās garantijas, kas minētas 122. un 124. apsvērumā un attiecas uz apstrādi, ko veic saņēmēja iestāde.

(144) Apvienotās Karalistes tiesību sistēmā dažādi tiesību akti skaidri atļauj šādu tālāku apmaiņu. Konkrēti, i) 2017. gada Digitālās ekonomikas likums atļauj apmaiņu starp publiskajām iestādēm vairākiem nolūkiem, piemēram, ja notikusi krāpniecība pret publisko sektoru, kas publiskajām iestādēm radītu zaudējumus vai zaudējumu risku ([203]), vai ir parāds publiskajai iestādei vai valstij ([204]); ii) 2013. gada Noziedzības un tiesu likums, kas ļauj apmainīties ar informāciju ar Valsts noziedzības apkarošanas aģentūru (VNAA) ([205]), lai apkarotu, izmeklētu smagu un organizētu noziedzību un sauktu pie atbildības par to; iii) 2007. gada Smago noziegumu likums, kas ļauj publiskajām iestādēm krāpniecības novēršanas nolūkos izpaust informāciju krāpšanas apkarošanas organizācijām ([206]).

(145) Šie likumi skaidri nosaka, ka informācijas apmaiņai jāatbilst 2018. gada DAL noteiktajiem principiem. Turklāt Policijas kolēģija ir izdevusi Atļauto profesionālo praksi informācijas apmaiņā ([207]), lai palīdzētu policijai ievērot tās datu aizsardzības pienākumus saskaņā ar Apvienotās

([198]) Lielākajā daļā gadījumu ministrs ir tā iestāde, kura izdod orderus saskaņā ar 2016. gada IPL, savukārt Skotijas ministri ir pilnvaroti izdot mērķētas pārtveršanas orderus, savstarpējās palīdzības orderus un mērķētas iejaukšanās iekārtās orderus, kad personas vai telpas, kurās jāveic pārtveršana, un iekārta, kurā jāiejaucas, atrodas Skotijā (sk. 2016. gada IPL 22. un 103. pantu). Ja notiek mērķēta iejaukšanās iekārtās, tiesībaizsardzības iestādes vadītājs (aprakstīts 2016. gada IPL 6. pielikuma 1. un 2. daļā) var izdot orderi saskaņā ar 2016. gada IPL 106. panta nosacījumiem.

([199]) 2016. gada IPL 2. daļas 2. nodaļā paredzēts ierobežots skaits gadījumu, kad pārtveršanu var veikt bez ordera. Tie ietver: pārtveršanu ar sūtītāja vai saņēmēja piekrišanu, pārtveršanu administratīvos vai izpildes nolūkos, pārtveršanu, kas notiek noteiktās iestādēs (cietumos, psihiatriskajās slimnīcās un imigrācijas aizturēšanas iestādēs), kā arī pārtveršanu, kas tiek veikta saskaņā ar attiecīgo starptautisko līgumu.

([200]) Tieslietu komisāri palīdz izmeklēšanas pilnvaru komisāram (IPK) – neatkarīgai struktūrai, kas pārrauga izlūkošanas aģentūru izmeklēšanas pilnvaru izmantošanu (sīkāku informāciju sk. 162. un turpmākajos apsvērumos).

([201]) Sk. jo īpaši 2016. gada IPL 19. un 23. pantu.

([202]) 2018. gada DAL 36. panta 3. punkts.

([203]) 2017. gada Digitālās ekonomikas likuma 56. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2017/30/section/56.

([204]) 2017. gada Digitālās ekonomikas likuma 48. pants.

([205]) 2013. gada Noziedzības un tiesu likuma 7. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2013/22/section/7.

([206]) 2007. gada Smago noziegumu likuma 68. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2007/27/contents.

([207]) Atļautā profesionālā prakse informācijas apmaiņā, pieejama vietnē https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

Karalistes VDAR, DAL un 1998. gada Cilvēktiesību likumu. Informācijas apmaiņas atbilstību piemērojamajam datu aizsardzības tiesiskajam regulējumam, protams, var pārskatīt tiesā ([208]).

(146) Turklāt līdzīgi tam, ko paredz Direktīvas (ES) 2016/680 9. pants, 2018. gada DAL paredz, ka personas datus, kas ievākti jebkādā tiesībaizsardzības nolūkā, var apstrādāt ar tiesībaizsardzību nesaistītā nolūkā, ja apstrādi atļauj tiesību akti ([209]).

(147) Šis apmaiņas veids aptver divus scenārijus: 1) ja kriminālizmeklēšanas iestāde apmainās ar datiem ar tiesībaizsardzības iestādi, kas nav krimināltiesiska un izlūkošanas aģentūra (piemēram, finanšu vai nodokļu iestāde, konkurences iestāde, jauniešu sociālais dienests); un 2) ja kriminālizmeklēšanas iestāde apmainās ar datiem ar izlūkošanas aģentūru. Pirmajā scenārijā personas datu apstrāde ietilps Apvienotās Karalistes VDAR, kā arī 2018. gada DAL 2. daļas darbības jomā. Komisija (12).–111. apsvērumā ir izvērtējusi Apvienotās Karalistes VDAR un 2018. gada DAL 2. daļā paredzētās garantijas un ir nonākusi pie secinājuma, ka Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni personas datiem, kas nosūtīti no Eiropas Savienības uz Apvienoto Karalisti Regulas (ES) 2016/679 ietvaros.

(148) Otrajā scenārijā attiecībā uz kriminālizmeklēšanas iestāžu savākto datu apmaiņu ar izlūkošanas aģentūru valsts drošības nolūkos juridiskais pamats, kas atļauj šādu apmaiņu, ir 2008. gada Pretterorisma likuma (2008. gada PTL) 19. pants ([210]). Saskaņā ar šo likumu jebkura persona var sniegt informāciju jebkuram izlūkdienestam kādas šā dienesta funkcijas izpildes, tostarp "valsts drošības", nolūkiem.

(149) Attiecībā uz nosacījumiem, saskaņā ar kuriem var veikt datu apmaiņu valsts drošības nolūkiem, Izlūkdienestu likums ([211]) un Drošības dienestu likums ([212]) ierobežo izlūkdienestu spēju iegūt datus līdz apjomam, kas ir nepieciešams, lai pildītu to likumā noteiktās funkcijas. Tiesībaizsardzības aģentūrām, kas vēlas apmainīties ar datiem ar izlūkdienestiem, papildus aģentūru likumā noteiktajām funkcijām, kas noteiktas Izlūkdienestu likumā un Drošības dienestu likumā ([213]), jāņem vērā vairāki faktori/ierobežojumi. 2008. gada PTL 20. pantā ir skaidri norādīts, ka jebkurai datu apmaiņai saskaņā ar 19. pantu joprojām ir jāatbilst datu aizsardzības tiesību aktiem; tas nozīmē, ka tiek piemēroti visi 2018. gada DAL 3. daļas ierobežojumi un prasības. Turklāt, tā kā 1998. gada Cilvēktiesību likuma izpratnē kompetentās iestādes ir publiskās iestādes, tām jānodrošina, ka tās rīkojas atbilstīgi konvencijas tiesībām, tostarp ECTK 8. pantam. Šie ierobežojumi nodrošina, ka visa datu apmaiņa starp tiesībaizsardzības aģentūrām un izlūkdienestiem atbilst datu aizsardzības tiesību aktiem un ECTK.

([208]) Sk., piemēram, lietu *M, R v the Chief Constable of Sussex Police* [2019], EWHC 975 (Admin), kur Augstā tiesa tika lūgta izskatīt datu apmaiņu starp policiju un Uzņēmējdarbības noziegumu mazināšanas partnerību (*BCRP*), organizāciju, kas pilnvarota pārvaldīt izslēgšanas paziņojumu shēmas, ar ko aizliedz personām iekļūt tās biedru komerctelpās. Tiesa izskatīja datu apmaiņu, kas veikta, pamatojoties uz līgumu, kura mērķis bija aizsargāt sabiedrību un novērst noziedzību, un galu galā secināja, ka lielākā daļa datu apmaiņas aspektu bija likumīgi, izņemot attiecībā uz kādu sensitīvu informāciju, ar kuru policija apmainījās ar *BCRP*. Cits piemērs ir lieta *Cooper v NCA* [2019], EWCA Civ 16, kurā Apelācijas tiesa apstiprināja datu apmaiņu starp policiju un Smagās organizētās noziedzības apkarošanas aģentūru (SONAA), kas ir tiesībaizsardzības aģentūra un pašlaik ietilpst VNAA.

([209]) 2018. gada DAL 36. panta 4. punkts.

([210]) 2008. gada Pretterorisma likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([211]) 1994. gada Izlūkdienestu likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) 1989. gada Drošības dienestu likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) 1994. gada Izlūkdienestu likuma 2. panta 2. punkts nosaka, ka "izlūkdienesta priekšnieks ir atbildīgs par šī dienesta efektivitāti, un viņa pienākums ir nodrošināt: a) kārtību, kā panākt, lai izlūkdienests nesaņem citu informāciju kā vien to, kas vajadzīga tā funkciju pareizai izpildei, un lai šis dienests neizpauž nekādu informāciju, izņemot, ja tas ir nepieciešams i) šim nolūkam; ii) valsts drošības interesēs; iii) smagu noziegumu novēršanas vai atklāšanas nolūkā; vai iv) jebkura krimināprocesa nolūkā; un b) ka izlūkdienests neveic nekādas darbības, lai sekmētu kādas Apvienotās Karalistes politiskās partijas intereses", savukārt 1989. gada Drošības dienestu likuma 2. panta 2. punktā noteikts, ka "ģenerāldirektors ir atbildīgs par dienesta efektivitāti, un viņa pienākums ir nodrošināt: a) kārtību, kā panākt, lai dienests nesaņem citu informāciju kā vien to, kas vajadzīga tā funkciju pareizai izpildei, un lai šis dienests neizpauž nekādu informāciju, izņemot, ja tas ir nepieciešams šim nolūkam vai smagu noziegumu novēršanai vai atklāšanai vai jebkurā krimināprocesā; un b) ka dienests neveic nekādas darbības, lai sekmētu kādas politiskas partijas intereses; un c) ka ir vienošanās ar Valsts noziedzības apkarošanas aģentūras ģenerāldirektoru par to, kā dienesta rīcību saskaņā ar šā likuma 1. panta 4. punktu saskaņot ar policijas vienību, Valsts noziedzības apkarošanas aģentūras un citu tiesībaizsardzības iestāžu darbību".

(150) Ja kompetentā iestāde plāno ar personas datiem, kas apstrādāti saskaņā ar 2018. gada DAL 3. daļu, apmainīties ar trešās valsts tiesībaizsardzības iestādēm, piemēro konkrētas prasības ([214]). Šādu nosūtīšanu var veikt, ja tā balstīta ministra pieņemtos noteikumos par aizsardzības līmeņa pietiekamību, vai, ja šādu noteikumu nav, jānodrošina atbilstošas garantijas. 2018. gada DAL 75. pants paredz, ka ir jābūt atbilstošām garantijām, ja tās ir noteiktas juridiskajā instrumentā, kas ir saistošs paredzētajam saņēmējam, vai ja pārzinis, novērtējot visus apstākļus, kas saistīti ar šāda veida personas datu nosūtīšanu uz trešo valsti vai starptautisko organizāciju, secina, ka pastāv datu aizsardzībai atbilstošas garantijas.

(151) Ja nosūtīšana nav balstīta noteikumos par aizsardzības līmeņa pietiekamību vai atbilstošās garantijās, tā var notikt tikai noteiktos, konkrētos apstākļos, kas minēti kā "īpaši apstākļi" ([215]). Tas attiecas uz gadījumiem, kad nosūtīšana ir nepieciešama: a) lai aizsargātu datu subjekta vai citas personas vitālas intereses; b) lai pasargātu datu subjekta leģitīmās intereses; c) lai novērstu tūlītējus un nopietnus draudus sabiedriskajai drošībai dalībvalstī vai trešā valstī; d) atsevišķos gadījumos – jebkādā tiesībaizsardzības nolūkā; vai e) atsevišķos gadījumos – juridiskam mērķim (piemēram, saistībā ar tiesvedību vai juridisku konsultāciju saņemšanu). Var atzīmēt, ka d) un e) apakšpunktu nepiemēro, ja datu subjekta tiesības un brīvības nosūtīšanas kontekstā ir svarīgākas par sabiedrības interesēm. Šie apstākļi atbilst īpašām situācijām un nosacījumiem, kas Direktīvas (ES) 2016/680 38. pantā atzīti par "atkāpēm".

(152) Turklāt, ja materiāls, ko tiesībaizsardzības iestādes ieguvušas, pamatojoties uz orderi, ar kuru atļauj pārtveršanu vai iejaukšanos iekārtās, tiek nodots trešai valstij, 2016. gada IPL noteiktas papildu garantijas. Šāda izpaušana, kas definēta kā "informācijas izpaušana ārvalstīs", ir atļauta tikai tad, ja izdevējiestāde uzskata, ka pastāv īpaši atbilstoši pasākumi, kas ierobežo to personu skaitu, kurām dati tiek izpausti, to, cik lielā mērā kāds materiāls tiek izpausts, kā arī jebkura materiāla pavairošanas apmēru un izgatavoto kopiju skaitu. Turklāt izdevējiestāde var uzskatīt, ka ir nepieciešami atbilstoši pasākumi, lai nodrošinātu, ka ikviena materiāla jebkuras daļas izgatavota kopija tiek iznīcināta, tiklīdz vairs nav būtiska iemesla tās glabāšanai (ja tā nav tikusi iznīcināta iepriekš) ([216]).

(153) Visbeidzot, noteikta veida tālāka nosūtīšana no Apvienotās Karalistes uz Amerikas Savienotajām Valstīm nākotnē varētu tikt veikta, pamatojoties uz "Nolīgumu starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā" ("Apvienotās Karalistes un ASV nolīgums" vai "nolīgums") ([217]), kas noslēgts 2019. gada oktobrī ([218]). Kaut arī Apvienotās Karalistes un ASV nolīgums šā lēmuma pieņemšanas laikā vēl nav stājies spēkā, tā paredzamā spēkā stāšanās var ietekmēt to datu tālāku nosūtīšanu uz ASV, kas vispirms nosūtīti uz Apvienoto Karalisti, pamatojoties uz lēmumu. Precīzāk, uz datiem, kas no ES nosūtīti pakalpojumu sniedzējiem Apvienotajā Karalistē, varētu attiecināt elektronisko pierādījumu sniegšanas orderus, ko izdevušas kompetentās ASV tiesībaizsardzības iestādes un kas Apvienotajā Karalistē piemērojami saskaņā ar minēto nolīgumu, tiklīdz tas būs stājies spēkā. Šo iemeslu dēļ šī lēmuma nolūkiem ir būtisks nosacījumu un garantiju novērtējums, saskaņā ar kuriem šādus orderus var izdot un izpildīt.

([214]) Sk. 2018. gada DAL 3. daļas 5. nodaļu.

([215]) 2018. gada DAL 76. pants.

([216]) 2016. gada IPL 54. un 130. pants. Izdevējiestādēm jāapsver nepieciešamība ieviest īpašas garantijas ārvalstu iestādēm nodotajiem materiāliem, lai pārliecinātos, ka uz datiem attiecas garantijas attiecībā uz datu glabāšanu, iznīcināšanu un izpaušanu, kas ir līdzīgas 2016. gada IPL 53. un 129. pantā noteiktajām.

([217]) Nolīgums starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([218]) Šī ir pirmā vienošanās, kas panākta saskaņā ar ASV Likumu par datu likumīgu izmantošanu ārvalstīs (*CLOUD*). Amerikas Savienoto Valstu *CLOUD* likums ir ASV federālais likums, kas tika pieņemts 2018. gada 23. martā un, grozot 1986. gada Likumu par glabāto saziņu, precizē, ka ASV pakalpojumu sniedzējiem ir pienākums izpildīt ASV rīkojumus izpaust satura un ar saturu nesaistītus datus neatkarīgi no tā, kur šie dati tiek glabāti. *CLOUD* likums arī ļauj slēgt izpildlīgumus ar ārvalstu valdībām, pamatojoties uz kuriem ASV pakalpojumu sniedzēji var nodot satura datus tieši šīm ārvalstu valdībām (*CLOUD* likuma teksts ir pieejams vietnē https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) Šajā sakarā jāatzīmē, ka, pirmkārt, attiecībā uz tā materiālo darbības jeb piemērošanas jomu minētais nolīgums ir piemērojams tikai tiem noziegumiem, par kuriem var sodīt ar maksimālo brīvības atņemšanu termiņu vismaz trīs gadi (definēts kā "smags noziegums") ([219]), tostarp "teroristiskai darbībai". Otrkārt, datus, kas tiek apstrādāti citā jurisdikcijā, saskaņā ar minēto nolīgumu var iegūt tikai pēc "ordera (..), kuru tiesa, tiesnesis, maģistrāts vai cita neatkarīga iestāde var pārskatīt vai pārraudzīt saskaņā ar izdevējas puses valsts tiesību aktiem pirms tiesvedības par ordera izpildi vai pēc tās" ([220]). Treškārt, jebkuram orderim jābūt "balstītam prasībās sniegt pamatotu attaisnojumu, kas balstīts uz skaidri formulētiem un ticamiem faktiem, konkrētību, likumību un smagumu attiecībā uz izmeklējamo rīcību" ([221]), un "tam jāattiecas uz konkrētiem kontiem, kā arī jāidentificē konkrēta persona, konts, adrese, personīgā ierīce vai jebkurš cits īpašs identifikators" ([222]). Ceturtkārt, datiem, kas iegūti saskaņā ar minēto nolīgumu, tiek nodrošināta aizsardzība, kas līdzvērtīga īpašajām garantijām, ko paredz tā dēvētais "ES un ASV jumta nolīgums" ([223]) – visaptverošs datu aizsardzības nolīgums, kuru ES un ASV noslēdza 2016. gada decembrī un kurā izklāstīti datu nosūtīšanai tiesībaizsardzības sadarbības jomā piemērojamās garantijas un tiesības, kas visas ir iekļautas minētajā nolīgumā, piemērojot *mutatis mutandis*, jo īpaši ņemot vērā nosūtīšanas īpašo raksturu (proti, nosūtīšanu no privātiem operatoriem tiesībaizsardzības iestādēm, nevis nosūtīšanu starp tiesībaizsardzības iestādēm) ([224]). Apvienotās Karalistes un ASV nolīgums īpaši paredz, ka ES un ASV jumta nolīgumā paredzētajai aizsardzībai līdzvērtīga tiks piemērota "visai personas informācijai, kas iegūta, izpildot orderus, uz kuriem attiecas nolīgums, lai nodrošinātu līdzvērtīgu aizsardzību" ([225]).

(155) Tāpēc datiem, kas saskaņā ar Apvienotās Karalistes un ASV nolīgumu nosūtīti ASV iestādēm, būtu jāpiešķir ES tiesību instrumentā paredzētā aizsardzība ar nepieciešamajiem pielāgojumiem, lai atspoguļotu attiecīgās nosūtīšanas raksturu. Apvienotās Karalistes iestādes ir arī apstiprinājušas, ka jumta nolīguma aizsardzība attieksies uz visu personas informāciju, kas sagatavota vai saglabāta saskaņā ar šo nolīgumu, neatkarīgi no pieprasījuma iesniedzējas iestādes rakstura vai veida (piemēram, gan federālās, gan štatu tiesībaizsardzības iestādes ASV), lai visos gadījumos nodrošinātu līdzvērtīgu aizsardzību. Tomēr Apvienotās Karalistes iestādes ir arī paskaidrojušas, ka informācija par datu aizsardzības pasākumu konkrētu īstenošanu joprojām tiek apspriesta starp Apvienoto Karalisti un ASV. Sarunās ar Eiropas Komisijas dienestiem par šo lēmumu Apvienotās Karalistes iestādes apstiprināja, ka tās ļaus minētajam nolīgumam stāties spēkā tikai tad, kad būs pārliecinātas, ka tā īstenošana atbilst tajā paredzētajām juridiskajām saistībām, tostarp skaidrībai par atbilstību datu aizsardzības standartiem visiem datiem, kas tiek pieprasīti saskaņā ar šo nolīgumu. Tā kā nolīguma iespējamā stāšanās spēkā var ietekmēt šajā lēmumā izvērtēto aizsardzības līmeni, Apvienotajai Karalistei, tiklīdz tā ir pieejama, kā arī jebkurā gadījumā pirms nolīguma stāšanās spēkā būtu jāsniedz Eiropas Komisijai jebkāda informācija un papildu precizējums par veidu, kā ASV pildīs savas nolīgumā paredzētās saistības, lai nodrošinātu šā lēmuma pienācīgu uzraudzību saskaņā ar Regulas (ES) 2016/679 45. panta 4. punktu. Īpaša uzmanība tiks pievērsta jumta nolīgumā paredzētās aizsardzības piemērošanai un pielāgošanai konkrētam nosūtīšanas veidam, uz kuru attiecas Apvienotās Karalistes un ASV nolīgums.

(156) Vispārīgi runājot, jebkuri attiecībā uz nolīguma stāšanos spēkā un piemērošanu būtiski notikumi tiks pienācīgi ņemti vērā, pastāvīgi uzraugot šo lēmumu, tostarp attiecībā uz nepieciešamajiem secinājumiem, kas jāizdara, ja pastāv norādes, ka pēc būtības līdzvērtīgs aizsardzības līmenis vairs netiek nodrošināts.

3.2.3. *Pārraudzība*

(157) Atkarībā no pilnvarām, kādas kompetentās iestādes izmanto, apstrādājot personas datus tiesībaizsardzības nolūkā (neatkarīgi no tā, vai saskaņā ar 2018. gada DAL vai 2016. gada IPL), dažādas struktūras nodrošina šo pilnvaru izmantošanas pārraudzību. Konkrēti, informācijas komisārs pārrauga personas datu apstrādi, ja tā ietilpst

([219]) Nolīguma 1. panta 14. punkts.
([220]) Nolīguma 5. panta 2. punkts.
([221]) Nolīguma 5. panta 1. punkts.
([222]) Nolīguma 4. panta 5. punkts. Reāllaika pārtveršanai piemēro papildu un stingrāku standartu: orderiem jābūt izdotiem uz noteiktu periodu, kas nedrīkst būt ilgāks par to, kas ir pamatoti nepieciešams ordera nolūku sasniegšanai, un tos izdod tikai tad, ja šo pašu informāciju nav iespējams pamatoti iegūt, izmantojot mazāk traucējošu metodi (nolīguma 5. panta 3. punkts).
([223]) Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par personiskas informācijas aizsardzību saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu un atklāšanu, kā arī saukšanu pie krimināltatbildības par tiem, OV L 336, 10.12.2016., 3. lpp., pieejams vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN.
([224]) Nolīguma 9. panta 1. punkts.
([225]) Nolīguma 9. panta 1. punkts.

2018. gada DAL 3. daļas piemērošanas jomā ([226]). Neatkarīgu un tiesisku pārraudzību attiecībā uz izmeklēšanas pilnvaru izmantošanu saskaņā ar 2016. gada IPL nodrošina izmeklēšanas pilnvaru komisāra birojs (IPKB) ([227]) (šī daļa ir aplūkota (250).–255. apsvērumā). Turklāt papildu pārraudzību garantē parlaments, kā arī citas struktūras.

3.2.3.1. 2018. gada DAL 3. daļas pārraudzība

(158) Informācijas komisāra (kura neatkarība un organizācija paskaidrota 87. apsvērumā) vispārīgās funkcijas saistībā ar personas datu apstrādi, kas ietilpst 2018. gada DAL 3. daļas piemērošanas jomā, ir noteiktas 2018. gada DAL 13. pielikumā. IKB galvenais uzdevums ir uzraudzīt un īstenot 2018. gada DAL 3. daļu, kā arī veicināt sabiedrības informētību, konsultēt parlamentu, valdību un citas iestādes un struktūras. Lai saglabātu tiesu iestāžu neatkarību, informācijas komisārs nav pilnvarots pildīt savas funkcijas attiecībā uz personas datu apstrādi, ko veic persona, kas rīkojas tiesu varas ietvaros, vai tiesa vai tribunāls, kas rīkojas tiesu varas ietvaros. Šādos apstākļos pārraudzības funkcijas veic citas struktūras, kā paskaidrots 99.–103. apsvērumā.

(159) Komisāram ir vispārējas izmeklēšanas, korektīvas, atļaujas došanas un padomdevēja pilnvaras attiecībā uz personas datu apstrādi, uz kuru attiecas 3. daļa. Komisāram ir pilnvaras informēt pārzini vai apstrādātāju par iespējamu 2018. gada DAL 3. daļas pārkāpumu, izteikt brīdinājumus vai rājienu pārzinim vai apstrādātājam, kurš ir pārkāpis likuma 3. daļas noteikumus, kā arī pēc savas iniciatīvas vai pēc pieprasījuma sniegt atzinumus parlamentam, valdībai vai citām iestādēm un struktūrām, kā arī sabiedrībai par visiem jautājumiem, kas saistīti ar personas datu aizsardzību ([228]).

(160) Turklāt komisāram ir pilnvaras izdot informatīvus paziņojumus ([229]), novērtējuma paziņojumus ([230]) un izpildes paziņojumus ([231]), kā arī tiesības piekļūt pārziņu un apstrādātāju dokumentiem, piekļūt viņu telpām ([232]) un piemērot administratīvos naudas sodus soda paziņojuma veidā ([233]). IKB regulatīvās rīcības politikā ir izklāstīti apstākļi, kādos tas izsniedz attiecīgi informatīvo, novērtējuma, izpildes un soda paziņojumus ([234]) (sk. arī 93. apsvērumu un Direktīvas (ES) 2016/680 lēmuma par aizsardzības līmeņa pietiekamību 101.–102. apsvērumu).

(161) Saskaņā ar jaunākajiem gada pārskatiem (2018.–2019. ([235]), 2019.–2020. ([236])) informācijas komisārs ir veicis vairākas izmeklēšanas un īstenojis izpildes pasākumus attiecībā uz datu apstrādi tiesībaizsardzības iestādēs. Piemēram, komisārs 2019. gada oktobrī veica izmeklēšanu un publicēja atzinumu par sejas atpazīšanas tehnoloģiju izmantošanu tiesībaizsardzības iestāžu vajadzībām publiskās vietās. Īpaša uzmanība izmeklēšanā tika pievērsta sejas atpazīšanas iespēju izmantošanai tiešraidē Dienvidvelsas policijā un Metropoles policijas dienestā (*MPS*). Turklāt informācijas komisārs izmeklēja *MPS* "bandu matricu" ([237]) un konstatēja virkni nopietnu datu aizsardzības tiesību aktu pārkāpumu, kas varēja mazināt sabiedrības uzticību matricai un datu izmantošanas veidam. Informācijas komisārs 2018. gada novembrī izdeva

([226]) 2018. gada DAL 116. pants.
([227]) Sk. 2016. gada IPL un jo īpaši 1. nodaļas 8. daļu.
([228]) 2018. gada DAL 13. pielikuma 2. punkts.
([229]) Uzlikt pārzinim un apstrādātājam (un noteiktos apstākļos jebkurai citai personai) pienākumu sniegt nepieciešamo informāciju (2018. gada DAL 142. pants).
([230]) Ļaut veikt izmeklēšanu un revīziju, kuru īstenošanai var būt nepieciešams, lai pārzinis vai apstrādātājs ļautu komisāram iekļūt noteiktās telpās, inspicēt vai pārbaudīt dokumentus vai aprīkojumu, intervēt personas, kuras pārziņa uzdevumā apstrādā personas datus (2018. gada DAL 146. pants).
([231]) Atļaujot izmantot korektīvās pilnvaras, kas pārzinim/apstrādātājiem uzliek pienākumu veikt konkrētas darbības vai atturēties no to veikšanas (2018. gada DAL 149. pants).
([232]) 2018. gada DAL 154. pants.
([233]) 2018. gada DAL 155. pants.
([234]) Regulatīvās rīcības politika, sk. 96. zemsvītras piezīmi.
([235]) Informācijas komisāra gada pārskats un finanšu pārskati par 2018.–2019. gadu, sk. 101. zemsvītras piezīmi.
([236]) Informācijas komisāra gada pārskats un finanšu pārskati par 2019.–2020. gadu, sk. 82. zemsvītras piezīmi.
([237]) Datubāze, kurā tika reģistrēti izlūkdati par iespējamiem bandu locekļiem un ar bandām saistītu noziegumu upuriem.

izpildes paziņojumu, un *MPS* pēc tam veica nepieciešamos pasākumus, lai paaugstinātu drošību un pārskatatbildību un nodrošinātu, ka dati tiek izmantoti samērīgi. Vēl viens izpildes darbības piemērs ir komisāra 2018. gada maijā piespriestais 325 000 GBP naudas sods valsts prokuratūrai par nešifrētu DVD nozaudēšanu, kuros bija policijas interviju ieraksti. Informācijas komisārs arī veica izmeklēšanu par plašākiem tematiem, piemēram, 2020. gada pirmajā pusgadā – par mobilo tālruņu izrakstu izmantošanu policijas darba vajadzībām un cietušo personu datu apstrādi policijā. Turklāt komisārs pašlaik izmeklē lietu, kas saistīta ar tiesībaizsardzības iestāžu piekļuvi datiem, kuri ir privātā sektora struktūras *Clearview AI Inc.* rīcībā ([238]).

(162) Papildus informācijas komisāra izpildes pilnvarām, kas minētas apsvērumos (160. un 161. apsvērumā), daži datu aizsardzības tiesību aktu pārkāpumi ir noziedzīgi nodarījumi, un tāpēc par tiem var tikt piemēroti kriminālsodi (2018. gada DAL 196. pants). Tas attiecas, piemēram, uz personas datu iegūšanu, izpaušanu vai glabāšanu bez pārziņa piekrišanas un panākšanu, ka personas dati tiek izpausti citai personai bez pārziņa piekrišanas ([239]); informācijas, kas ir anonimizēti personas dati, atkārtotu identificēšanu, ja tai nav piekritis par personas datu anonimizēšanu atbildīgais pārzinis ([240]); komisāra pilnvaru īstenošanas apzinātu kavēšanu saistībā ar personas datu pārbaudi saskaņā ar starptautiskajām saistībām ([241]), nepatiesu ziņu sniegšanu, atbildot uz informatīvu paziņojumu, vai informācijas iznīcināšanu saistībā ar informatīviem un novērtējuma paziņojumiem ([242]).

3.2.3.2. Citas pārraudzības struktūras kriminālatiesību aktu piemērošanas jomā

(163) Papildus informācijas komisāram kriminālatiesību aktu piemērošanas jomā pastāv vairākas pārraudzības struktūras ar īpašām pilnvarām datu aizsardzības jautājumos. Tostarp, piemēram, par biometrisko materiālu glabāšanu un izmantošanu atbildīgais komisārs ("biometrijas komisārs") ([243]) un par novērošanas kamerām atbildīgais komisārs ([244]).

3.2.3.3. Parlamentārā pārraudzība kriminālatiesību aktu piemērošanas jomā

(164) Izvēlētā iekšlietu komiteja (*HASC*) nodrošina parlamentāro pārraudzību tiesībaizsardzības jomā. Šajā komitejā ir 11 parlamenta deputāti no trim lielākajām politiskajām partijām. Komitejas uzdevums ir pārbaudīt izdevumus, administrāciju un politiku Iekšlietu ministrijā un saistītajās valsts pārvaldes struktūrās, t. i., policijā un VNAA, kuru darbu komiteja var īpaši pārbaudīt ([245]).

([238]) Sk. IKB paziņojumu, pieejams vietnē https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/.

([239]) 2018. gada DAL 170. pants.

([240]) 2018. gada DAL 171. pants.

([241]) 2018. gada DAL 119. panta 6. punkts.

([242]) Finanšu gadā, kas aptvēra laikposmu no 2019. gada 1. aprīļa līdz 2020. gada 31. martam, IKB izmeklēšanas rezultātā izsniegti četri brīdinājumi un sāktas astoņas kriminālvajāšanas. Šīs lietas tika ierosinātas saskaņā ar 1998. gada Datu aizsardzības likuma 55. pantu, 2000. gada Informācijas brīvības likuma 77. pantu un 2018. gada Datu aizsardzības likuma 170. pantu. 75 % gadījumu atbildētāji atzina vainu, ļaujot izvairīties no ilgstošiem tiesas procesiem un ar tiem saistītajām izmaksām. (Informācijas komisāra gada pārskats un finanšu pārskati par 2019.–2020. gadu, sk. 87. zemsvītras piezīmi, 40. lpp.)

([243]) Biometrijas komisāra amats tika izveidots ar 2012. gada Likumu par brīvību aizsardzību (LBA) (sk.: https://www.legislation.gov.uk/ukpga/2012/9/contents). Citu funkciju starpā biometrijas komisārs lemj par to, vai policija drīkst saglabāt dokumentus par DNS profilu un pirkstu nospiedumus, kas iegūti no personām, kuras tikušas arestētas, bet kurām nav tikusi izvirzīta apsūdzība par atbilstošu noziedzīgu nodarījumu (1984. gada LPPK 63.G pants). Turklāt Biometrijas komisārs ir vispārēji atbildīgs par DNS un pirkstu nospiedumu glabāšanu un izmantošanu, kā arī glabāšanu valsts drošības apsvērumu dēļ (2012. gada LBA 20. panta 2. punkts). Biometrijas komisāru ieceļ saskaņā ar Kodeksu par valsts amatpersonu iecelšanu amatā (kodekss pieejams šādā vietnē: https://www.gov.uk/government/publications/governance-code-for-public-appointments), un viņa iecelšanas nosacījumi skaidri paredz, ka viņu var atbrīvot no amata vienīgi iekšlietu ministrs konkrētos, precīzi definētos apstākļos; šādi apstākļi ir pienākumu nepildīšana trīs mēnešu garumā, notiesāšana par noziedzīgu nodarījumu vai iecelšanas nosacījumu neievērošana.

([244]) Par novērošanas kamerām atbildīgā komisāra amats tika izveidots ar 2012. gada Likumu par brīvību aizsardzību, un tā uzdevums ir veicināt Novērošanas kameru prakses kodeksa ievērošanu; pārbaudīt šī kodeksa darbību un konsultēt ministrus par to, vai šis kodekss ir jāgroza. Komisāru ieceļ saskaņā ar tādiem pašiem noteikumiem kā biometrijas komisārus, un tam ir līdzīgas pilnvaras, resursi un aizsardzība pret atcelšanu.

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

(165) Komiteja savas kompetences robežās var izvēlēties savu izmeklēšanas priekšmetu, tostarp konkrētas lietas, ja vien lieta netiek izskatīta tiesā. Komiteja var arī lūgt plaša spektra attiecīgās grupas un personas iesniegt rakstiskus un mutiskus pierādījumus. Tā sagatavo ziņojumus par konstatējumiem un sniedz ieteikumus valdībai ([246]). Tiek gaidīts, ka valdība sniegs atbildi uz katru ziņojuma ieteikumu, un tai jāatbild 60 dienu laikā ([247]).

(166) Novērošanas jomā komiteja arī sagatavoja ziņojumu par 2000. gada Izmeklēšanas pilnvaru regulēšanas likumu (2000. gada IPRL) ([248]), kurā tika konstatēts, ka 2000. gada IPRL nav piemērots mērķim. Tās ziņojums tika ņemts vērā, aizstājot ievērojamas 2000. gada IPRL daļas ar 2016. gada IPL. Pilns izmeklēšanas saraksts ir atrodams komitejas tīmekļa vietnē ([249]).

(167) HASC uzdevumus Skotijā veic Tieslietu apakškomiteja policijas darba jautājumos, savukārt Ziemeļīrijā – Tieslietu komiteja ([250]).

3.2.4. *Tiesiskās aizsardzības līdzekļi*

(168) Attiecībā uz datu apstrādi tiesībaizsardzības iestādēs ir pieejami tiesiskās aizsardzības mehānismi saskaņā ar 2018. gada DAL 3. daļu un 2016. gada IPL, kā arī 1998. gada Cilvēktiesību likumu.

(169) Šī mehānismu virkne sniedz datu subjektiem iedarbīgus administratīvus un tiesiskus aizsardzības līdzekļus, kas jo īpaši ļauj viņiem īstenot to tiesības, tostarp tiesības piekļūt saviem personas datiem vai panākt šādu datu labošanu vai dzēšanu.

(170) Pirmkārt, saskaņā ar 2018. gada DAL 165. pantu datu subjektam ir tiesības iesniegt sūdzību informācijas komisāram, ja datu subjekts uzskata, ka attiecībā uz viņa personas datiem ir pārkāpta 2018. gada DAL 3. daļa ([251]). Informācijas komisārs ir pilnvarots novērtēt pārziņa un apstrādātāja atbilstību 2018. gada DAL, neatbilstības gadījumā pieprasīt tiem veikt nepieciešamos pasākumus un uzlikt naudas sodu.

([246]) Uz izvēlēto komiteju, tostarp Izvēlēto iekšlietu komiteju, attiecas Pārstāvju palātas pastāvīgie rīkojumi. Pastāvīgie rīkojumi ir noteikumi, par kuriem vienojas Pārstāvju palāta un kuri nosaka parlamenta darba kārtību. Izvēlēto komiteju kompetence ir plaša, jo Pastāvīgā rīkojuma 152. panta 1. punkts paredz, ka "izvēlētās komitejas ieceļ, lai pārbaudītu galveno valdības ministriju, kā noteikts šī rīkojuma 2. punktā, un saistīto valsts pārvaldes struktūru izdevumus, administrāciju un politiku". Tas ļauj Izvēlētajai iekšlietu komitejai izskatīt jebkuru Iekšlietu ministrijas politiku, kas ietver politiku (un saistītos tiesību aktus) par izmeklēšanas pilnvarām. Turklāt Pastāvīgā rīkojuma 152. panta 4. punktā ir skaidri norādīts, ka komitejām ir dažādas pilnvaras, tostarp iespēja pieprasīt personām sniegt liecības vai dokumentus par konkrētu jautājumu un sagatavot ziņojumus. Informācija par komitejas pašreizējām un iepriekšējām izmeklēšanām pieejama vietnē https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Anglijas un Velsas Izvēlētās iekšlietu komitejas pilnvaras ir noteiktas Pārstāvju palātas pastāvīgajos rīkojumos, kas pieejami vietnē https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Pieejams vietnē https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Pieejams vietnē https://committees.parliament.uk/committee/83/home-affairs-committee.

([250]) Skotijas Tieslietu apakškomitejas policijas darba jautājumos reglaments ir pieejams vietnē https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, savukārt Ziemeļīrijas Tieslietu komitejas reglaments izklāstīts vietnē http://www.niassembly.gov.uk/assembly-business/standing-orders/.

([251]) Pēdējā IKB gada pārskatā ir detalizēti norādīts saņemto un izbeigto sūdzību raksturs. Konkrēti, par "policijas darbu un sodāmības reģistru" saņemto sūdzību skaits ir 6 % no kopējā saņemto sūdzību skaita (pieaugums par 1 % salīdzinājumā ar iepriekšējo finanšu gadu). Gada pārskats arī parāda, ka visvairāk sūdzību bija par subjektu piekļuves pieprasījumiem (46 % no kopējo sūdzību skaita, pieaugums par 8 % salīdzinājumā ar iepriekšējo finanšu gadu) (IKB gada pārskats par 2019.–2020. gadu, 55. lpp.; sk. 88. zemsvītras piezīmi).

(171) Otrkārt, 2018. gada DAL nodrošina tiesības uz tiesiskās aizsardzības līdzekli pret informācijas komisāru, ja tas nespēj pienācīgi apstrādāt datu subjekta iesniegto sūdzību. Konkrētāk, ja komisārs "nevirza" ([252]) datu subjekta iesniegto sūdzību, sūdzības iesniedzējam ir pieejami tiesiskās aizsardzības līdzekļi, jo viņš var vērsties pirmā līmeņa tribunālā ([253]), lai tas uzdotu komisāram veikt atbilstošus pasākumus sakarā ar sūdzību vai informēt sūdzības iesniedzēju par sūdzības virzību ([254]). Turklāt jebkura persona, kurai komisārs ir izdevis kādu no iepriekš minētajiem paziņojumiem (informatīvu, novērtējuma, izpildes vai soda paziņojumu), var to pārsūdzēt pirmā līmeņa tribunālā. Ja tribunāls uzskata, ka komisāra lēmums neatbilst tiesību aktiem vai ka informācijas komisāram vajadzēja citādi izmantot savu rīcības brīvību, tribunālam ir jāatļauj pārsūdzība vai jānosaka aizstājējs paziņojums vai lēmums, ko informācijas komisārs būtu varējis izdot vai pieņemt ([255]).

(172) Treškārt, personas var tieši panākt tiesisko aizsardzību pret pārziņiem un apstrādātājiem tiesā. Konkrēti, saskaņā ar 2018. gada DAL 167. pantu datu subjekts tiesā var iesniegt pieteikumu par viņa tiesību (kas noteiktas datu aizsardzības tiesību aktos) pārkāpumu, un tiesa ar rīkojumu var pieprasīt, lai pārzinis veic jebkādus pasākumus (vai atturas no to veikšanas) attiecībā uz apstrādi, lai nodrošinātu atbilstību 2018. gada DAL. Turklāt saskaņā ar 2018. gada DAL 169. pantu jebkura persona, kas cietusi kaitējumu datu aizsardzības tiesību aktu (tostarp 2018. gada DAL 3. daļas) prasību pārkāpuma dēļ, izņemot Apvienotās Karalistes VDAR, ir tiesīga saņemt no pārziņa vai apstrādātāja kompensāciju par šo kaitējumu, izņemot gadījumu, kad pārzinis vai apstrādātājs pierāda, ka tas nekādā veidā nav atbildīgs par notikumu, kas izraisījis kaitējumu. Kaitējums ietver gan finansiālus zaudējumus, gan kaitējumu, kas nav saistīts ar finansiāliem zaudējumiem, piemēram, spriedzi.

(173) Visbeidzot ikviena persona, ciktāl tā uzskata, ka publiskās iestādes ir pārkāpušas tās tiesības, tostarp tiesības uz privātumu un datu aizsardzību, var saņemt kompensāciju Apvienotās Karalistes tiesās saskaņā ar 1998. gada Cilvēktiesību likumu ([256]), un pēc valsts tiesiskās aizsardzības līdzekļu izsmelšanas persona var saņemt kompensāciju, vēršoties Eiropas Cilvēktiesību tiesā par Eiropas Cilvēktiesību konvencijā garantēto tiesību pārkāpumiem ([257]) (sk. 111. apsvērumu).

3.2.4.1. Tiesiskās aizsardzības mehānismi, kas pieejami saskaņā ar 2016. gada IPL

(174) Personas var saņemt kompensāciju par 2016. gada IPL pārkāpumiem, vēršoties Izmeklēšanas pilnvaru tribunālā. Tiesiskās aizsardzības iespējas, kas pieejamas saskaņā ar 2016. gada IPL, ir aprakstītas turpmāk 263.– 269. apsvērumā.

([252]) 2018. gada DAL 166. pants jo īpaši attiecas uz šādām situācijām: a) komisārs neveic atbilstošus pasākumus, lai atbildētu uz sūdzību, b) komisārs nesniedz sūdzības iesniedzējam informāciju par sūdzības virzību vai par sūdzības iznākumu, līdz pagājis trīs mēnešu periods, kas sākas no brīža, kad komisārs saņēmis sūdzību, vai c) ja komisārs sūdzības izskatīšanu šajā periodā nav pabeidzis – nesniedz sūdzības iesniedzējam šādu informāciju turpmākajā trīs mēnešu periodā.

([253]) Pirmā līmeņa tribunāls ir tiesa, kuras kompetencē ir izskatīt apelācijas sūdzības par valsts regulatīvo iestāžu pieņemtajiem lēmumiem. Informācijas komisāra lēmuma gadījumā kompetentā palāta ir "Vispārējā regulatīvā palāta", kuras jurisdikcijā ietilpst visa Apvienotā Karaliste.

([254]) 2018. gada DAL 166. pants. Kā piemērs veiksmīgam prasījumam pret IKB tribunālā minams gadījums, kad IKB apstiprināja datu subjekta sūdzības saņemšanu, bet nenorādīja, kādu rīcību plāno veikt, un tāpēc tika dots rīkojums apstiprināt 21 kalendārās dienas laikā: vai tas gatavojās izskatīt sūdzības un, ja tā, pēc tam informēt sūdzības iesniedzēju par izmeklēšanas virzību ne retāk kā ik pēc 21 kalendārās dienas (spriedums vēl nav publicēts), un lieta, kad pirmā līmeņa tribunāls uzskatīja, ka nav skaidrs, vai IKB atbilde sūdzības iesniedzējam ir uzskatāma par sūdzības iznākumu (sk. lietu *Susan Milne v The Information Commission* [2020], spriedums pieejams vietnē https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) 2018. gada DAL 162. un 163. pants.

([256]) Sk., piemēram, lietu *Brow v Commissioner of Police of the Metropolis & Anor* [2019], EWCA Civ 1724, kur saskaņā ar 1998. gada DAL un 1998. gada Cilvēktiesību likumu par nelikumīgu personas informācijas iegūšanu un neatļautu izmantošanu tika piespriesta kaitējuma atlīdzināšana 9000 GBP apmērā, un lietu *R (on the application of Bridges) v Chief Constable of South Wales* [2020], EWCA Civ 1058, kur Apelācijas tiesa pasludināja par nelikumīgu Velsas policijas izvietoto seju atpazīšanas sistēmu, jo tā bija pretrunā ar ECTK 8. pantu un pārziņa veiktais novērtējums par ietekmi uz datu aizsardzību neatbilda 2018. gada DAL.

([257]) Eiropas Cilvēktiesību konvencijas 34. pantā noteikts, ka "Tiesa var saņemt sūdzību no jebkuras fiziskas personas, nevalstiskas organizācijas vai fizisko personu grupas, kas apgalvo, ka kāda no Augstajām Līgumslēdzējām Pusēm ir pārkāpusi viņu tiesības, kas noteiktas konvencijā vai tās protokolos. Augstās Līgumslēdzējas Puses apņemas nekādā veidā nekavēt šo tiesību efektīvu izmantošanu".

3.3. **Apvienotās Karalistes publisko iestāžu piekļuve datiem un datu izmantošana valsts drošības nolūkos**

(175) Apvienotās Karalistes tiesību sistēmā izlūkdienesti, kuri ir pilnvaroti vākt elektronisko informāciju, kas ir pārziņu vai apstrādātāju rīcībā valsts drošības apsvērumu nolūkiem, situācijās, kas attiecas uz aizsardzības līmeņa pietiekamības jomu, ir Drošības dienests ([258]) (MI5), Slepenās izlūkošanas dienests ([259]) (SIS) un Valdības sakaru štābs ([260]) (*GCHQ*) ([261]).

3.3.1. *Juridiskais pamats, ierobežojumi un garantijas*

(176) Apvienotajā Karalistē izlūkošanas aģentūru pilnvaras ir noteiktas 2016. gada IPL un 2000. gada IPRL, kas kopā ar 2018. gada DAL paredz šo pilnvaru materiālo un personisko darbības jomu, kā arī ierobežojumus un garantijas šo pilnvaru izmantošanai. Šīs pilnvaras, kā arī tām piemērojamie ierobežojumi un garantijas ir sīki izvērtēti nākamajās iedaļās.

3.3.1.1. Izmeklēšanas pilnvaras, ko īsteno valsts drošības kontekstā

(177) 2016. gada IPL nodrošina tiesisko regulējumu izmeklēšanas pilnvaru izmantošanai, t. i., pilnvaras pārtvert, piekļūt saziņas datiem un veikt iejaukšanos iekārtās. Ar 2016. gada IPL ieviests vispārējs aizliegums un par noziedzīgu nodarījumu atzīta tādu metožu izmantošanu, kas bez likumīga pilnvarojuma ļauj piekļūt saziņas saturam, piekļūt saziņas datiem vai iejaukties iekārtās ([262]). Tas atspoguļojas faktā, ka šo izmeklēšanas pilnvaru izmantošana ir likumīga tikai tad, ja to veic, pamatojoties uz orderi vai pilnvarojumu ([263]).

(178) 2016. gada IPL paredz detalizētus noteikumus par visu izmeklēšanas pilnvaru darbības jomu un piemērošanu, kā arī konkrētajiem ierobežojumiem un garantijām. Atšķirīgi noteikumi tiek piemēroti atkarībā no izmeklēšanas pilnvaru veida (saziņas pārtveršana, saziņas datu iegūšana un glabāšana un iejaukšanās iekārtās),

([258]) MI5 ir iekšlietu ministra pakļautībā. 1989. gada Drošības dienestu likums nosaka MI5 funkcijas: valsts drošības aizsardzība (tostarp aizsardzība pret spiegošanu, terorismu un sabotāžas draudiem no ārvalstu aģentu darbībām un no darbībām, kuru mērķis ir gāzt vai graut parlamentāro demokrātiju ar politiskiem, rūpnieciskiem vai vardarbīgiem līdzekļiem), Apvienotās Karalistes ekonomiskās labklājības aizsardzība pret ārējiem draudiem un policijas vienību un citu tiesībaizsardzības aģentūru darbību atbalstīšana smagu noziegumu novēršanā un atklāšanā.

([259]) SIS ir ārlietu ministra pakļautībā, un tās funkcijas ir noteiktas 1994. gada Izlūkdienestu likumā. Tā funkcijas ir iegūt un sniegt informāciju par personu darbībām vai nodomiem ārpus Britu salām, kā arī veikt citus uzdevumus, kas saistīti ar šādu personu darbībām vai nodomiem. Šīs funkcijas var veikt tikai valsts drošības interesēs, Apvienotās Karalistes ekonomiskās labklājības interesēs vai smagu noziegumu novēršanas vai atklāšanas atbalsta nolūkā.

([260]) *GCHQ* ir ārlietu ministra pakļautībā, un tā funkcijas ir noteiktas 1994. gada Izlūkdienestu likumā. Šīs funkcijas ir: a) uzraudzīt, izmantot vai traucēt elektromagnētiskos un citus izstarojumus un iekārtas, kas rada šādus izstarojumus, iegūt un sniegt informāciju, kas iegūta no vai saistīta ar šādiem izstarojumiem vai iekārtām, kā arī no šifrēta materiāla; b) sniegt konsultācijas un palīdzību attiecībā uz valodām, tostarp terminoloģiju, ko izmanto tehniskos jautājumos un kriptogrāfijā, un citiem jautājumiem, kas saistīti ar informācijas aizsardzību, bruņotajiem spēkiem, valdībai vai citām organizācijām vai personām, kuras uzskata par piemērotām. Šīs funkcijas var veikt tikai valsts drošības interesēs, Apvienotās Karalistes ekonomiskās labklājības interesēs, attiecībā uz ārpus Britu salām esošu personu darbībām vai nodomiem vai smagu noziegumu novēršanas vai atklāšanas atbalsta nolūkā.

([261]) Citas valsts pārvaldes struktūras, kas veic valsts drošībai nozīmīgas funkcijas, ir Aizsardzības izlūkdienests (DI), Valsts drošības padome un sekretariāts, Apvienotā izlūkošanas organizācija (JIO) un Apvienotā izlūkošanas komiteja (JIC). Tomēr ne *JIC*, ne *JIO* nevar izmantot izmeklēšanas pilnvaras saskaņā ar 2016. gada IPL, savukārt *DI* ir ierobežotas iespējas izmantot savas pilnvaras.

([262]) Aizliegums attiecas gan uz publiskajiem, gan privātajiem sakaru tīkliem, kā arī uz sabiedrisko pasta pakalpojumu gadījumos, kad pārtveršana tiek veikta Apvienotajā Karalistē. Aizliegums neattiecas uz privātā tīkla pārzini, ja pārzinis ir devis tiešu vai netiešu piekrišanu pārtveršanas veikšanai (2016. gada IPL 3. pants).

([263]) Īpašos ierobežotos gadījumos ir iespējama likumīga pārtveršana bez ordera, proti, pārtverot ar sūtītāja vai saņēmēja piekrišanu (2016. gada IPL 44. pants), ierobežotu administratīvu vai izpildes nolūku gadījumā (IPL 45.–48. pants), dažās īpašās iestādēs (2016. gada IPL 49.–51. pants) un saskaņā ar ārvalstu pieprasījumiem (2016. gada IPL 52. pants).

kā arī no tā, vai pilnvaras tiek izmantotas konkrētam nolūkam ([264]) vai masveidā. Detalizēta informācija par katra 2016. gada IPL minētā pasākuma darbības jomu, garantijām un ierobežojumiem ir aprakstīta konkrētajā iedaļā turpmāk.

(179) Turklāt 2016. gada IPL ir papildināts ar vairākiem likumā noteiktajiem prakses kodeksiem, kurus izdevis ministrs, apstiprinājušas abas parlamenta palātas ([265]) un kuri ir piemērojami visā valstī, sniedzot papildu norādījumus par šo pilnvaru izmantošanu ([266]). Lai arī datu subjekti savu tiesību izmantošanā var tieši paļauties uz 2016. gada IPL noteikumiem, 2016. gada IPL 7. pielikuma 5. punktā paredz, ka prakses kodeksi ir pieņemami kā pierādījumi civilprocesos un krimināprocesos, un tiesa, tribunāls vai uzraudzības iestāde, tiesvedībā lemjot par attiecīgo jautājumu, var ņemt vērā jebkādu neatbilstību kodeksiem ([267]). Saistībā ar novērtējumu par Apvienotās Karalistes iepriekšējā novērošanas jomas tiesību akta – 2000. gada IPRL – kvalitāti Eiropas Cilvēktiesību tiesas virsparāta skaidri atzina Apvienotās Karalistes prakses koda atbilstību un pieņēma, ka tā noteikumus varētu ņemt vērā, vērtējot tādu tiesību aktu paredzamību, kas atļauj novērošanu ([268]).

(180) Būtu jāatzīmē, ka valsts drošības dienestiem un noteiktām tiesībaizsardzības iestādēm ([269]) ir pieejamas mērķētas pilnvaras (mērķēta pārtveršana ([270]), saziņas datu iegūšana ([271]), saziņas datu glabāšana ([272]) un mērķēta iejaukšanās iekārtās ([273])), savukārt tikai izlūkdienesti ir tiesīgi izmantot masveida pilnvaras (proti, masveida pārtveršana ([274]), saziņas datu masveida iegūšana ([275]), masveida iejaukšanās iekārtās ([276]) un masveida personas datu kopas ([277])).

(181) Lemjot, kuras izmeklēšanas pilnvaras izmantot, izlūkošanas aģentūrai ir jāpilda 2016. gada IPL 2. panta 2. punkta a) apakšpunktā uzskaitītie "vispārējie pienākumi saistībā ar privātumu", kas ietver nepieciešamības un samērīguma pārbaudi. Konkrētāk, saskaņā ar šo noteikumu publiskajai iestādei, kurai ir nodoms izmantot izmeklēšanas pilnvaras, jāapsver i) vai to, ko tā vēlas sasniegt ar orderi, pilnvarojumu vai paziņojumu, var pamatoti sasniegt ar

([264]) Runājot par, piemēram, šādu pasākumu darbības jomu, 3. un 4. daļas ietvaros (saziņas datu glabāšana un iegūšana) pasākuma darbības joma ir cieši saistīta ar to telesakaru operatoru definīciju, uz kuru lietotāju datiem pasākums attiecas. Citu piemēru var sniegt saistībā ar masveida pilnvaru izmantošanu. Šajā gadījumā šīs pilnvaras ir izmantojamas tikai attiecībā uz saziņu, kuru saņēmušas vai nosūtījušas personas ārpus Britu salām.

([265]) 2016. gada IPL 7. pielikums nosaka kodeksu darbības jomu, procedūru, kas jāievēro, tos izsniedzot, to pārskatīšanas noteikumus un kodeksu ietekmi.

([266]) 2016. gada IPL prakses kodeksi ir pieejami vietnē https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice.

([267]) Lai novērtētu iestāžu rīcības likumīgumu, tiesas un tribunāli izmanto prakses kodeksus. Sk., piemēram: *Dias v Cleveland Police* [2017], UKIPTrib15_586-CH, kur Izmeklēšanas pilnvaru tribunāls atsaucās uz konkrētiem Saziņas datu prakses kodeksa fragmentiem, lai izprastu "noziedzības novēršanas vai atklāšanas vai nekārtību novēršanas" pamatu definīciju, kas izmantota, lūdzot pilnvarojumu saziņas datu iegūšanai. Kodekss tika iekļauts argumentācijā, lai noskaidrotu, vai šis pamatojums ticis izmantots nepareizi. Tiesa secināja, ka apstrīdētā rīcība bija nelikumīga. Tiesas ir vērtējušas arī kodeksu sniegto garantiju līmeni, sk., piemēram, *Just for Law Kids v Secretary of State for the Home Department* [2019], EWHC 1772 (Admin), kur Augstā tiesa konstatēja, ka primārie un sekundārie tiesību akti kopā ar iekšējiem norādījumiem nodrošināja pietiekamas garantijas; vai *R (National Council for Civil Liberties) v Secretary of State for the Home Department & Others* [2019], EWHC 2057 (Admin), kur tiesa konstatēja, ka gan 2016. gada IPL, gan Prakses kodeksā par iejaukšanos iekārtās bija iekļauti pietiekami noteikumi attiecībā uz prasību par orderu konkrētumu.

([268]) Lietā *Big Brother Watch* Eiropas Cilvēktiesību tiesas virspalāta norādīja, ka informācijas komisāra kodekss ir publisks dokuments, kuru apstiprinājušas abas parlamenta palātas, kuru valdība publicējusi tiešsaistē un drukātā formātā un kurš ir jāņem vērā gan personām, kuras veic pārtveršanas pienākumus, gan tiesām (sk. iepriekš 93.–94. punktu). Rezultātā šī tiesa ir pieņēmusi, ka tā noteikumus var ņemt vērā, vērtējot IPRL paredzamību (sk. *Kennedy*, minēts iepriekš, 157. punkts). Tādējādi tiesa pieņemtu, ka vietējie tiesību akti ir pietiekami pieejami (sk. Eiropas Cilvēktiesību tiesa (virspalāta), *Big Brother Watch and others v United Kingdom*, prasību pieteikumu Nr.: 58170/13, 62322/14 un 24960/15, 2021. gada 25. maijs, 366. punkts).

([269]) Attiecībā uz sarakstu ar attiecīgajām tiesībaizsardzības iestādēm, kuras saskaņā ar 2016. gada IPL var piemērot mērķētas izmeklēšanas pilnvaras, sk. 139. zemsvītras piezīmi.

([270]) 2016. gada IPL 2. daļa.

([271]) 2016. gada IPL 3. daļa.

([272]) 2016. gada IPL 4. daļa.

([273]) 2016. gada IPL 5. daļa.

([274]) 2016. gada IPL 136. pants.

([275]) 2016. gada IPL 158. pants.

([276]) 2016. gada IPL 176. pants.

([277]) 2016. gada IPL 199. pants.

citiem mazāk traucējošiem līdzekļiem; ii) vai aizsardzības līmenis, kas jāpiemēro attiecībā uz informācijas iegūšanu, pamatojoties uz orderi, pilnvarojumu vai paziņojumu, ir augstāks šīs informācijas īpašās sensitivitātes dēļ; iii) sabiedrības intereses telesakaru sistēmu un pasta pakalpojumu integritātes un drošības jomā un iv) visi citi sabiedrības interešu aspekti privātuma aizsardzības jomā ([278]).

(182) Veids, kā šie kritēriji jāpiemēro, un veids, kā to atbilstība tiek vērtēta ministra un neatkarīgo tieslietu komisāru atļaujas izmantot šādas pilnvaras ietvaros, ir sīkāk noteikts attiecīgajos prakses kodeksos. Jebkuras šīs izmeklēšanas pilnvaras izmantošanai vienmēr jābūt "samērīgai ar sasniedzamo mērķi, [kas] ietver līdzsvaru starp privātās dzīves aizskāruma nopietnību (un citiem apsvērumiem, kas izklāstīti 2. panta 2. punktā) un nepieciešamību veikt darbību izmeklēšanas, operatīvajā vai spēju jomā". Tas jo īpaši nozīmē, ka tai "būtu jāsniedz reālas izredzes gaidāmā ieguvuma gūšanai un tai nevajadzētu būt nesamērīgai vai patvaļīgai" un "privātās dzīves neaizskaramības ierobežojums būtu jāuzskata par nesamērīgu, ja meklēto informāciju pamatoti varētu iegūt ar citiem mazāk traucējošiem līdzekļiem" ([279]). Konkrētāk, atbilstība samērīguma principam jānovērtē, ņemot vērā šādus kritērijus: "i) ierosinātā privātās dzīves neaizskaramības ierobežojuma apmērs pret to, ko mēģina sasniegt; ii) kā un kāpēc piemērojamās metodes radīs pēc iespējas mazāku iejaukšanos attiecīgajai personai un citiem; iii) vai darbība ir likuma atbilstoša piemērošana un pamatots veids, ņemot vērā visas pamatotās alternatīvas vēlamā sasniegšanai; iv) kādas citas metodes attiecīgā gadījumā vai nu netika ieviestas, vai arī tika izmantotas, bet kuras tiek vērtētas kā nepietiekamas, lai sasniegtu operatīvos mērķus, neizmantojot ierosinātās izmeklēšanas pilnvaras" ([280]).

(183) Praksē, kā paskaidroja Apvienotās Karalistes iestādes, tas nodrošina, ka izlūkošanas aģentūra, pirmkārt, nosaka operatīvo mērķi (tādējādi norobežojot vākšanu, piemēram, starptautiskas terorisma apkarošanas nolūkam, konkrētā ģeogrāfiskā apgabalā), un, otrkārt, pamatojoties uz šo operatīvo mērķi, jāapsver, kura tehniskā iespēja (piemēram, mērķēta vai masveida pārtveršana, iejaukšanās iekārtās, saziņas datu iegūšana) ir samērīgāka (proti, vismazāk traucējoša privātumam, sk. IPL 2. panta 2. punktu) attiecībā uz sasniedzamo mērķi, un tāpēc to var atļaut saskaņā ar vienu no pieejamajiem likumīgajiem pamatiem.

(184) Vērts atzīmēt, ka šo atsaukšanos uz nepieciešamības un samērīguma standartiem ir atzīmējis un atzinīgi novērtējis arī ANO īpašais referents jautājumos par privātumu, Džozefs Kanatači, kurš attiecībā uz 2016. gada IPL izveidoto sistēmu paziņoja, ka "[š]ķiet, ka gan izlūkdienestos, gan tiesībaizsardzības aģentūrās ieviestās procedūras sistemātiski prasa apsvērt novērošanas pasākuma vai operācijas nepieciešamību un samērīgumu, pirms to iesaka pilnvarojumam, kā arī pārskatīt uz tā paša pamata" ([281]). Viņš arī atzīmēja, ka, tiekoties ar tiesībaizsardzības aģentūru un valsts drošības dienestu pārstāvjiem, "[viņš] sadzirdējis vienprātīgu viedokli, ka tiesībām uz privātumu jābūt galvenajam apsvērumam, pieņemot lēmumu par novērošanas pasākumiem. Viņi visi izprata un novērtēja nepieciešamību un samērīgumu kā galvenos principus, kuri jāņem vērā".

([278]) Saziņas pārtveršanas prakses kodeksā noteikts, ka citi samērīguma pārbaudes elementi ir šādi: "i) ierosinātā privātās dzīves neaizskaramības ierobežojuma apmērs pret to, ko mēģina sasniegt; ii) kā un kāpēc piemērojamās metodes radīs pēc iespējas mazāku iejaukšanos attiecīgajai personai un citiem; iii) vai darbība ir likuma atbilstoša piemērošana un pamatots veids, ņemot vērā visas pamatotās alternatīvas vēlamā sasniegšanai; iv) kādas citas metodes attiecīgā gadījumā vai nu netika ieviestas, vai arī tika izmantotas, bet kuras tiek vērtētas kā nepietiekamas, lai sasniegtu operatīvos mērķus, neizmantojot ierosinātās izmeklēšanas pilnvaras". Saziņas pārtveršanas prakses kodeksa 4.16. punkts ir pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([279]) Sk. Saziņas pārtveršanas prakses kodeksa 4.12. un 4.15. punktu, kas ir pieejami vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

([280]) Sk. Saziņas pārtveršanas prakses kodeksa 4.16. punktu.

([281]) Īpašā referenta jautājumos par privātumu misijas beigu paziņojums, kas sniegts, beidzoties viņa misijai Lielbritānijas un Ziemeļīrijas Apvienotajā Karalistē, pieejams vietnē https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, 1.a punkts.

(185) Konkrētie dažādu orderu izsniegšanas kritēriji, kā arī 2016. gada IPL noteiktie ierobežojumi un garantijas attiecībā uz katru izmeklēšanas pilnvaru ir sīki izklāstīti 186.–243. apsvērumā.

3.3.1.1.1. Mērķēta pārtveršana un pārbaude

(186) Ir triju veidu orderi, kas attiecas uz mērķētu pārtveršanu: mērķētās pārtveršanas orderis ([282]), mērķētās pārbaudes orderis un savstarpējās palīdzības orderis ([283]). Nosacījumi šādu orderu iegūšanai, kā arī attiecīgās garantijas ir noteiktas 2016. gada IPL 2. daļas 1. nodaļā.

(187) Mērķētas pārtveršanas orderis ļauj pārtvert saziņu, kas aprakstīta orderī, tās pārraidīšanas laikā un iegūt citus datus, kas attiecas uz šo saziņu ([284]), tostarp sekundāros datus ([285]). Mērķētas pārbaudes orderis pilnvaro personu veikt pārbaudi pārtvertajam saturam, kas iegūts, pamatojoties uz masveida pārtveršanas orderi ([286]).

(188) Jebkuru orderi saskaņā ar 2016. gada IPL 2. daļu var izdot ministrs ([287]) un apstiprināt tieslietu komisārs ([288]). Visos gadījumos jebkura veida mērķēta ordera darbības laiks ir ierobežots līdz 6 mēnešiem ([289]), un attiecībā uz tā grozīšanu ([290]) un atjaunošanu ([291]) tiek piemēroti īpaši noteikumi.

(189) Pirms ordera izdošanas ministram jāveic nepieciešamības un samērīguma novērtējums ([292]). Konkrēti, attiecībā uz mērķētas pārtveršanas orderi un mērķētas pārbaudes orderi ministram jāpārbauda, vai pasākums ir nepieciešams kādam no šiem nolūkiem: valsts drošības intereses; smaga nozieguma novēršana vai atklāšana vai Apvienotās Karalistes ekonomiskās labklājības intereses ([293]), ciktāl šīs intereses attiecas arī uz valsts drošības interesēm ([294]). Savukārt savstarpējās palīdzības orderi (sk. iepriekš 139. apsvērumu) var izdot tikai tad, ja ministrs uzskata, ka pastāv apstākļi, kas ir līdzvērtīgi apstākļiem, kādos viņš izdotu orderi smagu noziegumu novēršanai un atklāšanai ([295]).

(190) Turklāt ministram būtu jāizvērtē, vai pasākums ir samērīgs ar sasniedzamo mērķi ([296]). Pieprasīto pasākumu samērīguma novērtējumā jāņem vērā 2016. gada IPL 2. panta 2. punktā noteiktie vispārējie pienākumi saistībā ar privātumu, jo īpaši nepieciešamība novērtēt, vai to, ko vēlas panākt ar orderi, pilnvarojumu vai paziņojumu var

([282]) 2016. gada IPL 15. panta 2. punkts.
([283]) 2016. gada IPL 15. panta 4. punkts.
([284]) 2016. gada IPL 15. panta 2. punkts.
([285]) Sekundārie dati ir dati, kuri pievienoti pārtvertajai saziņai vai ir loģiski saistīti ar to, tos var loģiski nošķirt no šīs saziņas, un, ja tie tiktu šādi nošķirti, tas neatklātu neko no tā, ko pamatoti varētu uzskatīt par saziņas nozīmi (ja tāda ir). Daži sekundāro datu piemēri ietver maršrutētāja konfigurācijas vai ugunsmūrus vai laika periodu, kurā maršrutētājs ir bijis aktīvs tīklā, kad tie ir daļa no pārtvertās saziņas, pievienoti tai vai ir loģiski saistīti ar to. Vairāk informācijas sk. definīcijā 2016. gada IPL 16. pantā un Saziņas pārtveršanas prakses kodeksa 2.19. punktā, sk. 278. zemsvītras piezīmi.
([286]) Šī pārbaude tiek veikta kā izņēmums 2016. gada IPL 152. panta 4. punktam, kas paredz aizliegumu identificēt to personu saziņu, kuras atrodas Britu salās. Sk. 229. apsvērumu.
([287]) Skotijas ministrs apstiprina orderi, ja tas attiecas uz nopietnu noziedzīgu darbību Skotijā (sk. 2016. gada IPL 21. un 22. pantu), savukārt ministrs var nozīmēt vecāko ierēdni izsniegt savstarpējās palīdzības orderi, ja izrādās, ka pārtveršana attieksies uz personu vai telpām, kas atrodas ārpus Apvienotās Karalistes (2016. gada IPL 40. pants).
([288]) 2016. gada DAL 19. un 23. pants.
([289]) 2016. gada IPL 32. pants.
([290]) 2016. gada IPL 39. pants. Noteiktas personas var veikt ierobežotas izmaiņas orderos saskaņā ar 2016. gada IPL izklāstītajiem nosacījumiem. Persona, kura izdevusi orderi, var jebkurā laikā anulēt orderi. Tā jādara, ja orderis vairs nav vajadzīgs kādu būtisku iemeslu dēļ vai ar orderi atļautā rīcība vairs nav samērīga ar sasniedzamo mērķi.
([291]) 2016. gada IPL 33. pants. Lēmums par ordera atjaunošanu jāapstiprina tieslietu komisāram.
([292]) 2016. gada IPL 19. pants.
([293]) Saistībā ar jēdzienu "Apvienotās Karalistes ekonomiskās labklājības intereses, ciktāl šīs intereses skar valsts drošību" Eiropas Cilvēktiesību tiesas virspalāta *Big Brother Watch and others v United Kingdom* (sk. iepriekš 268. zemsvītras piezīmi) 371. punktā konstatēja, ka šis jēdziens pietiekami attiecas uz valsts drošību. Lai gan tiesas konstatējums šajā lietā bija saistīts ar šā jēdziena izmantošanu 2000. gada IPRL, tas pats jēdziens ir izmantots 2016. gada IPL.
([294]) 2016. gada IPL 20. panta 2. punkts.
([295]) 2016. gada IPL 20. panta 3. punkts.
([296]) 2016. gada IPL 19. panta 1. punkta b) apakšpunkts, 19. panta 2. punkta b) apakšpunkts un 19. panta 3. punkta b) apakšpunkts.

pamatoti panākt ar citiem mazāk traucējošiem līdzekļiem, un vai attiecībā uz informācijas iegūšanu, pamatojoties uz orderi, piemērojamais aizsardzības līmenis ir augstāks šīs informācijas īpašās sensitivitātes dēļ (sk. iepriekš 181. apsvērumu).

(191) Šajā nolūkā ministram jāņem vērā visi pieteikuma elementi, kurus pieprasījuma iesniedzēja iestāde norādījusi, jo īpaši tie, kas saistīti ar pārtveramajām personām un pasākuma atbilstību izmeklēšanai. Šādi elementi ir izklāstīti Saziņas pārtveršanas prakses kodeksā, un to aprakstam ir jābūt pietiekami konkrētam ([297]). Turklāt 2016. gada IPL 17. pantā noteikts, ka visos orderos, kas izdoti saskaņā ar tā 2. nodaļu, ir jānorāda vai jāapraksta konkrētā persona vai personu grupa, organizācija vai telpas, kuras jāpārtver ("mērķis"). Mērķētas pārtveršanas ordera vai mērķētas pārbaudes ordera gadījumā tie var attiekties arī uz personu grupu, vairāk nekā vienu personu vai organizāciju vai vairāk nekā vienu telpu kopu (saukts arī par "tematisko orderi") ([298]). Šādos gadījumos orderī jāapraksta personu grupas vai operācijas/ izmeklēšanas kopīgais nolūks un jānosauc vai jāapraksta tik daudz šo personu/organizāciju vai telpu kopu, cik tas saprātīgi ir iespējams ([299]). Visbeidzot, visos orderos, kas izdoti saskaņā ar 2016. gada IPL 2. daļu, jānorāda adreses, numuri, aparāti, faktori vai faktoru kombinācija, kas jāizmanto saziņas identificēšanai ([300]). Šajā sakarā Saziņas pārtveršanas prakses kodeksā ir noteikts, ka mērķētas pārtveršanas ordera un mērķētas pārtveršanas ordera gadījumā "orderī jānorāda (vai jāapraksta) faktori vai faktoru kombinācija, kas tiks izmantoti saziņas identificēšanai. Ja saziņa jāidentificē, atsaucoties uz tālruņa numuru (piemēram), numurs jānorāda pilnībā. Bet, ja saziņas identificēšanai tiks izmantoti ļoti sarežģīti vai pastāvīgi mainīgi interneta selektori, šie selektori pēc iespējas jāapraksta" ([301]).

(192) Svarīga garantija šajā kontekstā ir tas, ka ministra veiktais novērtējums par ordera izdošanu ir jāapstiprina neatkarīgam tieslietu komisāram ([302]), kurš jo īpaši pārbaudīs, vai lēmums izdot orderi atbilst nepieciešamības un samērīguma principiem ([303]) (par tieslietu komisāru statusu un lomu sk. turpmāk 251.–256. apsvērumā). 2016. gada IPL arī paskaidrots, ka, veicot šādu pārbaudi, tieslietu komisāram jāpiemēro tie paši principi, kuri tiktu piemēroti tiesā, iesniedzot pieteikumu pārskatīšanai tiesā ([304]). Tādējādi tiek nodrošināts, ka ikvienā gadījumā pirms piekļuves datiem neatkarīga struktūra sistemātiski pārbauda nepieciešamības un samērīguma principu ievērošanu.

(193) 2016. gada IPL paredz dažus konkrētus un precīzus izņēmumus attiecībā uz mērķētas pārtveršanas īstenošanu bez ordera. Ierobežotie gadījumi ir detalizēti izklāstīti likumā ([305]), un, izņemot gadījumu, kurš ir balstīts uz sūtītāja/ saņēmēja piekrišanu, tos īsteno personas (privātas vai valsts pārvaldes struktūras), kas nav valsts drošības dienesti. Turklāt šāda veida pārtveršanu veic nolūkiem, kas atšķiras no izlūkdatu vākšanas ([306]), un dažos gadījumos ir maz ticams, ka vākšana var notikt nosūtīšanas scenārija kontekstā (piemēram, ja pārtveršanu veic psihiatriskajā slimnīcā

([297]) Pieprasītā informācija ietver vēsturisko informāciju (personu/organizāciju / telpu kopas apraksts, pārtveramā saziņa) un to, kā šīs informācijas iegūšana dos ieguvumu izmeklēšanai, kā arī rīcības, kurai tiek prasīta atļauja, aprakstu. Gadījumā, ja nav iespējams aprakstīt personas/organizāciju/telpas, iekļauj paskaidrojumu, kāpēc tas nebija iespējams vai kāpēc tika veikts tikai vispārīgs apraksts (Saziņas pārtveršanas prakses kodeksa 5.32. un 5.34. punkts, sk. 278. zemsvītras piezīmi).

([298]) 2016. gada IPL 17. panta 2. punkts. Sk. arī Saziņas pārtveršanas prakses kodeksu, 5.11. un turpmākos punktus, sk. 278. zemsvītras piezīmi.

([299]) 2016. gada IPL 31. panta 4. un 5. pants.

([300]) 2016. gada IPL 31. panta 8. punkts.

([301]) Sk. arī Saziņas pārtveršanas prakses kodeksu, 5.37. un 5.38. punktu, sk. 278. zemsvītras piezīmi.

([302]) Tieslietu komisāra apstiprinājums nav nepieciešams, ja ministrs uzskata, ka ordera izdošana ir steidzami nepieciešama (IPL 19. panta 1. punkts). Tomēr tieslietu komisārs ir jāinformē īsā laika posmā un jāizlemj, vai apstiprināt orderi. Pretējā gadījumā orderis vairs nav spēkā (2016. gada IPL 24. un 25. pants).

([303]) 2016. gada IPL 23. panta 1. punkts.

([304]) 2016. gada IPL 23. panta 2. punkts.

([305]) Sk. 2016. gada IPL 44.–51. pantu un Saziņas pārtveršanas prakses kodeksa 12. pantu (sk. 278. zemsvītras piezīmi).

([306]) Šāds gadījums ir, piemēram, tad, ja pārtveršana ir nepieciešama cietumā vai psihiatriskajā slimnīcā (lai pārbaudītu aizturētās personas vai pacienta uzvedību) vai jāveic pasta vai telesakaru operatoram, lai, piemēram, konstatētu ļaunprātīgu saturu.

vai cietumā). Ņemot vērā tās struktūras būtību, uz kuru attiecas šie konkrētie gadījumi (struktūra, kas nav valsts drošības dienests), piemēro visas 2018. gada DAL 2. daļā un Apvienotās Karalistes VDAR minētās garantijas, ieskaitot IKB pārraudzību un pieejamos tiesiskās aizsardzības mehānismus. Turklāt papildus 2018. gada DAL minētajām garantijām dažos gadījumos 2016. gada IPL arī paredz IPKB *ex post* pārraudzību ([307]).

(194) Ņemot vērā pārtvertās(-o) personas(-u) konkrēto statusu, pēc pārtveršanas ir piemērojami papildu ierobežojumi un garantijas ([308]). Piemēram, tādu lietu pārtveršana, uz kurām attiecas advokāta un klienta saziņas konfidencialitāte, ir atļauta tikai ārkārtēju un spiedīgu apstākļu gadījumā; personai, kura izsniedz orderi, jāņem vērā sabiedrības intereses par tādu lietu konfidencialitāti, uz kurām attiecas advokāta un klienta saziņas konfidencialitāte, un ka uz šāda materiāla apstrādi, glabāšanu un izpaušanu attiecas konkrētas prasības ([309]).

(195) Turklāt 2016. gada IPL paredz īpašas garantijas attiecībā uz drošību, glabāšanu un izpaušanu, kas ministram būtu jāņem vērā pirms mērķēta ordera izdošanas ([310]). Konkrēti, 2016. gada IPL 53. panta 5. punktā ir noteikts, ka katra kopija, kas izgatavota no šī materiāla, kurš savākts saskaņā ar orderi, ir jāuzglabā drošā veidā un jāiznīcina, tiklīdz vairs nav būtiska iemesla tā glabāšanai, savukārt 2016. gada IPL 53. panta 2. punktā noteikts, ka to personu skaitam, kurām materiāls tiek izpausts, un apmēram, kādā materiāls tiek izpausts, darīts pieejams vai kopēts, jābūt ierobežotam līdz minimumam, kas nepieciešams likumā paredzētajiem nolūkiem.

(196) Visbeidzot, ja materiāls, kas pārtverts, izmantojot vai nu mērķētu pārtveršanas orderi, vai arī savstarpējās palīdzības orderi, ir jānodod trešai valstij ("informācijas izpaušana ārvalstīs"), 2016. gada IPL paredz, ka ministram jānodrošina, lai tiktu ieviesti pasākumi, kas nodrošina, ka šajā trešā valstī pastāv līdzīgas drošības, glabāšanas un izpaušanas garantijas ([311]). Turklāt 2018. gada DAL 109. panta 2. punktā paredzēts, ka izlūkdienesti personas datus drīkst nosūtīt ārpus Apvienotās Karalistes teritorijas tikai tad, ja nosūtīšana ir nepieciešams un samērīgs pasākums pārziņa likumā noteikto funkciju vai citu mērķu sasniegšanai, kā paredzēts 1989. gada Drošības dienestu likuma 2. panta 2. punkta a) apakšpunktā vai 1994. gada Izlūkdienestu likuma 2. panta 2. punkta a) apakšpunktā un 4. panta 2. punkta a) apakšpunktā ([312]). Ir svarīgi norādīt, ka šīs prasības piemēro arī gadījumos, kad izmanto atbrīvojumu sakarā ar valsts drošību atbilstīgi 2018. gada DAL 110. pantam, jo 2018. gada DAL 110. pants neparedz 2018. gada DAL 109. pantu kā vienu no noteikumiem, kuru var nepiemērot, ja valsts drošības aizsardzības nolūkā nepieciešams atbrīvojums no konkrētiem noteikumiem.

3.3.1.1.2. Saziņas datu mērķēta iegūšana un glabāšana

(197) 2016. gada IPL ļauj ministram pieprasīt telesakaru operatoriem saglabāt saziņas datus, lai nodrošinātu virknei publisko iestāžu, tostarp tiesībaizsardzības un izlūkošanas aģentūrām, mērķētu piekļuvi tiem. 2016. gada IPL 4. daļa paredz saziņas datu glabāšanu, savukārt 3. daļa paredz saziņas datu mērķētu iegūšanu (*TCD*). 2016. gada IPL 3. un 4. daļa arī nosaka konkrētus ierobežojumus šo pilnvaru izmantošanai un paredz īpašas garantijas.

([307]) Sk. *a contrario* IPL 229. panta 4. punktu.

([308]) 2016. gada IPL 26.–29. pantā ir noteikti ierobežojumi mērķētas pārtveršanas un pārbaudes orderu iegūšanai attiecībā uz tādas saziņas pārtveršanu, kuru nosūtījusi vai kura paredzēta personai, kas ir parlamenta (jebkura Apvienotās Karalistes parlamenta) deputāts, tādu lietu pārtveršanu, uz kurām attiecas advokāta un klienta saziņas konfidencialitāte, tādas saziņas pārtveršanu, kas, pēc pārtvērējas iestādes domām, ir saziņa, kas satur konfidenciālu žurnālistikas materiālu, un gadījumos, kad ordera mērķis ir identificēt vai apstiprināt žurnālistikas informācijas avotu.

([309]) 2016. gada IPL 26. pants.

([310]) 2016. gada IPL 19. panta 1. punkts.

([311]) 2016. gada IPL 54. pants. Garantijas, kas saistītas ar materiāla izpaušanu ārvalstu iestādēm, ir plašāk noteiktas prakses kodeksos: sk. jo īpaši Saziņas pārtveršanas prakses kodeksa 9.26. un turpmākos punktus, kā arī 9.87. punktu un Prakses kodeksa par iejaukšanos iekārtās 9.33. un turpmākos punktus, kā arī 9.41. punktu (sk. 278. zemsvītras piezīmi).

([312]) Šie mērķi ir: Drošības dienestam – smagu noziegumu novēršana vai atklāšana vai jebkādi kriminālprocesi (1989. gada Drošības dienestu likuma 2. panta 2. punkta a) apakšpunkts), izlūkdienestam – valsts drošības intereses, smagu noziegumu novēršana vai atklāšana vai jebkurš kriminālprocess (1994. gada Izlūkdienestu likuma 2. panta 2. punkta a) apakšpunkts) un *GCHQ* – jebkurš kriminālprocess (1994. gada Izlūkdienestu likuma 4. panta 2. punkta a) apakšpunkts). Sk. arī 2018. gada DAL paskaidrojuma rakstu, kas pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Termins "saziņas dati" aptver saziņas "kurš", "kad", "kur" un "kā", bet ne saturu, t. i., teikto vai rakstīto. Atšķirībā no pārtveršanas saziņas datu iegūšana un glabāšana ir vērsta nevis uz saziņas satura iegūšanu, bet gan uz tādas informācijas iegūšanu kā tālruņa pakalpojuma abonents vai detalizēts rēķins. Tas var ietvert saziņas laiku un ilgumu, nosūtītāja un saņēmēja numuru vai e-pasta adresi un dažreiz to ierīču atrašanās vietu, no kurām tika īstenoti telesakari ([313]).

(199) Būtu jāatzīmē, ka saziņas datu glabāšana un iegūšana parasti neattiecas uz ES datu subjektu personas datiem, kas saskaņā ar šo lēmumu nosūtīti uz Apvienoto Karalisti. Pienākums saglabāt vai izpaust saziņas datus saskaņā ar 2016. gada IPL 3. un 4. daļu attiecas uz datiem, kurus telesakaru operatori Apvienotajā Karalistē vāc tieši no telesakaru pakalpojumu lietotājiem ([314]). Šāda veida "uz klientu vērsta" apstrāde parasti nenozīmē nosūtīšanu, pamatojoties uz šo lēmumu, proti, nosūtīšanu no pārziņa/apstrādātāja ES pārzinim/apstrādātājam Apvienotajā Karalistē.

(200) Tomēr informācijas pilnīguma labad nosacījumi un garantijas, kas regulē šos iegūšanas un glabāšanas režīmus, ir analizēti turpmākajos apsvērumos.

(201) Kā priekšnoteikums jānorāda, ka saziņas datu glabāšana un mērķēta iegūšana ir pieejama gan valsts drošības dienestiem, gan noteiktām tiesībaizsardzības iestādēm ([315]). Nosacījumi, kas paredz saziņas datu glabāšanu un/vai iegūšanu, var atšķirties atkarībā no pasākuma pieprasīšanas pamatojuma, proti, valsts drošības vai tiesībaizsardzības mērķa.

(202) Konkrētāk, lai gan jaunais režīms ir ieviesis vispārējo prasību pēc *ex ante* atļaujas, ko piešķir neatkarīga struktūra un ko piemēro visos gadījumos, kad saziņas dati tiek glabāti un/vai iegūti (vai nu tiesībaizsardzības, vai valsts drošības nolūkā), pēc Eiropas Savienības Tiesas ([316]) sprieduma lietā *Tele2/Watson* ir ieviestas īpašas garantijas, ja pasākumu pieprasa tiesībaizsardzības nolūkā. Konkrētāk, ja saziņas datu glabāšanu vai iegūšanu pieprasa tiesībaizsardzības nolūkā, *ex ante* atļaujas piešķiršana vienmēr jāveic izmeklēšanas pilnvaru komisāram. Tā ne vienmēr notiek, ja pasākumu pieprasa valsts drošības nolūkā, jo, kā aprakstīts turpmāk, dažos gadījumos šāda veida pasākumiem atļauju var izsniegt cita persona, kura izsniedz atļauju. Turklāt jaunā režīma ietvaros slieksnis, attiecībā uz kuru saziņas datu glabāšana un iegūšana var tikt atļauta, ir paaugstināts uz "smagiem noziegumiem" ([317]).

([313]) Saziņas dati ir definēti 2016. gada IPL 261. panta 5. punktā. Saziņas dati tiek iedalīti "notikumu datos" (jebkuri dati, kas identificē vai apraksta notikumu, neatkarīgi no tā, vai tas attiecas uz tā atrašanās vietu, telesakaru sistēmā vai ar tās starpniecību, ja notikumu veido viena vai vairākas vienības, kas iesaistītas noteiktā darbībā noteiktā laikā) un "vienības datos" (jebkuri dati, kas a) attiecas uz i) vienību, ii) saistību starp telesakaru pakalpojumu un vienību vai iii) saistību starp jebkuru telesakaru sistēmu un vienību, b) pilnībā vai daļēji sastāv no datiem, kas identificē vai apraksta vienību (neatkarīgi no tā, vai atsaucoties uz vienības atrašanās vietu), un c) nav notikumu dati).

([314]) Tas izriet no saziņas datu definīcijas, kas sniegta 2016. gada IPL 261. panta 5. punktā, saskaņā ar kuru saziņas datus glabā vai iegūst telesakaru operators un tie vai nu attiecas uz telesakaru pakalpojuma lietotāju, vai uz šī pakalpojuma sniegšanu, vai ir ietverti, iekļauti kā daļa saziņā, pievienoti saziņai vai loģiski saistīti ar saziņu (sk. arī Saziņas datu prakses kodeksu, kas pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, 2.22.–2.33. punkts). Turklāt 2016. gada IPL 261. panta 10. punktā sniegtā telesakaru operatora definīcija paredz, ka telesakaru operators ir persona, kura piedāvā vai sniedz telesakaru pakalpojumus personām Apvienotajā Karalistē vai kura kontrolē vai nodrošina telesakaru sistēmu, kas ir (pilnībā vai daļēji) Apvienotajā Karalistē vai kontrolēta no Apvienotās Karalistes. Šīs definīcijas skaidri norāda, ka saistības atbilstīgi 2016. gada IPL nevar uzlikt telesakaru operatoriem, kuru aprīkojums neatrodas Apvienotajā Karalistē vai netiek kontrolēts no tās un kuri nepiedāvā vai nesniedz pakalpojumus personām Apvienotajā Karalistē (sk. arī Saziņas datu prakses kodeksa 2.1. punktu). Ja ES abonenti (neatkarīgi no tā, vai tie atrodas ES vai Apvienotajā Karalistē) izmanto pakalpojumus Apvienotajā Karalistē, jebkādu saziņu saistībā ar šī pakalpojuma sniegšanu tieši apkopotu pakalpojumu sniedzējs Apvienotajā Karalistē, nevis nosūtītu tos no ES.

([315]) Attiecīgās iestādes ir uzskaitītas 2016. gada IPL 4. pielikumā, un tajās ietilpst policijas vienības, izlūkdienesti, dažas ministrijas un valdības departamenti, Valsts noziedzības apkarošanas aģentūra, Viņas Majestātes ieņēmumu un muitas dienests, Konkurences un tirgu iestāde, informācijas komisārs, ātrā palīdzība, ugunsdzēsības un glābšanas dienesti, kā arī iestādes, piemēram, veselības un pārtikas drošuma jomā.

([316]) Apvienotās lietas C-203/15 un C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

([317]) Sk. 61. panta 7. punkta b) apakšpunktu attiecībā uz saziņas datu iegūšanu un 87. panta 10.A punktu attiecībā uz saziņas datu glabāšanu.

i) *Atļauja saziņas datu iegūšanai*

(203) Saskaņā ar 2016. gada IPL 3. daļu attiecīgās publiskās iestādes ir pilnvarotas iegūt saziņas datus no telesakaru operatora vai jebkuras citas personas, kura spēj iegūt un izpaust šādus datus. Atļauja var neattiekties uz saziņas satura ([318]) pārtveršanu, un tā zaudē spēku pēc viena mēneša ([319]) ar iespēju to atjaunot, izsniedzot papildu atļauju ([320]). Saziņas datu iegūšanai ir nepieciešama izmeklēšanas pilnvaru komisāra (IPK) atļauja ([321]) (informāciju par IPK statusu un pilnvarām sk. turpmāk 250.–251. apsvērumā). Tā tas ir vienmēr, ja saziņas datu iegūšanu pieprasa attiecīga tiesībaizsardzības iestāde. Tomēr atbilstīgi 2016. gada IPL 61. pantam tad, ja dati tiek iegūti Apvienotās Karalistes valsts drošības vai ekonomiskās labklājības interesēs, ciktāl tas ir svarīgi valsts drošībai, vai ja pieteikumu iesniedz izlūkošanas aģentūras loceklis saskaņā ar 61. panta 7. punkta b) apakšpunktu ([322]), iegūšanu alternatīvi ([323]) var atļaut IPK vai norīkots vecākais ierēdnis ([324]). Norīkotajam ierēdnim jābūt neatkarīgam attiecībā uz konkrēto izmeklēšanu vai operāciju un viņam jābūt praktiskām zināšanām par cilvēktiesību principiem un tiesību aktiem, jo īpaši attiecībā uz nepieciešamību un samērīgumu ([325]). Uz norīkotā ierēdņa pieņemto lēmumu attiecas IPK *ex post* pārraudzība (sīkāku informāciju par IPK *ex post* pārraudzības funkcijām sk. turpmāk 254. apsvērumā).

(204) Atļauja iegūt saziņas datus ir balstīta pasākuma nepieciešamības un samērīguma novērtējumā. Precīzāk, pasākuma nepieciešamība tiek vērtēta, ņemot vērā tiesību aktos uzskaitītos iemeslus ([326]). Ņemot vērā šī pasākuma mērķēto raksturu, tam jābūt nepieciešamam arī īpašai izmeklēšanai vai operācijai ([327]). Citas prasības pasākumu nepieciešamības novērtējumam ir noteiktas Saziņas datu prakses kodeksā ([328]). Šajā kodeksā jo īpaši paredzēts, ka pieprasījuma iesniedzējas iestādes iesniegtajā pieteikumā jānorāda trīs obligātie elementi šāda pieprasījuma nepieciešamības pamatojumam: i) izmeklējamais notikums, piemēram, noziegums vai neaizsargātās pazudušās personas atrašanās vieta; ii) persona, kuras dati nepieciešami, piemēram, aizdomās turamais, liecinieks vai pazudusi persona, un tas, kā viņi ir saistīti ar notikumu; un iii) nepieciešamie saziņas dati, piemēram, tālruņa numurs vai IP adrese, un tas, kā šie dati ir saistīti ar personu un notikumu ([329]).

(205) Turklāt saziņas datu ieguvei jābūt samērīgai ar sasniedzamo mērķi ([330]). Saziņas datu prakses kodeksā ir paskaidrots, ka, veicot šādu novērtējumu, personai, kura izsniedz atļauju, būtu jāveic līdzsvara pārbaude starp "personas tiesību un brīvību ierobežojuma apmēru un konkrēto ieguvumu izmeklēšanai vai operācijai, kuru veic attiecīgā publiskā iestāde sabiedrības interesēs" un ka, ņemot vērā visus konkrētā gadījuma apsvērumus "personas tiesību

([318]) 2016. gada IPL 60.A panta 6. punkts.

([319]) Šis periods tiek saīsināts līdz trim dienām, ja atļauju piešķir steidzamu iemeslu dēļ (2016. gada IPL 65. panta 3. punkta A daļa).

([320]) Saskaņā ar 2016. gada IPL 65. pantu atjaunotā atļauja būs derīga vienu mēnesi no esošās atļaujas darbības termiņa beigām. Persona, kura piešķīrusi atļauju, var jebkurā laikā atsaukt atļauju, ja tā uzskata, ka prasības vairs netiek izpildītas.

([321]) 2016. gada IPL 60.A panta 1. punkts. Saziņas datu iegūšanas atļauju birojs (*OCDA*) veic šo funkciju IPK vārdā (sk. Saziņas datu prakses kodeksa 5.6. punktu).

([322]) Pieteikums saskaņā ar 2016. gada IPL 61. panta 7. punkta b) apakšpunktu tiek iesniegts "atbilstošam noziedzības apkarošanas nolūkam", un tas nozīmē – saskaņā ar 2016. gada IPL 61. panta 7. punkta A daļu: "Ja saziņas dati pilnībā vai daļēji ir notikumu dati, smagu noziegumu novēršanas vai atklāšanas nolūks; jebkurā citā gadījumā nolūks ir novērst vai atklāt noziegumus vai novērst nekārtības".

([323]) Saziņas datu prakses kodeksā ir noteikts: "ja pieteikumu, kas attiecas uz valsts drošību, var iesniegt vai nu saskaņā ar 60.A, vai 61. pantu, lēmumu par to, kurš atļaujas piešķiršanas ceļš ir vispiemērotākais jebkurā gadījumā, pieņem atsevišķas publiskās iestādes. Publiskajām iestādēm, kuras vēlas, lai atļauju piešķirtu norīkots vecākais ierēdnis, būtu jāievieš skaidras pamatnostādnes par to, kad šis atļaujas izsniegšanas ceļš ir piemērots" (Saziņas datu prakses kodeksa 5.19. punkts, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) 2016. gada IPL 70. panta 3. punktā sniegta "norīkotā ierēdņa" definīcija, kas mainās atkarībā no attiecīgās publiskās iestādes (kā noteikts 2016. gada IPL 4. pielikumā).

([325]) Plašāka informācija par norīkotā vecākā ierēdņa neatkarību ir sniegta Saziņas datu prakses kodeksā (Saziņas datu prakses kodekss, 4.12.–4.17. punkts, sk. 323. zemsvītras piezīmi).

([326]) Iemesli ir šādi: i) valsts drošība; ii) noziedzības novēršana vai atklāšana vai nekārtību novēršana ("notikumu datu" gadījumā – tikai smagu noziegumu); iii) Apvienotās Karalistes ekonomiskās labklājības intereses, ciktāl šīs intereses attiecas arī uz valsts drošības interesēm; iv) sabiedriskās drošības interesēs; v) lai novērstu nāvi vai traumas vai jebkādu kaitējumu personas fiziskajai vai garīgajai veselībai vai lai mazinātu traumu vai kaitējumu personas fiziskajai vai garīgajai veselībai; vi) lai palīdzētu izmeklēt iespējamas tiesu kļūdas vai vii) lai identificētu mirušu personu vai personu, kas noteikta stāvokļa dēļ nespēj sevi identificēt (2016. gada IPL 61. panta 7. punkts).

([327]) 2016. gada IPL 60.A panta 1. punkta b) apakšpunkts.

([328]) Saziņas datu prakses kodekss, 3.3. un turpmākie punkti, sk. 323. zemsvītras piezīmi.

([329]) Saziņas datu prakses kodekss, 3.13. punkts, sk. 323. zemsvītras piezīmi.

([330]) 2016. gada IPL 60. panta 1. punkta c) apakšpunkts.

ierobežojums joprojām nevar būt attaisnojams, jo negatīvā ietekme uz citas personas vai personu grupas tiesībām ir pārāk nopietna". Turklāt, lai īpaši novērtētu pasākuma samērīgumu, kodeksā ir uzskaitīti vairāki elementi, kas būtu jāiekļauj pieprasījuma iesniedzējas iestādes iesniegtajā pieteikumā ([331]). Turklāt īpaša uzmanība jāpievērš iegūstamo saziņas datu veidam ("vienības" vai "notikumu" dati ([332])), un priekšroka dodama mazāk traucējošas kategorijas datu izmantošanai ([333]). Saziņas datu prakses kodeksā ir arī īpašas instrukcijas atļaujām, kas saistītas ar konkrētu profesiju personu (piemēram, ārstu, juristu, žurnālistu, parlamentāriešu vai mācītāju) ([334]) saziņas datiem, uz kuriem attiecas papildu garantijas ([335]).

ii) *Paziņojums, ar ko pieprasa saziņas datu glabāšanu*

(206) 2016. gada IPL 4. daļā ir izklāstīti saziņas datu glabāšanas noteikumi un jo īpaši kritēriji, kas ļauj ministram izdot paziņojumu par datu glabāšanu ([336]). IPL ieviestās garantijas ir tādas pašas kā tad, kad dati tiek glabāti vai nu tiesībaizsardzības nolūkā, vai valsts drošības interesēs.

(207) Šādu paziņojumu par datu glabāšanu mērķis ir nodrošināt, lai telesakaru operatori ne ilgāk kā 12 mēnešus glabātu attiecīgos saziņas datus, kuri citādi tiktu izdzēsti, ja tie vairs nebūtu nepieciešami uzņēmējdarbības vajadzībām ([337]). Glabātajiem datiem ir jābūt pieejamiem prasītajā laika posmā, ja publiskajai iestādei vēlāk būtu nepieciešamība tos iegūt, pamatojoties ar atļauju mērķētai saziņas datu iegūšanai, kas paredzēta 2016. gada IPL 3. daļā un aprakstīta 203.–205. apsvērumā.

(208) Tādas pilnvaras izmantošanai, kas ietver prasību par konkrētu datu glabāšanu, ir noteikti vairāki ierobežojumi un garantijas. Ministrs var izsniegt paziņojumu par datu glabāšanu vienam vai vairākiem operatoriem ([338]) tikai tad, ja viņš uzskata, ka prasība saglabāt datus ir nepieciešama kādam no likumā noteiktajiem mērķiem ([339]) un ir samērīga ar sasniedzamo mērķi ([340]). Kā

([331]) Iekļaujamajā informācijā jāietver: i) izklāsts par to, kādu ieguvumu datu iegūšana sniegs izmeklēšanai vai operācijai; ii) paskaidrojums par pieprasīto laika periodu atbilstību, tostarp to, kā šie periodi ir samērojami ar izmeklējamo notikumu; iii) paskaidrojums par to, kāpēc aizskāruma līmenis ir pamatots, ņemot vērā ieguvumu, ko dati sniegs izmeklēšanai (šajā pamatojumā būtu jāiekļauj apsvērums par to, vai mērķa sasniegšanai varētu veikt mazāk traucējošas izmeklēšanas darbības); iv) personas tiesību (jo īpaši uz privātumu un attiecīgā gadījumā vārda brīvību) apsvērums un šo tiesību līdzsvarošana ar izmeklēšanas ieguvumiem; v) sīka informācija par to, kāds netiešs aizskārums var rasties un kā pieprasītie laika periodi ietekmē netiešo aizskārumu (Saziņas datu prakses kodeksa 3.22.–3.26. punkts, sk. 323. zemsvītras piezīmi).

([332]) Sk. 313. zemsvītras piezīmi.

([333]) Ja pieprasījums skar traucējošākus saziņas datus (proti, notikumu datus), kodeksā ir noteikts, ka ir lietderīgāk vispirms iegūt vienības datus vai notikumu datus iegūt tieši ierobežotos un īpaši steidzamos gadījumos (Saziņas datu prakses kodekss, 6.10.–6.14. punkts, sk. 323. zemsvītras piezīmi).

([334]) Saziņas datu prakses kodekss, 8.8.–8.44. punkts, sk. 323. zemsvītras piezīmi.

([335]) Prakses kodekss nosaka, ka "personai, kura izsniedz atļauju, jāpiemēro īpaša rūpība, izskatot šādus pieteikumus, tostarp papildu apsvērumus par to, vai šādiem pieteikumiem varētu būt neparedzētas sekas un vai izmantojums vislabāk atbilst sabiedrības interesēm" (Saziņas datu prakses kodekss, 8.8. punkts). Turklāt šāda veida pieteikumi ir jāreģistrē, un nākamajā pārbaudē šādus pieteikumus atzīmē IPK uzmanībai (Saziņas datu prakses kodeksa 8.10. punkts, sk. 323. zemsvītras piezīmi).

([336]) 2016. gada IPL 87.–89. pants.

([337]) Saskaņā ar 2016. gada IPL 90. pantu telesakaru operators, kuram tiek sniegts paziņojums par datu saglabāšanu, var lūgt to pārskatīt ministram, kurš atļauju izsniedzis.

([338]) Saskaņā ar 2016. gada IPL 87. panta 2. punkta a) apakšpunktu paziņojums par datu glabāšanu var attiekties uz konkrētu operatoru vai jebkādu operatoru aprakstu.

([339]) Mērķi ir i) valsts drošības intereses; ii) atbilstošais noziedzības apkarošanas nolūks (kā noteikts 2016. gada IPL 87. panta 10.A punktā); iii) Apvienotās Karalistes ekonomiskās labklājības intereses, ciktāl šīs intereses attiecas arī uz valsts drošības interesēm; iv) sabiedriskās drošības intereses; v) lai novērstu nāvi vai traumas vai jebkādu kaitējumu personas fiziskajai vai garīgajai veselībai vai lai mazinātu traumu vai kaitējumu personas fiziskajai vai garīgajai veselībai; vai vi) lai palīdzētu izmeklēt iespējamās tiesas kļūdas (IPL 87. pants).

([340]) 2016. gada IPL 87. pants. Turklāt saskaņā ar attiecīgo prakses kodeksu, lai novērtētu paziņojuma par datu glabāšanu samērīgumu, piemēro 2016. gada IPL 2. panta 2. punktā noteiktos kritērijus, jo īpaši prasību novērtēt, vai ar paziņojumu sasniedzamo mērķi pamatoti varētu sasniegt ar mazāk traucējošiem līdzekļiem. Līdzīgi saziņas datu iegūšanas samērīguma novērtējumam Saziņas datu prakses kodeksā ir paskaidrots, ka šāds novērtējums ietver "līdzsvaru starp personas tiesību uz privāto dzīvi ierobežošanas apmēru un konkrētu ieguvumu izmeklēšanai (Saziņas datu prakses kodekss, 16.3. punkts, sk. 323. zemsvītras piezīmi).

paskaidrots 2016. gada IPL ([341]), ministram pirms paziņojuma par datu glabāšanu izdošanas ir jāņem vērā: paziņojuma iespējamie ieguvumi ([342]); telesakaru pakalpojumu apraksts; glabājamo datu ierobežošanas piemērotība, atsaucoties uz atrašanās vietu vai to personu aprakstu, kurām tiek sniegti telesakaru pakalpojumi ([343]); iespējamais jebkura telesakaru pakalpojuma lietotāju skaits (ja zināms), uz kuru attiecas paziņojums ([344]); paziņojuma izpildes tehniskā iespējamība; iespējamās paziņojuma izpildes izmaksas un jebkura cita paziņojuma ietekme uz telesakaru operatoru (vai operatoru aprakstu), uz kuru tas attiecas ([345]). Kā sīkāk aprakstīts Saziņas datu prakses kodeksa 17. nodaļā, visos paziņojumos par datu glabāšanu ir jānorāda katrs datu veids, kurš jāglabā, un tas, kā šis datu veids atbilst nepieciešamajām glabāšanas pārbaudēm.

(209) Visos gadījumos (gan valsts drošības, gan tiesībaizsardzības mērķiem) ministra lēmums izdot paziņojumu par datu glabāšanu saskaņā ar tā dēvēto "divkāršās drošības procedūru" jāapstiprina neatkarīgam tieslietu komisāram, kuram īpaši jāpārskata, vai paziņojums par attiecīgu saziņas datu glabāšanu ir nepieciešams un samērīgs viena vai vairāku likumā noteikto mērķu sasniegšanai ([346]).

3.3.1.1.3. Iejaukšanās iekārtās

(210) Iejaukšanās iekārtās ir metožu kopums, ko izmanto, lai iegūtu dažādus datus no iekārtām ([347]), tostarp datoriem, planšetdatoriem un viedtālruņiem, kā arī kabeļiem, vadiem un atmiņas ierīcēm ([348]). Iejaukšanās iekārtās ļauj iegūt gan saziņas saturu, gan iekārtu datus ([349]).

(211) Saskaņā ar 2016. gada IPL 13. panta 1. punktu izlūkdienestam, lai veiktu iejaukšanos iekārtās, ir nepieciešama atļauja, pamatojoties uz orderi, atbilstīgi "divkāršās drošības" procedūrai, kas noteikta 2016. gada IPL, ar nosacījumu, ka pastāv "saikne ar Britu salām" ([350]). Saskaņā ar Apvienotās Karalistes iestāžu sniegtajiem

([341]) Sk. 2016. gada IPL 88. pantu.

([342]) Ieguvumi var būt esoši vai gaidāmi, un tiem jāatbilst likumā paredzētajiem nolūkiem, kādiem datus drīkst glabāt (Saziņas datu prakses kodeksa 17.17. punkts, sk. 323. zemsvītras piezīmi).

([343]) Šie apsvērumi ietver konstatējumu, vai paziņojuma par datu glabāšanu pilnīga ģeogrāfiskā aptvere ir nepieciešama un samērīga un vai ir nepieciešami un samērīgi iekļaut vai izslēgt kādus konkrētus personu aprakstus (Saziņas datu prakses kodeksa 17.17. punkts, sk. 323. zemsvītras piezīmi).

([344]) Tas palīdzēs ministram apsvērt gan aizskāruma līmeni klientiem, gan arī glabājamo datu sniegtos iespējamos ieguvumus (Saziņas datu prakses kodeksa 17.17. punkts, sk. 323. zemsvītras piezīmi).

([345]) 2016. gada IPL 88. pants.

([346]) 2016. gada IPL 89. pants.

([347]) Saskaņā ar 2016. gada IPL 135. panta 1. punktu un 198. panta 1. punktu "iekārta" ietver iekārtas, kas rada elektromagnētisku, akustisku vai citu izstarojumu, un jebkuras ierīces, kuras var izmantot saistībā ar šādām iekārtām.

([348]) Prakses kodekss par iejaukšanos iekārtās, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, 2.2. punkts.

([349]) Iekārtu dati 2016. gada IPL 100. pantā ir definēti kā sistēmas dati un dati, kuri a) ietverti, iekļauti kā daļa saziņā, pievienoti saziņai vai loģiski saistīti ar saziņu (gan nosūtītāja, gan citādi) vai jebkuru citu informācijas vienību; b) loģiski nošķirami no pārējās saziņas vai informācijas vienības un c) ja tie būtu nošķirti, neizpaustu neko no tā, ko pamatoti varētu uzskatīt par saziņas nozīmi (ja tāda ir) vai informācijas vienību.

([350]) Lai prasība saņemt orderi būtu obligāta, 2016. gada IPL 13. panta 1. punktā arī noteikts, ka izlūkdienesta darbība būtu viens vai vairāki pārkāpumi saskaņā ar 1990. gada Likuma par datoru ļaunprātīgu izmantošanu 1.–3.A pantu, kas būtu lielākajā daļā apstākļu, sk. Prakses kodeksu par iejaukšanos iekārtās, 3.32. un 3.6.–3.9. punkts). Saskaņā ar 2016. gada IPL 13. panta 2. punktu "saikne ar Britu salām" pastāv šādos gadījumos: a) kāda no rīcībām notiktu Britu salās (neatkarīgi no tā, kur atrodas iekārta, kurā tiktu vai varētu tikt veikta iejaukšanās), b) izlūkdienests uzskata, ka jebkura iekārta, kurā tiktu vai varētu tikt veikta iejaukšanās, kādā brīdī, kamēr notiek iejaukšanās, būtu vai varētu atrasties Britu salās, vai c) iejaukšanās mērķis ir iegūt i) saziņu, ko nosūta persona vai personai, kura pagaidām atrodas vai izlūkdienesta ieskatā atrodas Britu salās, ii) privātu informāciju par personu, kura pagaidām atrodas vai izlūkdienesta ieskatā atrodas Britu salās, vai iii) iekārtu datus, kas ir daļa no i) vai ii) apakšpunktā minētās saziņas vai privātās informācijas vai ir saistīti ar to.

paskaidrojumiem situācijās, kad dati no Eiropas Savienības tiek nosūtīti uz Apvienoto Karalisti šī lēmuma piemērošanas jomas ietvaros, vienmēr pastāv "saikne ar Britu salām", un tādēļ uz jebkādu iejaukšanos iekārtās, kas aptver šādus datus, attiecas 2016. gada IPL 13. panta 1. punkta obligātā prasība saņemt orderi ([351]).

(212) Noteikumi par mērķētas iejaukšanās iekārtās orderiem ir izklāstīti 2016. gada IPL 5. daļā. Tāpat kā mērķēta pārtveršana, arī mērķēta iejaukšanās iekārtās attiecas uz konkrētu "mērķi", kurš jāizklāsta orderī ([352]). Sīkāka informācija par to, kā jāidentificē "mērķis", ir atkarīga no jautājuma un tās iekārtas veida, kurā paredzēta iejaukšanās. Jo īpaši IPL 115. panta 3. punktā ir norādīti elementi, kas jāiekļauj orderī (piemēram, personas vai organizācijas vārds/nosaukums, atrašanās vietas apraksts), piemēram, atkarībā no tā, vai iejaukšanās attiecas uz iekārtu, kura pieder konkrētai personai vai organizācijai vai personu grupai vai kuru tās izmanto, vai kura atrodas to valdījumā, kura atrodas noteiktā vietā utt. ([353]). Mērķi, kādiem var izsniegt mērķētas iejaukšanās iekārtās orderi, ir atkarīgi no publiskās iestādes, kas to pieprasa ([354]).

(213) Līdzīgi kā mērķētas pārtveršanas gadījumā, izdevējiestādei ir jāapsver, vai pasākums ir nepieciešams konkrēta nolūka sasniegšanai un vai tas ir samērīgs ar sasniedzamo mērķi ([355]). Turklāt tai vajadzētu arī apsvērt, vai pastāv garantijas attiecībā uz drošību, glabāšanu un izpaušanu, kā arī attiecībā uz informācijas izpaušanu ārvalstīs ([356]) (sk. 196. apsvērumu).

(214) Orderis jāapstiprina tieslietu komisāram, izņemot steidzamus gadījumus ([357]). Pēdējā gadījumā tieslietu komisārs ir jāinformē, ka orderis ir izdots, un tas jāapstiprina trīs darba dienu laikā. Gadījumā, ja tieslietu komisārs atsakās to apstiprināt, orderis vairs nav spēkā, un to nav iespējams atjaunot ([358]). Turklāt tieslietu komisāram ir pilnvaras pieprasīt tādu datu dzēšanu, kas iegūti saskaņā ar orderi ([359]). Tas, ka orderis izdots steidzamā kārtā, neietekmē nedz *ex post* pārraudzību (sk. 244.–255. apsvērumu), nedz personu iespējas pieprasīt kompensāciju (sk. 260.–270. apsvērumu). Personas var sūdzēties IKB vai iesniegt prasību par apgalvoto rīcību Izmeklēšanas pilnvaru tribunālam parastajā veidā. Visos gadījumos tieslietu komisāra pārbaude, kas tiek piemērota, lemjot par ordera apstiprināšanu, ir nepieciešamības un samērīguma pārbaude, kas piemērojama mērķētas pārtveršanas pieprasījumiem ([360]) (sk. iepriekš 192. apsvērumu).

([351]) Informācijas pilnības labad jāatzīmē, ka pat situācijās, kad nepastāv "saikne ar Britu salām" un tāpēc uz iejaukšanos iekārtās neattiecas ordera saņemšanas obligātā prasība, kas noteikta 2016. gada IPL 13. panta 1. punktā, izlūkdienestam, plānojot iesaistīties darbībās, attiecībā uz kurām tas var iegūt masveida iejaukšanās iekārtās orderi, šāds orderis būtu jāsaņem, balstoties uz politiku (sk. Prakses kodeksu par iejaukšanos iekārtās, 3.24. punkts). Pat ja iejaukšanās iekārtās orderis saskaņā ar 2016. gada IPL nav juridiski obligāts un tas nav saņemts, balstoties uz politiku, uz izlūkdienestu darbībām attiecas vairāki nosacījumi un ierobežojumi saskaņā ar 1994. gada Izlūkdienestu likuma 7. pantu. Tas jo īpaši ietver prasību saņemt atļauju no ministra, kuram jābūt pārliecinātam, ka jebkura darbība nepārsniedz to, kas nepieciešams pareizai izlūkdienesta funkciju izpildei.

([352]) 2016. gada IPL 115. pants reglamentē ordera saturu, norādot, ka tajā jāiekļauj personu, organizāciju, atrašanās vietu vai personu grupas, kas veido "mērķi", vārds/nosaukums vai apraksts, izmeklēšanas rakstura apraksts un to darbību apraksts, kurām iekārta tiek izmantota. Tajā jāapraksta arī iekārtas veids un rīcība, kādu personai, kurai adresēts orderis, ir atļauts veikt.

([353]) Sk. Prakses kodeksu par iejaukšanos iekārtās, 5.7. punkts, sk. 348. zemsvītras piezīmi.

([354]) Valsts drošības dienesti var lūgt izdot iejaukšanās iekārtās orderi, ja tas nepieciešams valsts drošības nolūkos, lai atklātu smagus noziegumus un/vai Apvienotās Karalistes ekonomiskās labklājības interesēs, ciktāl šīs intereses attiecas arī uz valsts drošības interesēm (2016. gada IPL 102.–103. pants). Atkarībā no dienesta var pieprasīt iejaukšanās iekārtās orderi tiesībaizsardzības nolūkos, ja tas nepieciešams smaga nozieguma atklāšanai vai novēršanai vai nāves, traumu vai personas fiziskās vai garīgās veselības kaitējuma novēršanai vai jebkuras traumas vai kaitējuma personas fiziskajai vai garīgajai veselībai seku mazināšanai (sk. 2016. gada IPL 106. panta 1. un 3. punktu).

([355]) 2016. gada IPL 102. panta 1. punkts.

([356]) 2016. gada IPL 129.–131. pants.

([357]) 2016. gada IPL 109. pants.

([358]) 2016. gada IPL 109. panta 4. punkts.

([359]) 2016. gada IPL 110. panta 3. punkta b) apakšpunkts. Saskaņā ar Prakses kodeksa par iejaukšanos iekārtās 5.67. punktu steidzamību nosaka saskaņā ar to, vai būtu praktiski iespējams lūgt tieslietu komisāra apstiprinājumu ordera izdošanai laikā, kas ir pieejams, lai apmierinātu operatīvu vai izmeklēšanas vajadzību. Steidzamiem orderiem būtu jāietilpst vienā vai abās šādās kategorijās: i) nenovēršams apdraudējums dzīvībai vai nopietns kaitējums – piemēram, ja persona ir nolaupīta un ir novērtēts, ka tās dzīvība ir nenovēršami apdraudēta; vai ii) izlūkdatu vākšanas vai izmeklēšanas iespēja ar ierobežotu rīcības laiku – piemēram, Apvienotajā Karalistē tūlīt nonāks A klases narkotiku sūtījums un tiesībaizsardzības iestādes vēlas, lai arestu veikšanas nolūkā būtu pieejama informācija par smagā nozieguma izdarītājiem. Sk. 348. zemsvītras piezīmi.

([360]) 2016. gada IPL 108. pants.

(215) Visbeidzot, īpašas garantijas, kas piemērojamas mērķētas pārtveršanas gadījumā, attiecas arī uz iejaukšanos iekārtās attiecībā uz ordera darbības ilgumu, tā atjaunošanu un grozīšanu, kā arī uz parlamenta deputātu, advokāta un klienta saziņas konfidencialitātei pakļautu priekšmetu un žurnālistikas materiāla pārtveršanu (sīkāku informāciju sk. 193. apsvērumā).

3.3.1.1.4. Masveida pilnvaru īstenošana

(216) Masveida pilnvaras ir reglamentētas 2016. gada IPL 6. daļā. Turklāt prakses kodeksos ir paredzēta sīkāka informācija par masveida pilnvaru izmantojumu. Lai gan Apvienotās Karalistes tiesību aktos nav definētas "masveida pilnvaras", 2016. gada IPL kontekstā tās aprakstītas kā liela tādu datu daudzuma vākšana un glabāšana, kurus valdība ieguvusi ar dažādiem līdzekļiem (proti, masveida pārtveršanas pilnvaras, masveida iegūšana, masveida iejaukšanās iekārtās un masveida personas datu kopas) un kuriem pēc tam iestādes var piekļūt. Šis apraksts tiek precizēts, salīdzinot to ar to, kas nav "masveida pilnvaras": tās nav pielīdzināmas tā sauktajai "masveida novērošanai" bez ierobežojumiem vai garantijām. Gluži pretēji, kā paskaidrots turpmāk, tajā ir iekļauti ierobežojumi un garantijas, kas paredzēti, lai nodrošinātu, ka piekļuve datiem netiek piešķirta nediferencēti vai nepamatoti ([361]). Masveida pilnvaras var izmantot tikai tad, ja ir konstatēta saikne starp tehnisko pasākumu, kuru valsts izlūkošanas aģentūra plāno izmantot, un operatīvo mērķi, kuram šāds pasākums ir pieprasīts.

(217) Turklāt masveida pilnvaras ir pieejamas tikai izlūkošanas aģentūrām, un uz tām vienmēr attiecas ministra izdots un tieslietu komisāra apstiprināts orderis. Izvēloties izlūkdatu vākšanas līdzekļus, jāapsver, vai attiecīgo mērķi var sasniegt ar "mazāk traucējošiem līdzekļiem" ([362]). Šī pieeja izriet no tiesību aktu ietvara, kas balstīts samērīguma principā, un tāpēc prioritāte ir mērķēta vākšana, nevis masveida vākšana.

3.3.1.1.4.1. Masveida pārtveršana un masveida iejaukšanās iekārtās

(218) Masveida pārtveršanas režīms ir paredzēts 2016. gada IPL 6. daļas 1. nodaļā, savukārt tās pašas daļas 3. nodaļa regulē masveida iejaukšanos iekārtās. Šie režīmi būtībā ir vienādi, tāpēc nosacījumi un papildu garantijas, kas piemērojami šiem orderiem, analizēti kopā.

i) *Nosacījumi un kritēriji ordera izdošanai*

(219) Masveida pārtveršanas orderis attiecināms uz tādas saziņas pārtveršanu tās nosūtīšanas laikā, ko sūta vai saņem personas, kuras atrodas ārpus Britu salām ([363]), tā sauktā "ar ārvalstīm saistītā saziņa" ([364]), kā arī citiem

([361]) Saskaņā ar ziņojumu par masveida pilnvarām, ko pirms 2016. gada IPL apstiprināšanas iesniedza terorisma apkarošanas tiesību aktu neatkarīgais pārskatītājs Lords Deivids Andersons, *"jābūt skaidram, ka masveida datu vākšana un glabāšana nav pielīdzināma tā sauktajai "masveida novērošanai". Jebkurā tiesību sistēmā, kas ir šī nosaukuma cienīga, būs iekļauti ierobežojumi un garantijas, kas precīzi izstrādāti, lai piekļuve sensitīvu datu krātuvēm (..) netiktu piešķirta nediferencēti vai nepamatoti. Šādi ierobežojumi un garantijas likumprojektā noteikti pastāv.* Lords Deivids Andersons, 2016. gada augusta pārskata ziņojums par masveida pilnvarām, 1.9. punkts (izcēlums pievienots), pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

([362]) 2016. gada IPL 2. panta 2. punkts. Sk., piemēram, Saziņas datu masveida iegūšanas prakses kodeksa 4.11. punktu, kas pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

([363]) "Britu salas" ietver Apvienoto Karalisti, Normandijas salas un Menas salu, un tās ir definētas 1978. gada Interpretācijas likuma 1. pielikumā, kas pieejams vietnē https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Saskaņā ar 2016. gada IPL 136. pantu "ar ārvalstīm saistīta saziņa" nozīmē: i) saziņu, ko sūtījušas personas, kuras atrodas ārpus Britu salām, vai ii) saziņu, ko saņēmušas personas, kuras atrodas ārpus Britu salām. Šis režīms, kā to apstiprināja Apvienotās Karalistes iestādes, attiecas arī uz saziņu starp divām personām, kuras abas atrodas ārpus Britu salām. Eiropas Cilvēktiesību tiesas virspalāta sprieduma par lietu *Big Brother Watch and others v United Kingdom* (sk. iepriekš 279. zemsvītras piezīmi) 376. punktā konstatēja, ka attiecībā uz tādas saziņas (ārējās saziņas) līdzīgu ierobežošanu, ko var iegūt ar masveida pārtveršanu saskaņā ar 2000. gada IPRL, tas ir pietiekami norobežots un paredzams.

būtiskiem datiem un pārtvertā materiāla turpmākai atlasei pārbaudei ([365]). Masveida iejaukšanās iekārtās orderis ([366]) pilnvaro adresātu nodrošināt iejaukšanos jebkurā iekārtā, lai iegūtu ar ārvalstīm saistītu saziņu (tostarp jebko, kas ietver runu, mūziku, skaņas, vizuālos attēlus vai jebkura apraksta datus), iekārtu datus (datus, kas nodrošina vai atvieglo pasta dienesta darbību; telesakaru sistēmu; telesakaru pakalpojumus) vai jebkuru citu informāciju ([367]).

(220) Ministrs masveida pilnvaru orderi var izdot tikai pēc izlūkdienesta vadītāja iesniegta pieteikuma ([368]). Orderis, kas atļauj masveida pārtveršanu vai masveida iejaukšanos iekārtās, jāizdod tikai tad, ja tas nepieciešams valsts drošības interesēs un turpmākiem nolūkiem novērst vai atklāt smagu noziegumu vai attiecīgā gadījumā Apvienotās Karalistes ekonomiskās labklājības interesēs, ciktāl tās skar valsts drošību ([369]). Turklāt 2016. gada IPL 142. panta 7. punktā noteikts, ka masveida pārtveršanas orderis ir jāprecizē sīkāk nekā, vienkārši atsaucoties uz "valsts drošības interesēm", "Apvienotās Karalistes ekonomisko labklājību" un "smagu noziegumu novēršanu un apkarošanu", taču ir jānosaka saikne starp vēlamo pasākumu un vienu vai vairākiem operatīvajiem nolūkiem, kas iekļaujami orderī.

(221) Operatīvā nolūka izvēle ir daudzpakāpju procesa rezultāts. 142. panta 4. punkts paredz, ka orderī norādītie operatīvie nolūki ir jānorāda izlūkdienestu vadītāju uzturētajā sarakstā kā nolūki, kas, viņuprāt, uzskatāmi par operatīviem nolūkiem, kuru dēļ pārtverto saturu vai sekundāros datus, kas iegūti ar masveida pārtveršanas orderi, drīkst atlasīt pārbaudei. Operatīvo nolūku sarakstu apstiprina ministrs. Ministrs šādu apstiprinājumu var dot tikai tad, ja ir pārliecināts, ka operatīvais nolūks ir precizēts sīkāk nekā vispārīgs pamatojums ordera izsniegšanai (valsts drošība vai valsts drošība un ekonomiskā labklājība vai smagu noziegumu novēršana) ([370]). Katra attiecīgā trīs mēnešu perioda beigās ministram ir jānodod parlamenta IDK operatīvo nolūku saraksta kopija. Visbeidzot, premjerministram vismaz reizi gadā jāpārskata operatīvo nolūku saraksts ([371]). Kā atzīmēja Augstā tiesa, "to nozīmi nedrīkst mazināt līdz nenozīmīgām garantijām, jo tie kopā veido sarežģītu pārskatatbildības režīmu kopumu, kurā iesaistīts gan parlaments, gan augstākā līmeņa valdības locekļi" ([372]).

(222) Šādi operatīvie nolūki ierobežo arī pārtveršanas materiāla atlases apjomu pārbaudes posmam. Saskaņā ar masveida pilnvaru orderi jebkāda savāktā materiāla atlase pārbaudei jāpamato, ņemot vērā operatīvo(-os) nolūku(-us). Kā paskaidroja Apvienotās Karalistes iestādes, tas nozīmē, ka praktiski pārbaudes kārtība ministram jānovērtē jau ordera stadijā, sniedzot pietiekamu informāciju, lai izpildītu likumā noteiktos pienākumus atbilstīgi 2016. gada IPL 152. un 193. pantam ([373]). Ministram sniegtajā informācijā par šiem pasākumiem jāiekļauj, piemēram, informācija (attiecīgā gadījumā) par to, kā filtrēšanas kārtība var mainīties laikā, kamēr orderis būs spēkā ([374]). Sīkāku informāciju par procesu un garantijām, ko piemēro filtrēšanas un pārbaudes posmiem, sk. turpmāk 229. apsvērumā.

([365]) 2016. gada IPL 136. panta 4. punkts. Saskaņā ar paskaidrojumiem, kas saņemti no Apvienotās Karalistes valdības, masveida pārtveršanu var izmantot, piemēram, lai identificētu iepriekš nezināmus draudus Apvienotās Karalistes valsts drošībai, filtrējot un analizējot pārtverto materiālu, lai identificētu saziņu, kas var būt vērtīga izlūkošanas vajadzībām (Apvienotās Karalistes paskaidrojuma dokumenta H iedaļa "Valsts drošība", 27.–28. lpp., sk. 29. zemsvītras piezīmi). Kā paskaidrojušas Apvienotās Karalistes iestādes, šādus instrumentus var izmantot, lai izveidotu saikni starp zināmiem interesējošiem subjektiem, kā arī lai meklētu darbības pēdas personām, kuras varbūt vēl nav zināmas, bet kuras atklājas izmeklēšanas gaitā, un lai identificētu darbības modeļus, kas var norādīt uz draudiem Apvienotajai Karalistei.

([366]) Saskaņā ar 2016. gada IPL 13. panta 1. punktu izlūkdienestam, lai veiktu iejaukšanos iekārtās, ir nepieciešama atļauja, pamatojoties uz orderi, atbilstīgi 2016. gada IPL, ar nosacījumu, ka pastāv "saikne ar Britu salām", sk. 211. apsvērumu.

([367]) 2016. gada IPL 176. pants. Ar masveida iejaukšanās iekārtās orderi nevar atļaut rīcību, kas (ja vien tas nenotiek ar likumīgu pilnvarojumu) būtu nelikumīga pārtveršana (izņemot attiecībā uz glabāto saziņu). Saskaņā ar Apvienotās Karalistes paskaidrojuma dokumentu iegūtā informācija var būt nepieciešama, lai identificētu interesējošus subjektus, un parasti tā būtu piemērota liela mēroga operācijām (Apvienotās Karalistes paskaidrojuma dokumenta H iedaļa "Valsts drošība", 28. lpp., sk. 29. zemsvītras piezīmi).

([368]) 2016. gada IPL 138. panta 1. punkts un 178. panta 1. punkts.

([369]) 2016. gada IPL 138. panta 2. punkts un 178. panta 2. punkts.

([370]) Saskaņā ar Apvienotās Karalistes iestāžu sniegtajiem paskaidrojumiem, piemēram, operatīvais nolūks var ierobežot pasākuma piemērošanas jomu līdz draudu pastāvēšanai noteiktā ģeogrāfiskā apgabalā.

([371]) 2016. gada IPL 142. panta 4.–10. punkts.

([372]) Augstā tiesa, *Liberty*, [2019], EWHC 2057 (Admin), 167. punkts.

([373]) 2016. gada IPL 152. un 193. pants paredz, ka: a) atlase pārbaudei tiek veikta tikai orderī norādītajiem operatīvajiem nolūkiem, b) atlase pārbaudei ir nepieciešama un samērīga jebkuros apstākļos, un c) atlase pārbaudei nav pretrunā ar aizliegumu veikt pārbaudi, atlasot materiālu un identificējot saziņu, kuru ir sūtījušas personas vai kura ir paredzēta personām, par kurām ir zināms, ka tajā laikā tās atradās Britu salās.

([374]) Sk. Saziņas pārtveršanas prakses kodeksu, 6.6. punkts, sk. 278. zemsvītras piezīmi.

(223) Masveida pilnvaras var atļaut tikai tad, ja tās ir samērīgas ar sasniedzamo mērķi ([375]). Kā noteikts Pārtveršanas prakses kodeksā, jebkurš samērīguma novērtējums ietver "privātuma aizskāruma smaguma līdzsvarošanu (un citus 2. panta 2. punktā izklāstītos apsvērumus) ar nepieciešamību veikt darbību izmeklēšanas, operatīvajām vai spēju vajadzībām. Atļautajai rīcībai būtu jāsniedz reālas izredzes gūt gaidāmo ieguvumu, un tai nevajadzētu būt nesamērīgai vai patvaļīgai" ([376]). Kā jau minēts, praksē tas nozīmē, ka samērīguma pārbaude balstās uz līdzsvara pārbaudi starp sasniedzamo mērķi ("operatīvo(-ajiem) nolūku(-iem)") un pieejamajām tehniskajām iespējām (piemēram, mērķēta vai masveida pārtveršana, iejaukšanās iekārtās, saziņas datu iegūšana), dodot priekšroku vismazāk traucējošiem līdzekļiem (sk. iepriekš 181. un 182. apsvērumu). Ja mērķim ir atbilstoši vairāki pasākumi, priekšroka jādod mazāk traucējošiem līdzekļiem.

(224) Papildu garantiju pieprasītā pasākuma samērīguma novērtējumam nodrošina fakts, ka ministram jāsaņem attiecīgā informācija pienācīgai novērtējuma veikšanai. Konkrēti, Pārtveršanas prakses kodeksā un Prakses kodeksā par iejaukšanos iekārtās ir prasība iesniegtajā pieteikumā attiecīgajām iestādēm norādīt pieteikuma vēsturisko informāciju, pārtveramās saziņas aprakstu un telesakaru operatorus, kuru palīdzība ir nepieciešama, atļaujamās rīcības aprakstu, operatīvos nolūkus un paskaidrojumu, kāpēc rīcība ir nepieciešama un samērīga ([377]).

(225) Visbeidzot un svarīgi, ka ministra lēmums izdot orderi ir jāapstiprina neatkarīgam tieslietu komisāram, kurš izvērtē ierosinātā pasākuma nepieciešamības un samērīguma novērtējumu, izmantojot tos pašus principus, kurus izmantotu tiesa pieteikumā veikt pārskatīšanu tiesā ([378]). Konkrētāk, tieslietu komisārs ministra secinājumus par to, vai orderis ir nepieciešams un vai rīcība ir samērīga, pārskatīs, ņemot vērā 2016. gada IPL 2. panta 2. punktā noteiktos principus (vispārējie pienākumi saistībā ar privātumu). Tieslietu komisārs arī pārskatīs ministra secinājumus par to, vai katrs no orderī norādītajiem operatīvajiem nolūkiem ir nolūks, kuram ir vai var būt nepieciešama atlase. Ja tieslietu komisārs atsakās apstiprināt lēmumu par ordera izdošanu, ministrs var vai nu: i) akceptēt lēmumu un līdz ar to neizdot orderi; vai ii) nodot lietu izmeklēšanas pilnvaru komisāram lēmuma pieņemšanai (izņemot gadījumus, kad izmeklēšanas pilnvaru komisārs ir pieņēmis sākotnējo lēmumu) ([379]).

ii) *Papildu garantijas*

(226) 2016. gada IPL ir ieviesti papildu ierobežojumi masveida pilnvaru ordera darbības ilgumam, atjaunošanai un grozīšanai. Ordera darbības ilgums nedrīkst pārsniegt sešus mēnešus, un jebkurš lēmums par ordera atjaunošanu vai grozīšanu (izņemot nelielas izmaiņas) ir jāapstiprina arī tieslietu komisāram ([380]). Pārtveršanas prakses kodeksā un Prakses kodeksā par iejaukšanos iekārtās precizēts, ka izmaiņas ordera operatīvajos nolūkos tiek uzskatītas par būtiskiem grozījumiem orderī ([381]).

([375]) 2016. gada IPL 138. panta 1. punkta b) un c) apakšpunkts un 178. panta b) un c) apakšpunkts.

([376]) Sk. Saziņas pārtveršanas prakses kodeksu, 4.10. punkts, sk. 278. zemsvītras piezīmi.

([377]) Saziņas pārtveršanas prakses kodekss, 6.20. punkts, sk. 278. zemsvītras piezīmi, un Prakses kodekss par iejaukšanos iekārtās, 6.13. punkts, sk. 348. zemsvītras piezīmi.

([378]) 2016. gada IPL 138. panta 1. punkta g) apakšpunkts un 178. panta 1. punkta f) apakšpunkts. Eiropas Cilvēktiesību tiesa īpaši noteikusi, ka neatkarīgas struktūras iepriekšēja atļauja ir svarīga garantija pret ļaunprātīgu izmantošanu masveida pārtveršanas kontekstā. Eiropas Cilvēktiesību tiesa (virspalāta), *Big Brother Watch and others v United Kingdom* (sk. iepriekš 269. zemsvītras piezīmi), 351. un 352. punkts. Ir svarīgi ņemt vērā, ka šis spriedums attiecās uz iepriekšējo tiesisko regulējumu (2000. gada IPRL), kurš neietvēra dažas no 2016. gada IPL ieviestajām garantijām (tostarp neatkarīga tieslietu komisāra iepriekšēju atļauju).

([379]) 2016. gada IPL 159. panta 3. un 4. pants.

([380]) 2016. gada IPL 143.–146. pants un 184.–188. pants. Steidzamu grozījumu gadījumā ministrs var veikt tos bez apstiprinājuma, taču par to jāpaziņo komisāram, un komisāram pēc tam jāizlemj, vai apstiprināt vai noraidīt grozījumu (2016. gada IPL 147. pants). Orderis ir jāatceļ, ja tas vairs nav nepieciešams vai samērīgs vai ja pārtvertā satura, metadatu vai citu saskaņā ar orderi iegūto datu pārbaude vairs nav nepieciešama nevienam no orderī norādītajiem operatīvajiem nolūkiem (2016. gada IPL 148. un 189. pants).

([381]) Saziņas pārtveršanas prakses kodekss, 6.44.–6.47. punkts, sk. 278. zemsvītras piezīmi, un Prakses kodekss par iejaukšanos iekārtās, 6.48. punkts, sk. 348. zemsvītras piezīmi.

(227) Līdzīgi tam, kas paredzēts mērķētas pārtveršanas gadījumos, 2016. gada IPL 6. daļā ir paredzēts, ka ministram ir jānodrošina, ka pastāv garantijas attiecībā uz atbilstīgi orderim iegūtā materiāla glabāšanu un izpaušanu ([382]), kā arī informācijas izpaušanu ārvalstīs ([383]). Konkrēti, 2016. gada IPL 150. panta 5. punktā un 191. panta 5. punktā ir noteikts, ka katra kopija, kas izgatavota no šī materiāla, kurš savākts saskaņā ar orderi, ir jāuzglabā drošā veidā un jāiznīcina, tiklīdz vairs nav būtiska iemesla tās glabāšanai, savukārt 2016. gada IPL 150. panta 2. punktā un 191. panta 2. punktā noteikts, ka to personu skaitam, kurām materiāls tiek izpausts, un apmēram, kādā materiāls tiek izpausts, darīts pieejams vai kopēts, jābūt ierobežotam līdz minimumam, kas nepieciešams likumā paredzētajiem nolūkiem. ([384])

(228) Visbeidzot, ja materiāls, kas pārtverts, izmantojot vai nu masveida pārtveršanu, vai arī masveida iejaukšanos iekārtās, ir jānodod trešai valstij ("informācijas izpaušana ārvalstīs"), 2016. gada IPL paredz, ka ministram jānodrošina, lai tiktu ieviesti pasākumi, kas nodrošina, ka šajā trešā valstī pastāv līdzīgas drošības, glabāšanas un izpaušanas garantijas ([385]). Turklāt 2018. gada DAL 109. pantā ir noteiktas īpašas prasības attiecībā uz personas datu starptautisku nosūtīšanu, ko veic izlūkdienesti, uz trešām valstīm vai starptautiskai organizācijai, kā arī ir noteikts, ka datus nav atļauts nosūtīt uz valsti vai teritoriju ārpus Apvienotās Karalistes vai starptautiskai organizācijai, izņemot gadījumus, kad nosūtīšana ir nepieciešama un samērīga pārziņa likumā noteikto funkciju vai citu mērķu sasniegšanai, kā paredzēts 1989. gada Drošības dienestu likuma 2. panta 2. punkta a) apakšpunktā vai 1994. gada Izlūkdienestu likuma 2. panta 2. punkta a) apakšpunktā un 4. panta 2. punkta a) apakšpunktā ([386]). Ir svarīgi norādīt, ka šīs prasības piemēro arī gadījumos, kad izmanto atbrīvojumu sakarā ar valsts drošību atbilstīgi 2018. gada DAL 110. pantam, jo 2018. gada DAL 110. pants neparedz 2018. gada DAL 109. pantu kā vienu no noteikumiem, kuru var nepiemērot, ja valsts drošības aizsardzības nolūkā nepieciešams atbrīvojums no konkrētiem noteikumiem.

(229) Pēc tam, kad orderis ir apstiprināts un dati ir savākti masveidā, pirms to pārbaudes tiks veikta datu atlase. Atlases un pārbaudes posmam analītiķis veic samērīguma pārbaudi, kas, pamatojoties uz orderī iekļautajiem operatīvajiem nolūkiem (un, iespējams, pastāvošo filtrēšanas kārtību), nosaka atlases kritērijus. Kā paredzēts IPL 152. un 193. pantā, izdodot orderi, ministram jāpārliecinās, ka ir ieviesti pasākumi, lai garantētu, ka materiāla atlase tiek veikta tikai noteiktiem operatīviem nolūkiem un ka tas ir nepieciešami un samērīgi jebkuros apstākļos. Šajā sakarā Apvienotās Karalistes iestādes paskaidroja, ka masveidā pārtvertais materiāls vispirms tiek atlasīts, izmantojot automatizētu filtrēšanu, lai atmestu datus, kas, visticamāk, nav valsts drošības interesēs. Filtri periodiski atšķirsies (mainoties interneta plūsmas modeļiem, tipiem un protokoliem) un būs atkarīgi no tehnoloģiju un operatīvā konteksta. Pēc šī posma datus pārbaudei var atlasīt tikai tad, ja tie ir nepieciešami orderī norādītajiem operatīvajiem nolūkiem ([387]). 2016. gada IPL paredzētās garantijas savāktā materiāla pārbaudes nolūkiem attiecas uz jebkāda veida datiem (gan pārtvertu saturu, gan sekundāriem datiem) ([388]). 2016. gada IPL 152. un 193. pantā ir paredzēts arī vispārējs aizliegums pārbaudes nolūkiem atlasīt materiālu attiecībā uz sarunām, kuras nosūtījušas personas vai kuras paredzētas personām, kas atrodas Britu salās. Ja iestādes vēlas pārbaudīt šādu materiālu, tās atbilstīgi 2016. gada IPL 2. un 4. daļai iesniedz pieprasījumu mērķētas pārbaudes orderim, ko izdod ministrs un apstiprina tieslietu komisārs ([389]). Ja persona tīši izvēlas pārtverto saturu pārbaudei, pārkāpjot likumā noteiktās prasības ([390]), tā izdara noziedzīgu nodarījumu ([391]).

([382]) 2016. gada IPL 156. pants.

([383]) 2016. gada DAL 150. un 191. pants.

([384]) Eiropas Cilvēktiesību tiesas virspalāta lietā *Big Brother Watch and others v United Kingdom* (sk. iepriekš 268. zemsvītras piezīmi) atbalstīja papildu glabāšanas, piekļuves un izpaušanas garantiju sistēmu, kas tika paredzēta saskaņā ar 2000. gada IPRL, sk. 392.–394. un 402.–405. punktu. Tā pati garantiju sistēma ir paredzēta 2016. gada IPL.

([385]) 2016. gada DAL 151. un 192. pants.

([386]) Papildu informāciju par šiem mērķiem sk. 312. zemsvītras piezīmē.

([387]) Saziņas pārtveršanas kodeksos šajā sakarā norādīts, ka "šīs apstrādes sistēmas apstrādā datus no saziņas saitēm vai signāliem, kurus pārtvērēja iestāde ir izvēlējusies pārtvert. Pēc tam šo saišu un signālu plūsmai piemēro tādu filtrēšanas pakāpi, kas paredzēta tādu saziņas veidu atlasei, kas varētu būt vērtīgi izlūkošanas nolūkiem, vienlaikus atmetot tos, kuri, visticamāk, nebūs vērtīgi izlūkošanas nolūkiem. Šīs filtrēšanas rezultātā, kas dažādās apstrādes sistēmās atšķirsies, ievērojama daļa šo saišu saziņas un signālu tiks automātiski atmesti. Pēc tam var tikt veikti sarežģīti papildu meklējumi, lai izgūtu papildu saziņu, kurai varētu būt vislielākā vērtība izlūkošanas nolūkiem, kas attiecas uz aģentūras likumā noteiktajām funkcijām. Pēc tam šo saziņu var atlasīt pārbaudei vienam vai vairākiem orderī norādītajiem operatīvajiem nolūkiem, ja ir izpildīti nepieciešamības un samērīguma nosacījumi. Pilnvarotas personas pārbaudei var atlasīt tikai tos elementus, kas nav atmesti ar filtrēšanas palīdzību" (Saziņas pārtveršanas prakses kodeksi, 6.6. punkts, sk. 278. zemsvītras piezīmi).

([388]) Sk. 2016. gada IPL 152. panta 1. punkta a) un b) apakšpunktu, saskaņā ar kuru abu veidu datu (pārtvertā satura un sekundāro datu) pārbaude jāveic tikai noteiktajā nolūkā un tai jābūt nepieciešamai un samērīgai visos apstākļos.

([389]) Šāda veida orderis nav nepieciešams, ja dati saistībā ar personām, kuras atrodas Britu salās, ir sekundāri dati (sk. 2016. gada IPL 152. panta 1. punkta c) apakšpunktu).

([390]) 2016. gada IPL 152. un 193. pants.

([391]) 2016. gada IPL 155. un 196. pants.

(230) Analītiķa veiktajam materiāla atlases novērtējumam piemēro IPK *ex post* pārraudzību, kurā novērtē atbilstību īpašām garantijām, kas pārbaudes posmam noteiktas 2016. gada IPL ([392]) (sk. arī 229. apsvērumu). IPK ir pastāvīgi jāpārrauga (tostarp veicot revīzijas, pārbaudes un izmeklēšanas), kā publiskās iestādes īsteno 2016. gada IPL minētās izmeklēšanas pilnvaras ([393]). Šajā ziņā Pārtveršanas prakses kodeksā un Prakses kodeksā par iejaukšanos iekārtās ir precizēts, ka aģentūrai ir pienākums uzturēt reģistru, lai veiktu turpmāku pārbaudi un revīziju, un šajā reģistrā ir jāprecizē, kāpēc pilnvarotu personu piekļuve materiālam ir nepieciešama un samērīga, kā arī piemērojamie operatīvie nolūki ([394]). Piemēram, savā 2018. gada pārskatā izmeklēšanas pilnvaru komisāra birojs (IPKB) ([395]) secināja, ka analītiķu reģistrētie pamatojumi atsevišķu masveidā savāktu materiālu pārbaudei atbilda prasītajam samērīguma standartam, sniedzot pietiekamu informāciju par viņu "vaicājuma" iemesliem attiecībā uz sasniedzamo mērķi ([396]). IPKB 2019. gada ziņojumā saistībā ar masveida pilnvarām skaidri norādīja, ka tā mērķis ir turpināt masveida pārtveršanu pārbaudes, ieskaitot selektoru un meklēšanas kritēriju detalizētu pārbaudi ([397]). Tas arī turpinās katrā atsevišķā gadījumā rūpīgi pārbaudīt novērošanas pasākumu (mērķētu vai masveida) izvēli orderu saņemšanas pieteikumu izvērtēšanā saskaņā ar divkāršo drošību un pārbaudēs ([398]). Šī turpmākā uzraudzība tiks pienācīgi ņemta vērā saistībā ar Komisijas veiktu šā lēmuma uzraudzību saskaņā ar 281.–284. apsvērumu.

3.3.1.1.4.2. Saziņas datu masveida iegūšana

(231) 2016. gada IPL 6. daļas 2. nodaļā reglamentēti masveida iegūšanas orderi, ar ko pilnvaro adresātu pieprasīt telesakaru operatoram izpaust vai iegūt jebkādus operatora rīcībā esošos saziņas datus. Šie orderi arī pilnvaro pieprasītāju iestādi atlasīt datus turpmākajam pārbaudes posmam. Tā kā tas attiecas uz saziņas datu mērķētu glabāšanu un iegūšanu (sk. 199. apsvērumu), arī saziņas datu masveida iegūšana parasti neattiecas uz ES datu subjektu personas datiem, kas saskaņā ar šo lēmumu nosūtīti uz Apvienoto Karalisti. Pienākums izpaust saziņas datus saskaņā ar 2016. gada IPL 6. daļas 2. nodaļu attiecas uz datiem, kurus telesakaru operatori Apvienotajā Karalistē vāc tieši no telesakaru pakalpojumu lietotājiem ([399]). Šāda veida "uz klientu vērsta" apstrāde parasti nenozīmē nosūtīšanu, pamatojoties uz šo lēmumu, proti, nosūtīšanu no pārziņa/apstrādātāja ES pārzinim/apstrādātājam Apvienotajā Karalistē.

(232) Tomēr informācijas pilnīguma labad nosacījumi un garantijas, kas regulē saziņas datu masveida iegūšanu, ir aprakstīti turpmāk.

([392]) 2016. gada IPL 152. un 193. pants.

([393]) 2016. gada IPL 229. pants.

([394]) Saziņas pārtveršanas prakses kodekss, 6.74. punkts, sk. 278. zemsvītras piezīmi, un Prakses kodekss par iejaukšanos iekārtās, 6.78. punkts, sk. 348. zemsvītras piezīmi.

([395]) IPKB ir izveidots saskaņā ar 2016. gada IPL 238. pantu, lai nodrošinātu IPK nepieciešamo personālu, telpas, aprīkojumu un citas iespējas un pakalpojumus, kas nepieciešami tā funkciju veikšanai (sk. 251. apsvērumu).

([396]) IPKB 2018. gada pārskatā bija norādīts, ka *GCHQ* analītiķu reģistrētie pamatojumi "atbilst prasītajam standartam un analītiķi pietiekami detalizēti uzskaita savu masveida datu pieprasījumu samērīgumu". Izmeklēšanas pilnvaru komisāra 2018. gada pārskats, 6.22. punkts, sk. 464. zemsvītras piezīmi.

([397]) Izmeklēšanas pilnvaru komisāra 2019. gada pārskats, 7.6. punkts, sk. 463. zemsvītras piezīmi.

([398]) Izmeklēšanas pilnvaru komisāra 2019. gada pārskats, 10.22. punkts, sk. 463. zemsvītras piezīmi.

([399]) Tas izriet no saziņas datu definīcijas, kas sniegta 2016. gada IPL 261. panta 5. punktā, saskaņā ar kuru saziņas datus glabā vai iegūst telesakaru operators, un tie attiecas vai nu uz telesakaru pakalpojuma lietotāju, vai uz šī pakalpojuma sniegšanu, vai ir ietverti, iekļauti kā daļa saziņā, pievienoti saziņai vai loģiski saistīti ar saziņu (sk. arī Saziņas datu masveida iegūšanas prakses kodeksu, kas pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, 2.15.–2.22. punkts). Turklāt 2016. gada IPL 261. panta 10. punktā sniegtā telesakaru operatora definīcija paredz, ka telesakaru operators ir persona, kura piedāvā vai sniedz telesakaru pakalpojumus personām Apvienotajā Karalistē vai kura kontrolē vai nodrošina telesakaru sistēmu, kas ir (pilnībā vai daļēji) Apvienotajā Karalistē vai kontrolēta no Apvienotās Karalistes. Šīs definīcijas skaidri norāda, ka saistības atbilstīgi 2016. gada IPL nevar uzlikt telesakaru operatoriem, kuru aprīkojums neatrodas Apvienotajā Karalistē vai netiek kontrolēts no tās un kuri nepiedāvā vai nesniedz pakalpojumus personām Apvienotajā Karalistē (sk. arī Saziņas datu masveida iegūšanas prakses kodeksa 2.2. punktu). Ja ES abonenti (neatkarīgi no tā, vai tie atrodas ES vai Apvienotajā Karalistē) izmanto pakalpojumus Apvienotajā Karalistē, jebkādu saziņu saistībā ar šī pakalpojuma sniegšanu tieši apkopotu pakalpojumu sniedzējs Apvienotajā Karalistē, nevis nosūtītu tos no ES.

(233) 2016. gada IPL aizstāj tiesību aktus par masveida saziņas datu iegūšanu, kas bija EST sprieduma priekšmets lietā *Privacy International*. Šajā lietā aplūkotie tiesību akti tika atcelti, un jaunais režīms paredz konkrētus nosacījumus un garantijas, saskaņā ar kuriem šādu pasākumu var atļaut.

(234) Konkrēti, atšķirībā no iepriekšējā režīma, saskaņā ar kuru ministram bija pilnīga rīcības brīvība, atļaujot noteiktu pasākumu ([400]), 2016. gada IPL prasīts, lai ministrs izdotu orderi tikai tad, ja pasākums ir nepieciešams un samērīgs. Praksē tas nozīmē, ka starp piekļuvi datiem un izvirzīto mērķi jābūt saiknei ([401]). Konkrētāk, ministram jānovērtē saikne starp pieprasīto pasākumu un vienu vai vairākiem orderī norādītajiem "operatīvajiem nolūkiem" (sk. 219. apsvērumu), ievērojot samērīguma novērtējumu; attiecīgais prakses kodekss nosaka, ka "ministram jāņem vērā, vai to, kas ar ordera palīdzību sasniedzams, varēja pamatoti sasniegt ar citiem mazāk traucējošiem līdzekļiem (Likuma 2. panta 2. punkta a) apakšpunkts). Piemēram, nepieciešamās informācijas iegūšana, izmantojot mazāk traucējošu pilnvaru, piemēram, saziņas datu mērķētu iegūšanu" ([402]).

(235) Veicot šādu novērtējumu, ministrs paļausies uz informāciju, kas izlūkdienestu vadītājiem ir jāiesniedz savā pieteikumā ([403]), piemēram, iemesliem, kāpēc pasākums tiek uzskatīts par nepieciešamu kādam no likumā noteiktajiem iemesliem, un iemesliem, kāpēc sasniedzamo mērķi nevarēja pamatoti sasniegt ar citiem mazāk traucējošiem līdzekļiem ([404]). Turklāt operatīvie nolūki ierobežo apmēru, kādā datus, kas iegūti saskaņā ar orderi, var atlasīt pārbaudei ([405]). Kā noteikts attiecīgajā prakses kodeksā, operatīvajos nolūkos ir jāapraksta skaidra prasība un jāietver pietiekami detalizēta informācija, lai pārliecinātu ministru, ka iegūtos datus pārbaudei var atlasīt, tikai pamatojoties uz konkrētiem iemesliem ([406]). Faktiski ministram pirms ordera apstiprināšanas ir jāpārliecinās, ka ir ieviesti īpaši pasākumi, lai nodrošinātu, ka pārbaudei tiek atlasīts tikai tas materiāls, kas uzskatāms par nepieciešamu pārbaudei operatīviem nolūkiem un likumā paredzētajam nolūkam, un tiem jābūt samērīgiem un nepieciešamiem jebkuros apstākļos. Šī konkrētā prasība, kas atspoguļota 2016. gada IPL 158. un 172. pantā ([407]) attiecībā uz atlases vajadzībām izmantoto kritēriju nepieciešamības un samērīguma iepriekšēju novērtējumu, ir vēl viens svarīgs 2016. gada IPL ieviestā režīma jauninājums salīdzinājumā ar iepriekšējo režīmu.

(236) 2016. gada IPL arī ieviests ministra pienākums pirms ordera izdošanas saziņas datu masveida iegūšanai pārliecināties, ka pastāv konkrēti ierobežojumi savākto personas datu drošībai, glabāšanai un izpaušanai ([408]). Ja informācija tiek izpausta ārvalstīs, šajā kontekstā tiek piemērotas arī 227. apsvērumā aprakstītās garantijas attiecībā uz masveida pārtveršanu un masveida iejaukšanos iekārtās ([409]). Citi ierobežojumi ir noteikti tiesību aktos attiecībā uz masveida pilnvaru orderu darbības ilgumu ([410]), atjaunošanu ([411]) un grozīšanu ([412]).

(237) Svarīgi ir tas, ka tāpat kā attiecībā uz pārējām masveida pilnvarām ministram pirms ordera izdošanas jāsaņem tieslietu komisāra ([413]) apstiprinājums. Šī ir 2016. gada IPL ieviestā režīma svarīga iezīme.

([400]) 1984. gada Telesakaru likuma 94. panta 1. punkts paredzēja, ka ministrs ir tiesīgs izdot "vispārēja rakstura norādījumus, kas ministram šķiet nepieciešami vai lietderīgi valsts drošības interesēs (..)" (sk. 451. zemsvītras piezīmi).

([401]) Sk. spriedumu lietā *Privacy International*, 78. punkts.

([402]) Sk. Saziņas datu masveida iegūšanas prakses kodeksu, 4.11. punkts (sk. 399414. zemsvītras piezīmi).

([403]) Masveida iegūšanas orderi var pieprasīt tikai šādu izlūkdienestu vadītāji: i) Drošības dienesta ģenerāldirektors; ii) Slepenās izlūkošanas dienesta priekšnieks vai iii) *GCHQ* direktors (sk. 2016. gada IPL 158. un 263. pantu).

([404]) Sk. Saziņas datu masveida iegūšanas prakses kodeksu, 4.5. punkts (sk. 399. zemsvītras piezīmi).

([405]) Saskaņā ar 2016. gada IPL 161. pantu orderī norādītajiem operatīvajiem nolūkiem ir jābūt tiem, kuri izlūkdienestu vadītāju uzturētajā sarakstā ("operatīvo nolūku saraksts") norādīti kā nolūki, kas, viņuprāt, uzskatāmi par operatīviem nolūkiem, kuru dēļ saziņas datus, kas iegūti ar masveida pārtveršanas orderi, drīkst atlasīt pārbaudei.

([406]) Sk. Saziņas datu masveida iegūšanas prakses kodeksu, 6.6. punkts (sk. 399. zemsvītras piezīmi).

([407]) 2016. gada IPL 172. pantā paredzēts, ka jāievieš īpašas garantijas filtrēšanas un atlases posmam, lai pārbaudītu masveidā iegūto saziņu. Turklāt tīša pārbaude, pārkāpjot šīs garantijas, ir arī noziedzīgs nodarījums (sk. 2016. gada IPL 173. pantu).

([408]) 2016. gada IPL 171. pants.

([409]) 2016. gada IPL 171. panta 9. punkts.

([410]) 2016. gada IPL 162. pants.

([411]) 2016. gada IPL 163. pants.

([412]) 2016. gada IPL 164.–166. pants.

([413]) 2016. gada IPL 159. pants.

(238) IPK veic *ex post* pārraudzību attiecībā uz masveidā iegūtā materiāla (saziņas datu) pārbaudes procedūru (sk. turpmāk 254. apsvērumu). Šajā sakarā ar 2016. gada IPL ieviesa prasību, ka izlūkošanas analītiķim, kurš veic pārbaudi, pirms datu atlasīšanas pārbaudei jāreģistrē iemesls, kāpēc ierosinātā pārbaude ir nepieciešama un samērīga konkrētam operatīvajam nolūkam ([414]). IPKB 2019. gada pārskatā par *GCHQ* un MI5 praksi tika konstatēts, ka "masveida saziņas datu (*BCD*) kritiskā loma *GCHQ* veikto darbību klāstā pārbaudītajās lietās bija labi formulēta. Mēs izskatījām pieprasīto datu būtību un sniegtās izlūkošanas vajadzības un guvām pārliecību, ka dokumentācija apliecināja viņu pieejas nepieciešamību un samērīgumu" ([415]). MI5 reģistrētie pamatojumi atbilda labiem standartiem un apmierināja nepieciešamības un samērīguma principus" ([416]).

3.3.1.1.4.3. Masveida personas datu kopas glabāšana un pārbaude

(239) Masveida personas datu kopu (BPD) orderi ([417]) ļauj izlūkošanas aģentūrām glabāt un pārbaudīt datu kopas, kas satur personas datus, kuri attiecas uz vairākām personām. Saskaņā ar Apvienotās Karalistes iestāžu sniegtajiem paskaidrojumiem šādu datu kopu analīze var būt "vienīgais veids, kā Apvienotās Karalistes izlūkdienestu kopienai sekmēt izmeklēšanu un identificēt teroristus, izmantojot ļoti ierobežotus izlūkošanas informācijas pavedienus vai gadījumos, kad viņu saziņa tiek tīši slēpta" ([418]). Ir divu veidu orderi: "BPD klases orderi" ([419]), kas attiecas uz noteiktu datu kopu kategoriju, proti, datu kopām, kas ir līdzīgas pēc satura un paredzētā lietojuma un rada līdzīgus apsvērumus, piemēram, par aizskāruma un sensitivitātes pakāpi un datu izmantošanas samērīgumu, tādējādi ļaujot ministram apsvērt visu attiecīgās klases datu vienlaicīgas ieguves nepieciešamību un samērīgumu. Piemēram, BPD klases orderis var aptvert ceļojumu datu kopas, kas attiecas uz līdzīgiem maršrutiem ([420]). "Konkrētas BPD orderi" ([421]) turpretī attiecas uz vienu konkrētu datu kopu, piemēram, jauna vai neparasta veida datu kopu, kas neietilpst esošajā BPD klases orderī, vai datu kopu, kas attiecas uz konkrētiem personas datu veidiem ([422]), un tāpēc nepieciešamas papildu garantijas ([423]). 2016. gada IPL noteikumi, kas attiecas uz BPD, ļauj šādas datu kopas pārbaudīt un glabāt tikai tad, ja tas ir nepieciešami un samērīgi ([424]), kā arī atbilst vispārējiem pienākumiem attiecībā uz privātumu ([425]).

(240) Pilnvarojumam izsniegt *BPD* orderi piemēro "divkāršās drošības" procedūru: pasākuma nepieciešamības un samērīguma novērtējumu vispirms veic ministrs un pēc tam tieslietu komisārs ([426]). Ministram ir jāapsver pieprasītā ordera veida raksturs un tvērums, attiecīgo datu kategorija un atsevišķu masveida personas datu kopu skaits, kas, iespējams, ietilpst konkrētajā ordera veidā ([427]). Turklāt, kā norādīts Izlūkdienestu masveida personas datu kopu glabāšanas un izmantošanas prakses kodeksā, ir jāuztur sīka uzskaite, un tai veic IPK revīziju ([428]). BPD glabāšana un pārbaudīšana ārpus 2016. gada IPL darbības jomas robežām ir noziedzīgs nodarījums ([429]).

([414]) IPKB 2019. gada pārskats, 8.6. punkts, sk. 463. zemsvītras piezīmi.
([415]) IPKB 2019. gada pārskats, 10.4. punkts, sk. 463. zemsvītras piezīmi.
([416]) IPKB 2019. gada pārskats, 8.37. punkts, sk. 463. zemsvītras piezīmi.
([417]) 2016. gada IPL 200. pants.
([418]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, H iedaļa "Valsts drošība", 34. lpp., sk. 29. zemsvītras piezīmi.
([419]) 2016. gada IPL 204. pants.
([420]) Izlūkdienestu masveida personas datu kopu glabāšanas un izmantošanas prakses kodekss, 4.7. punkts, pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.
([421]) 2016. gada IPL 205. pants.
([422]) Piemēram, sensitīvi personas dati, sk. 2016. gada IPL 202. pantu un Izlūkdienestu masveida personas datu kopu glabāšanas un izmantošanas prakses kodeksa 4.21. un 4.12. punktu, sk. 469. zemsvītras piezīmi.
([423]) Pieteikums konkrētas BPD orderim ministram jāizskata individuāli, t. i., attiecībā uz vienu konkrētu datu kopu. Izlūkdienestam saskaņā ar IPL 205. pantu savā pieteikumā konkrētas *BPD* orderim ir jāiekļauj detalizēts paskaidrojums par attiecīgā materiāla būtību un apjomu, kā arī to "operatīvo nolūku" saraksts, kuriem attiecīgais izlūkdienests vēlas pārbaudīt *BPD* (ja izlūkdienests prasa orderi glabāšanai un pārbaudei, nevis tikai glabāšanai). Izdodot *BPD* klases orderi, ministrs tā vietā apsver visu datu kopu kategoriju vienlaikus.
([424]) 2016. gada IPL 204. un 205. pants.
([425]) 2016. gada IPL 2. pants.
([426]) 2016. gada DAL 204. un 205. pants.
([427]) Izlūkdienestu masveida personas datu kopu glabāšanas un izmantošanas prakses kodekss, 5.2. punkts, sk. 420. zemsvītras piezīmi.
([428]) Izlūkdienestu masveida personas datu kopu glabāšanas un izmantošanas prakses kodekss, 8.1.–8.15. punkts, sk. 420. zemsvītras piezīmi.
([429]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, H iedaļa "Valsts drošība", 34. lpp., sk. 29. zemsvītras piezīmi.

3.3.2. *Savāktās informācijas turpmāka izmantošana*

(241) Personas datus, kas apstrādāti saskaņā ar 2018. gada DAL 4. daļu, nedrīkst apstrādāt veidā, kas nav saderīgs ar nolūku, kādam tie tika vākti ([430]). 2018. gada DAL paredz, ka pārzinis var apstrādāt datus citam nolūkam, nevis tam, kuram dati tika vākti, ja tas ir saderīgs ar sākotnējo nolūku un ar nosacījumu, ka pārzinis ir likumīgi pilnvarots apstrādāt datus un ka apstrāde ir nepieciešama un samērīga ([431]). Turklāt 1989. gada Drošības dienestu likumā un 1994. gada Izlūkdienestu likumā ir noteikts, ka izlūkošanas aģentūru vadītāju pienākums ir nodrošināt, ka netiek iegūta vai izpausta informācija, izņemot gadījumus, kad tas nepieciešams aģentūras funkciju pareizai izpildei, vai attiecībā uz citiem ierobežotiem un konkrētiem nolūkiem, kas uzskaitīti attiecīgajos noteikumos ([432]).

(242) Turklāt 2018. gada DAL 109. pantā ir noteiktas konkrētas prasības izlūkdienestu veiktai personas datu starptautiskai nosūtīšanai trešām valstīm vai starptautiskām organizācijām. Saskaņā ar šo noteikumu personas datus nav atļauts nosūtīt uz valsti vai teritoriju ārpus Apvienotās Karalistes vai starptautiskai organizācijai, izņemot gadījumus, kad nosūtīšana ir nepieciešama un samērīga pārziņa likumā noteikto funkciju vai citu mērķu sasniegšanai, kā paredzēts 1989. gada Drošības dienestu likuma 2. panta 2. punkta a) apakšpunktā vai 1994. gada Izlūkdienestu likuma 2. panta 2. punkta a) apakšpunktā un 4. panta 2. punkta a) apakšpunktā ([433]). Ir svarīgi norādīt, ka šīs prasības piemēro arī gadījumos, kad izmanto atbrīvojumu sakarā ar valsts drošību atbilstīgi 2018. gada DAL 110. pantam, jo 2018. gada DAL 110. pants neparedz 2018. gada DAL 109. pantu kā vienu no noteikumiem, kuru var nepiemērot, ja valsts drošības aizsardzības nolūkā nepieciešams atbrīvojums no konkrētiem noteikumiem.

(243) Turklāt, kā norādījumos par izlūkdienestu veiktu apstrādi uzsvēris IKB, papildus 2018. gada DAL 4. daļā paredzētajām garantijām uz izlūkošanas aģentūru, kas kopīgo datus ar trešās valsts izlūkošanas struktūru, attiecas arī garantijas, kuras paredzētas citos piemērojamos leģislatīvajos pasākumos ar mērķi nodrošināt, ka personas dati tiek iegūti, kopīgoti un izskatīti likumīgi un atbildīgi ([434]). Piemēram, 2016. gada IPL nosaka papildu garantijas attiecībā uz tāda materiāla nosūtīšanu uz trešo valsti, kas savākts, izmantojot mērķētu pārtveršanu ([435]), mērķētu iejaukšanos iekārtās ([436]), masveida pārtveršanu ([437]), saziņas datu masveida iegūšanu ([438]) un masveida iejaukšanos iekārtās ([439]) (tā dēvētā "informācijas izpaušana ārvalstīs"). Konkrēti, iestādei, kas izsniedz orderi, jānodrošina, ka ir spēkā kārtība, ar kuru garantē, ka trešā valsts, saņemot datus, ierobežo to personu skaitu, kuras var aplūkot materiālu, izpaušanas apjomu un no jebkura materiāla izgatavotu kopiju skaitu līdz minimumam, kas nepieciešams 2016. gada IPL noteiktajiem atļautajiem nolūkiem ([440]).

3.3.3. *Pārraudzība*

(244) Valdības piekļuvi valsts drošības nolūkos pārrauga vairākas atšķirīgas struktūras. Informācijas komisārs pārrauga personas datu apstrādi, ņemot vērā 2018. gada DAL (plašāku informāciju par komisāra neatkarību, amata funkcijām un pilnvarām sk. 85.–98. apsvērumā), savukārt neatkarīgu un tiesisku pārraudzību attiecībā uz izmeklēšanas

([430]) 2018. gada DAL 87. panta 1. punkts.

([431]) 2018. gada DAL 87. panta 3. punkts. Kaut arī pārziņus var atbrīvot no šī principa saskaņā ar 2018. gada DAL 110. pantu tiktāl, ciktāl šāds atbrīvojums ir nepieciešams, lai aizsargātu valsts drošību, šāds atbrīvojums jāvērtē katrā gadījumā atsevišķi, un uz to var atsaukties tikai tiktāl, ciktāl konkrētā noteikuma piemērošanai būtu negatīvas sekas valsts drošībai (sk. 132. apsvērumu). Apvienotās Karalistes izlūkdienestu valsts drošības sertifikāti (pieejami vietnē https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) neaptver 2018. gada DAL 87. panta 3. punktu. Turklāt, tā kā jebkurai apstrādei cita nolūkā jābūt atļautai ar tiesību aktu, izlūkdienestiem jābūt skaidram juridiskajam pamatam turpmākai apstrādei.

([432]) Papildu informāciju par šiem nolūkiem sk. 312. zemsvītras piezīmē.

([433]) Sk. 312. zemsvītras piezīmi.

([434]) IKB norādījumi par izlūkdienestu veiktu apstrādi (sk. 161. zemsvītras piezīmi).

([435]) 2016. gada IPL 54. pants.

([436]) 2016. gada IPL 130. pants.

([437]) 2016. gada IPL 151. pants.

([438]) 2016. gada IPL 171. panta 9. punkts.

([439]) 2016. gada IPL 192. pants.

([440]) Kārtībai jāietver pasākumi, kas nodrošina, ka visas jebkura materiāla kopijas visu glabāšanas periodu tiek uzglabātas droši. Materiāls, kas iegūts, pamatojoties uz orderi, un katra tā izgatavotā kopija ir jāiznīcina, tiklīdz vairs nav būtiska iemesla to saglabāšanai (sk. 2016. gada IPL 150. panta 2. punktu, 150. panta 5. punktu un 151. panta 2. punktu). Ir vērts norādīt, ka iepriekšējā tiesiskajā regulējumā (2000. gada IPRL) paredzētās līdzīgās garantijas atbilst prasībām, kuras Eiropas Cilvēktiesību tiesa (noteikusi attiecībā uz tāda materiāla kopīgošanu ar ārvalstīm vai starptautiskajām organizācijām, kas iegūts ar masveida pārtveršanu (Eiropas Cilvēktiesību tiesa (virspalāta), *Big Brother Watch and others v United Kingdom* (sk. iepriekš 279. zemsvītras piezīmi), 362. un 399. punkts).

pilnvaru izmantošanu saskaņā ar 2016. gada IPL nodrošina IPK. IPK pārrauga 2016. gada IPL izmeklēšanas pilnvaru izmantojumu gan tiesībaizsardzības, gan valsts drošības iestādēs. Politisko pārraudzību garantē parlamenta Izlūkdienesta komiteja.

3.3.3.1. Pārraudzība atbilstīgi DAL 4. daļai

(245) Personas datu apstrādi, ko izlūkdienesti veic saskaņā ar 2018. gada DAL 4. daļu, pārrauga informācijas komisārs ([441]).

(246) Informācijas komisāra vispārīgās funkcijas saistībā ar izlūkdienestu veikto personas datu apstrādi saskaņā ar 2018. gada DAL 4. daļu ir noteiktas 2018. gada DAL 13. pielikumā. Uzdevumos ietilpst, bet ne tikai 2018. gada DAL 4. daļas uzraudzība un izpildes nodrošināšana, sabiedrības informētības veicināšana, ieteikumi parlamentam, valdībai un citām iestādēm par likumdošanas un administratīvajiem pasākumiem, pārziņu un apstrādātāju informētības veicināšana par viņu pienākumiem, informācijas sniegšanu datu subjektam par datu subjekta tiesību īstenošanu, izmeklēšanas veikšanu utt.

(247) Attiecībā uz 2018. gada DAL 3. daļu komisāram ir pilnvaras paziņot pārziņiem par iespējamu pārkāpumu un izdot brīdinājumus, ka ar apstrādi, iespējams, pārkāpj noteikumus, un, ja pārkāpums ir apstiprinājies, izteikt rājienu. Tas var arī izdot izpildes un soda paziņojumus par konkrētu tiesību akta noteikumu pārkāpumiem ([442]). Tomēr atšķirībā no citām 2018. gada DAL daļām komisārs nevar izdot novērtējuma paziņojumu valsts drošības struktūrai ([443]).

(248) Turklāt 2018. gada DAL 110. pantā ir paredzēts izņēmums attiecībā uz noteiktu komisāra pilnvaru izmantošanu, ja tas ir nepieciešams valsts drošības aizsardzības nolūkos. Tas ietver komisāra pilnvaras izdot (jebkura veida) paziņojumus saskaņā ar DAL (informatīvos, novērtējuma, izpildes un soda), pilnvaras veikt pārbaudes atbilstīgi starptautiskajām saistībām, iekļūšanas un pārbaudes pilnvaras un noteikumus par nodarījumiem ([444]). Kā paskaidrots 126. apsvērumā, šie izņēmumi tiks piemēroti tikai tad, ja tie būs nepieciešami un samērīgi, un katrā gadījumā tos apsvērs atsevišķi.

(249) IKB un Apvienotās Karalistes izlūkdienesti ir parakstījuši saprašanās memorandu ([445]), ar ko izveido sistēmu sadarbībai vairākos jautājumos, tostarp attiecībā uz paziņojumiem par datu aizsardzības pārkāpumiem un datu subjektu sūdzību izskatīšanu. Jo īpaši tajā paredzēts, ka, saņemot sūdzību, IKB izvērtēs, vai atbrīvojums sakarā ar valsts drošību ir piemērots pareizi. Atbildes uz IKB jautājumiem saistībā ar individuālu sūdzību izskatīšanu attiecīgā izlūkošanas aģentūra sniedz 20 darba dienu laikā, izmantojot atbilstošus drošus kanālus, ja ir iesaistīta klasificēta informācija. No 2018. gada aprīļa līdz šim brīdim IKB no fiziskām personām ir saņēmis 21 sūdzību par izlūkdienestiem. Katra sūdzība tika izvērtēta, un datu subjektam tika paziņots tās rezultāts ([446]).

([441]) 2018. gada DAL 116. pants.

([442]) Saskaņā ar 2018. gada DAL 13. pielikuma 2. punktu izpildes un soda paziņojumus pārzinim vai apstrādātājam var izsniegt saistībā ar to, ka pārkāpta 2018. gada DAL 4. daļas 2. nodaļa (apstrādes principi), 2018. gada DAL 4. daļas noteikums, kas piešķir tiesības datu subjektam, 2018. gada DAL 108. pantā noteiktās prasības ziņot komisāram par personas datu aizsardzības pārkāpumu, kā arī 2018. gada DAL 109. pantā noteiktie principi par personas datu nosūtīšanu uz trešām valstīm, valstīm, kas nav konvencijas dalībvalstis, un starptautiskām organizācijām (sīkāk par izpildes un soda paziņojumiem sk. 92. apsvērumā).

([443]) Saskaņā ar 2018. gada DAL 147. panta 6. punktu informācijas komisārs nedrīkst izdot novērtējuma paziņojumu iestādei, kas norādīta 2000. gada Informācijas brīvības likuma 23. panta 3. punktā. To vidū ir Drošības dienests (MI5), Slepenās izlūkošanas dienests (MI6) un Valdības sakaru štābs.

([444]) Noteikumi, uz kuriem var attiecināt atbrīvojumu, ir šādi: 108. pants (komisāra informēšana par personas datu aizsardzības pārkāpumu), 119. pants (pārbaude saskaņā ar starptautiskajām saistībām); 142.–154. pants un 15. pielikums (komisāra paziņojumi, iekļūšanas un pārbaudes pilnvaras); un 170.–173. pants (nodarījumi saistībā ar personas datiem). Turklāt attiecībā uz apstrādi, ko veic izlūkdienesti, – 13. pielikuma (citas komisāra vispārīgās funkcijas) 1. punkta a) un g) apakšpunkts un 2. punkts.

([445]) Informācijas komisijas biroja un Apvienotās Karalistes izlūkdienestu kopienas saprašanās memorands, sk. 165. zemsvītras piezīmi.

([446]) Septiņos no šiem gadījumiem IKB ieteica sūdzības iesniedzējam paust bažas datu pārzinim (gadījumos, kad persona ir vērsusies IKB, bet vispirms būtu vajadzējis vērsties pie datu pārziņa), vienā gadījumā IKB sniedza vispārīgu ieteikumu datu pārzinim (to izmanto, ja pārzinis ar savu rīcību šķietami nav pārkāpis tiesību aktus, bet, uzlabojot praksi, būtu bijis iespējams izvairīties no vēršanās pie IKB), savukārt pārējos 13 gadījumos no datu pārziņa netika prasīta nekāda rīcība (tas notiek, ja uz personas paustajām bažām attiecas 2018. gada Datu aizsardzības likums, jo tās ir saistītas ar personas informācijas apstrādi, bet, pamatojoties uz sniegto informāciju, šķiet, ka pārzinis nav pārkāpis tiesību aktus).

3.3.3.2. Izmeklēšanas pilnvaru izmantošanas pārraudzība saskaņā ar 2016. gada IPL

(250) Saskaņā ar 2016. gada IPL 8. daļu izmeklēšanas pilnvaru izmantošanas pārraudzību veic izmeklēšanas pilnvaru komisārs (IPK). IPK palīdz citi tieslietu komisāri, kurus kopā sauc par tieslietu komisāriem ([447]). 2016. gada IPL ir noteiktas garantijas, kas aizsargā tieslietu komisāru neatkarību. Tieslietu komisāriem tiek izvirzīta prasība ieņemt vai iepriekš ieņemt augstu amatu tiesu iestādē (t. i., tiem pašlaik jābūt vai jābūt bijušiem augstāko tiesu pārstāvjiem ([448]), un, tāpat kā jebkurš tiesu iestāžu pārstāvis, tie ir neatkarīgi no valdības ([449]). Saskaņā ar 2016. gada IPL 227. pantu IPK ieceļ premjerministrs, kurš ieceļ arī tik daudz tieslietu komisāru, cik uzskata par nepieciešamu. Visus komisārus neatkarīgi no tā, vai tie ir tiesu iestāžu pašreizējie vai bijušie pārstāvji, var iecelt, tikai pamatojoties uz triju augsto tiesnešu – Anglijas un Velsas, Skotijas un Ziemeļīrijas – un lorda kanclera kopīgu ieteikumu ([450]). Ministram jānodrošina IPK personāls, telpas, aprīkojums un citas iespējas un pakalpojumi ([451]). Komisāru pilnvaru laiks ir trīs gadi, un viņus var iecelt atkārtoti ([452]). Papildu garantējot tieslietu komisāru neatkarīgu, tos var atbrīvot no amata tikai tad, ja tiek izpildīti stingri nosacījumi, piemērojot augstu prasību slieksni: vai nu premjerministrs konkrētos apstākļos, kas uzskaitīti izsmeļošā sarakstā 2016. gada IPL 228. panta 5. punktā (piemēram, bankrots vai ieslodzījums), vai arī, ja katra parlamenta palāta ir pieņēmusi rezolūciju, ar kuru apstiprina atcelšanu ([453]).

(251) IPK un tieslietu komisāru darbu atbalsta izmeklēšanas pilnvaru komisāra birojs (IPKB). IPKB personālā ietilpst inspektoru komandu, iekšējie juridiskie un tehniskie speciālisti un tehnoloģiju konsultatīva grupa, kas sniedz ekspertu padomus. Tāpat kā atsevišķu tieslietu komisāru gadījumā, IPKB neatkarība ir aizsargāta. IPKB ir Iekšlietu ministrijai piederīga, bet neatkarīga iestāde, t. i., tā saņem finansējumu no Iekšlietu ministrijas, bet savas funkcijas veic neatkarīgi ([454]).

(252) Tieslietu komisāru galvenās funkcijas ir noteiktas 2016. gada IPL 229. pantā ([455]). Jo īpaši tieslietu komisāriem ir plašas iepriekšējas apstiprināšanas pilnvaras, kas ietilpst Apvienotās Karalistes tiesiskajā regulējumā ar 2016. gada IPL ieviestajās garantijās. Tieslietu komisāriem jāapstiprina orderi, kas saistīti ar mērķētu pārtveršanu, iejaukšanos iekārtās, masveida personas datu kopām, saziņas datu masveida iegūšanu, kā arī paziņojumi par saziņas datu glabāšanu ([456]). IPK vienmēr ir arī iepriekš jāapstiprina saziņas datu iegūšana tiesībaizsardzības nolūkā ([457]). Ja komisārs atsakās apstiprināt orderi, ministrs var vērsties pie izmeklēšanas pilnvaru komisāra, kura lēmums ir galīgs.

([447]) Saskaņā ar 2016. gada IPL 227. panta 7. un 8. punktu izmeklēšanas pilnvaru komisārs ir tieslietu komisārs, un izmeklēšanas pilnvaru komisārs un pārējie tieslietu komisāri kopā tiek saukti par tieslietu komisāriem. Šobrīd ir 15 tieslietu komisāri.

([448]) Saskaņā ar 2005. gada Konstitucionālās reformas likuma 3. daļas 60. panta 2. punktu "augsts amats tiesu iestādē" nozīmē tiesneša amatu jebkurā no šīm tiesām: i) Augstākā tiesa; ii) Anglijas un Velsas Apelācijas tiesa; iii) Anglijas un Velsas Augstā tiesa; iv) Skotijas Augstā civillietu tiesa; v) Ziemeļīrijas Apelācijas tiesa; vi) Ziemeļīrijas Augstā tiesa; vai parlamenta augšpalātas Lordu apelācijas komiteja.

([449]) Tiesu iestāžu neatkarība ir balstīta konvencijā, un tā ir plaši atzīta kopš 1701. gada Likuma par troņa mantošanas kārtību.

([450]) 2016. gada IPL 227. panta 3. punkts. Atbilstoši 2016. gada IPL 227. panta 4. punkta e) apakšpunktam tieslietu komisāri ir jāiesaka arī izmeklēšanas pilnvaru komisāram.

([451]) 2016. gada IPL 238. pants.

([452]) 2016. gada IPL 227. panta 2. punkts.

([453]) Atcelšanas process ir identisks citu tiesnešu atcelšanas procesam Apvienotajā Karalistē (sk., piemēram, 1981. gada Likuma par augstākā līmeņa tiesām 11. panta 3. punktu un 2005. gada Konstitucionālās reformas likuma 33. pantu, kam arī ir nepieciešama rezolūcija pēc tam, kad abas parlamenta palātas to ir apstiprinājušas). Līdz šim neviens tieslietu komisārs nav atcelts no amata.

([454]) Neatkarīga iestāde ir organizācija vai aģentūra, kas saņem finansējumu no valdības, bet spēj strādāt patstāvīgi (definīciju un plašāku informāciju par neatkarīgām iestādēm sk. Ministru kabineta biroja rokasgrāmatā par valsts pārvaldes struktūru klasifikāciju, pieejama vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf, un Pārstāvju palātas Valsts pārvaldes atlases komitejas 2014.–2015. gada sesijas pirmajā ziņojumā, kas pieejams vietnē https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf).

([455]) Saskaņā ar 2016. gada IPL 229. pantu tieslietu komisāram ir plašas pārraudzības pilnvaras, kas aptver arī izlūkošanas aģentūru savākto datu glabāšanas un izpaušanas pārraudzību.

([456]) Lēmumi par to, vai apstiprināt ministra lēmumu izdot orderi, ir pašu tieslietu komisāru ziņā. Ja komisārs atsakās apstiprināt orderi, ministrs var vērsties pie izmeklēšanas pilnvaru komisāra, kura lēmums ir galīgs.

([457]) IPK apstiprinājums vienmēr tiek pieprasīts gadījumos, kad saziņas dati tiek iegūti tiesībaizsardzības nolūkos (2016. gada IPL 60. A pants). Ja saziņas datus iegūst valsts drošības nolūkos, atļauju var piešķirt IPK vai, alternatīvi, norīkots attiecīgās publiskās iestādes vecākais ierēdnis (sk. 2016. gada IPL 61. un 61.A pantu un 203. apsvērumu).

(253) ANO īpašais referents jautājumos par privātumu ļoti atzinīgi novērtēja tieslietu komisāru posteņa izveidi ar 2016. gada IPL, jo "visi sensitīvākie vai traucējošākie novērošanas pieprasījumi ir jāapstiprina gan kabineta ministram, gan izmeklēšanas pilnvaru komisāra birojam". Jo īpaši viņš uzsvēra, ka "šis pārskatīšanas tiesā elements [izmantojot IPK lomu], ko atbalsta pieredzējušu inspektoru un tehnoloģiju ekspertu komanda ar labākiem resursiem, ir viena no nozīmīgākajām jaunajām garantijām, kas ieviestas ar IPL", aizstājot iepriekš sadrumstaloto pārraudzības iestāžu sistēmu un papildinot parlamenta Izlūkošanas un drošības komitejas un Izmeklēšanas pilnvaru tribunāla lomu" ([458]).

(254) Turklāt IPK ir pilnvaras veikt *ex post* pārraudzību ([459]), tai skaitā ar revīzijas, pārbaudes un izmeklēšanas palīdzību, izmeklēšanas pilnvaru izmantojumam saskaņā ar 2016. gada IPL un dažām citām pilnvarām un funkcijām, kas paredzētas attiecīgajos tiesību aktos ([460]). Šādas *ex post* pārraudzības rezultāti ir iekļauti ziņojumā, kas IPK ir jāsagatavo katru gadu un jāprezentē premjerministram ([461]), un tas jāpublicē un jāiesniedz parlamentā ([462]). Ziņojumā tiek ietverta būtiskā statistika un informācija par izmeklēšanas pilnvaru izmantojumu izlūkošanas aģentūrās un tiesībaizsardzības iestādēs, kā arī par garantiju izmantošanu attiecībā uz priekšmetiem, uz kuriem attiecas advokāta un klienta saziņas konfidencialitāte, konfidenciālu žurnālistikas materiālu un žurnālistikas informācijas avotiem, informācija par veiktajiem pasākumiem un operatīvie nolūki, kas izmantoti saistībā ar masveida pilnvaru orderiem. Visbeidzot, IPKB gada pārskatā norādīts, kurās jomās ieteikumi sniegti publiskajām iestādēm un kā tie risināti ([463]).

(255) Saskaņā ar 2016. gada IPL 231. pantu, ja IPK rīcībā nonāk informācija par jebkādu būtisku kļūdu, ko publiskās iestādes pieļāvušas, īstenojot savas izmeklēšanas pilnvaras, tam jāinformē attiecīgā persona, ja tas uzskata, ka kļūda ir nopietna un sabiedrības interesēs ir informēt personu ([464]). Jo īpaši 2016. gada IPL 231. pantā ir noteikts, ka, informējot personu par kļūdu, IPK jāsniedz informācija par visām tiesībām, ar kurām šī persona var vērsties Izmeklēšanas pilnvaru tribunālā, un jāsniedz tāda informācija, kuru komisārs uzskata par nepieciešamu šo tiesību īstenošanai, un izpaušana ir sabiedrības interesēs ([465]).

([458]) Īpašā referenta jautājumos par privātumu misijas beigu paziņojums, kas sniegts, beidzoties viņa misijai Lielbritānijas un Ziemeļīrijas Apvienotajā Karalistē (sk. 281. zemsvītras piezīmi).

([459]) 2016. gada IPL 229. pants. Tieslietu komisāra izmeklēšanas un informācijas pilnvaras ir noteiktas 2016. gada IPL 235. pantā.

([460]) Tas ietver novērošanas pasākumus saskaņā ar 2016. gada IPRL, funkciju izpildi saskaņā ar 1997. gada Policijas likuma 3. daļu (atļauja rīkoties attiecībā uz īpašumu) un ministra pildītās funkcijas saskaņā ar 1994. gada Izlūkdienestu likuma 5.–7. pantu (atļauj iejaukšanos bezvadu telegrāfā, iekļūšanu īpašumā un tā aizskārumu, 2000. gada IPL 229. pants).

([461]) 2016. gada IPL 230. pants. IPK var arī pēc savas iniciatīvas ziņot premjerministram par jebkuru jautājumu, kas saistīts ar viņa funkcijām. IPK pēc premjerministra lūguma arī atskaitās viņam, un premjerministrs var uzdot IPK pārskatīt jebkuru izlūkdienestu funkciju.

([462]) Dažas daļas var tikt izslēgtas, ja to publicēšana būtu pretrunā valsts drošības interesēm.

([463]) Piemēram, IPKB 2019. gada pārskatā (6.38. punkts) ir minēts, ka MI5 tika ieteikts mainīt savu masveida personas datu kopu (BPD) glabāšanas politiku, jo vajadzētu izmantot pieeju, kurā tiktu ņemts vērā visu BPD lauku un katra BPD lauka glabāšanas samērīgums. 2018. gada beigās IPKB nebija drošs, ka šis ieteikums tiek ievērots, un 2019. gada pārskatā paskaidrots, ka MI5 tagad ievieš jaunu procedūru šīs prasības izpildei. 2019. gada pārskatā (8.22. punkts) arī minēts, ka *GHCQ* sniegta virkne ieteikumu attiecībā uz reģistru uzskaiti par viņu vaicājumu par masveida datiem samērīgumu. Pārskats apstiprina, ka šajā jomā 2018. gada beigās ir veikti uzlabojumi. Izmeklēšanas pilnvaru komisāra biroja 2019. gada pārskats ir pieejams vietnē https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Turklāt katras publiskas iestādes pārbaudes, ko veic IPKB, noslēgumā tiek sagatavots ziņojums, kuru iesniedz iestādei un kurā ir ietverti jebkādi ieteikumi, kas izriet no minētās pārbaudes. Pēc tam IPKB katru nākamo pārbaudi sāk, pārskatot jebkādus iepriekšējos pēdējās pārbaudes ieteikumus, un jaunajā pārbaudes ziņojumā atspoguļo, vai iepriekšējie ieteikumi ir ņemti vērā vai tiek virzīti tālāk.

([464]) Kļūda uzskatāma par "nopietnu", ja komisārs uzskata, ka tā ir radījusi būtisku kaitējumu vai aizskārumu attiecīgajai personai (2016. gada IPL 231. panta 2. punkts). 2018. gadā ziņots par 22 kļūdām, no kurām astoņas tika uzskatītas par nopietnām, un to rezultātā tika sniegta informācija skartajai personai. Sk. izmeklēšanas pilnvaru komisāra biroja 2018. gada pārskata C pielikumu (sk. https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). 2019. gadā 14 kļūdas tika uzskatītas par nopietnām. Sk. izmeklēšanas pilnvaru komisāra biroja 2019. gada pārskata C pielikumu, sk. 463. zemsvītras piezīmi.

([465]) 2016. gada IPL 231. pantā noteikts, ka, informējot personu par kļūdu, IPK ir jāsniedz tāda informācija, ko komisārs uzskata par nepieciešamu šo tiesību īstenošanai, jo īpaši ņemot vērā to, ciktāl informācijas izpaušana būtu pretrunā ar sabiedrības interesēm vai kaitētu smagu noziegumu novēršanai vai atklāšanai, Apvienotās Karalistes ekonomiskajai labklājībai vai jebkura izlūkdienesta funkciju izpildes nepārtrauktībai.

3.3.3.3. Izlūkdienestu parlamentārā pārraudzība

(256) Izlūkošanas un drošības komitejas (IDK) veiktās parlamentārās pārraudzības likumīgais pamats ir 2013. gada Tiesiskuma un drošības likums (2013. gada TDL) ([466]). Ar šo likumu IDK ir izveidota kā Apvienotās Karalistes parlamenta komiteja. Kopš 2013. gada IDK ir piešķirtas lielākas pilnvaras, tostarp drošības dienestu operatīvās darbības pārraudzība. Saskaņā ar 2013. gada TDL 2. pantu IDK uzdevums ir pārraudzīt valsts drošības dienestu izdevumus, pārvaldību, politiku un darbību. 2013. gada TDL paredz, ka IDK var veikt operatīvo jautājumu izmeklēšanu, ja tie nav saistīti ar tobrīd notiekošajām operācijām ([467]). Saprašanās memorandā, par kuru vienojās premjerministrs un IDK ([468]), ir sīki izklāstīti elementi, kas jāņem vērā, apsverot, vai darbība nav saistīta ar kādu notiekošu operāciju ([469]). Premjerministrs var arī lūgt IDK izmeklēt notiekošās operācijas, un tā var pārskatīt aģentūru brīvprātīgi sniegto informāciju.

(257) Saskaņā ar 2013. gada TDL 1. pielikumu IDK var lūgt jebkuram no trīs izlūkdienestiem, lai tā vadītājs sniedz jebkādu informāciju. Aģentūrai šāda informācija ir jādara pieejama, ja vien ministrs to neaptur ar veto ([470]). Saskaņā ar Apvienotās Karalistes iestāžu sniegtajiem paskaidrojumiem praksē IDK tiek atteikts sniegt ļoti maz informācijas ([471]).

(258) IDK sastāv no locekļiem, kas pieder pie kādas no parlamenta palātām un ko pēc apspriešanās ar opozīcijas līderi ieceļ premjerministrs ([472]). IDK ir jāsagatavo gada pārskats parlamentam par tās funkciju izpildi, kā arī citi ziņojumi, ko tā uzskata par lietderīgiem ([473]). Turklāt IDK ir tiesības ik pēc trim mēnešiem saņemt sarakstu ar operatīvajiem nolūkiem, kas tiek izmantots, lai pārbaudītu masveidā iegūto materiālu ([474]). Izmeklēšanas pilnvaru komisāra veikto izmeklēšanu, pārbaužu vai revīziju kopijas premjerministrs nosūta IDK, ja ziņojumā aplūkotais jautājums attiecas uz likumā noteikto komitejas kompetenci ([475]). Visbeidzot, komiteja var lūgt IPK veikt izmeklēšanu, un komisāram jāinformē IDK par lēmumu veikt šādu izmeklēšanu ([476]).

(259) IDK arī sniedza atzinumu par 2016. gada IPL projektu, kā rezultātā tika izdarīti vairāki grozījumi, kas tagad ir atspoguļoti 2016. gada IPL ([477]). IDK jo īpaši ieteica stiprināt privātuma aizsardzību, ieviešot privātuma aizsardzības

([466]) Kā paskaidrojušas Apvienotās Karalistes iestādes, ar TDL IDK kompetence tika paplašināta, iekļaujot tajā funkciju pārraudzīt izlūkdienestu kopienu ārpus trijām aģentūrām un ļaujot retrospektīvi pārraudzīt aģentūru operatīvo darbību jautājumos, kas skar būtiskas valsts intereses.

([467]) 2013. gada TDL 2. pants.

([468]) Saprašanās memorands starp premjerministru un IDK, pieejams vietnē http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.

([469]) Saprašanās memorands starp premjerministru un IDK, 14. punkts, sk. 468. zemsvītras piezīmi.

([470]) Ministrs var uzlikt veto informācijas izpaušanai tikai divu iemeslu dēļ: ja informācija ir sensitīva un valsts drošības interesēs to nedrīkst izpaust IDK; ja tā ir tāda informācija, ka gadījumā, ja ministram to pieprasītu iesniegt Pārstāvju palātas īpašajai nozaru komitejai, ministrs uzskatītu (ne tikai valsts drošības apsvērumu dēļ) par pareizu to nedarīt (2013. gada TDL 1. pielikuma 4. punkta 2. apakšpunkts).

([471]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, H iedaļa "Valsts drošība", 43. lpp., sk. 31. zemsvītras piezīmi.

([472]) 2013. gada TDL 1. pants. Ministri nav tiesīgi kļūt par locekļiem. Locekļi ieņem savu amatu IDK uz tā parlamenta pilnvaru laiku, kura laikā viņi ir iecelti. Viņus var atbrīvot no amata ar tās palātas rezolūciju, kura tos iecēlusi, vai ja viņi vairs nav deputāti, vai ja viņi kļūst par ministriem. Loceklis var arī atkāpties no amata.

([473]) Komitejas ziņojumi un pārskati ir pieejami tiešsaistē vietnē https://isc.independent.gov.uk/publications/. 2015. gadā IDK publicēja ziņojumu "Privātums un drošība: mūsdienīgs un pārredzams tiesiskais regulējums" (sk.: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), kurā tā vērtēja tiesisko regulējumu attiecībā uz izlūkošanas aģentūru izmantotajām uzraudzības metodēm un nāca klajā ar vairākiem ieteikumiem, kas pēc tam tika izskatīti un iekļauti Izmeklēšanas pilnvaru likumprojektā, kurš kļuva par likumu – 2016. gada IPL. Valdības atbilde uz Privātuma un drošības ziņojumu ir pieejama vietnē https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

([474]) 2016. gada IPL 142., 161. un 183. pants.

([475]) 2016. gada IPL 234. pants.

([476]) 2016. gada IPL 236. pants.

([477]) Parlamenta Izlūkošanas un drošības komitejas ziņojums par Izmeklēšanas pilnvaru likumprojektu pieejams vietnē https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

kopumu, kas attiecas uz visām izmeklēšanas pilnvarām ([478]). Tā arī ierosināja izmaiņas ierosinātajās iespējās attiecībā uz iejaukšanos iekārtās, BPD un saziņas datiem un pieprasīja citus īpašus grozījumus, lai stiprinātu ierobežojumus un garantijas izmeklēšanas pilnvaru izmantošanā ([479]).

3.3.4. *Tiesiskās aizsardzības līdzekļi*

(260) Attiecībā uz valdības piekļuvi valsts drošības nolūkiem datu subjektiem īpaši jābūt iespējai celt prasību neatkarīgā un objektīvā tiesā, lai gūtu piekļuvi saviem personas datiem vai panāktu šādu datu labošanu vai dzēšanu ([480]). Šādai tiesu iestādei jo īpaši jābūt pilnvarām pieņemt saistošus lēmumus par izlūkdienestiem ([481]). Apvienotajā Karalistē, kā paskaidrots 261.–271. apsvērumā, vairākas tiesiskās aizsardzības iespējas tiesā sniedz datu subjektiem iespēju izmantot un saņemt šādus tiesiskās aizsardzības līdzekļus.

3.3.4.1. Tiesiskās aizsardzības mehānismi, kas pieejami saskaņā ar DAL 4. daļu

(261) Saskaņā ar 2018. gada DAL 165. pantu datu subjektam ir tiesības iesniegt sūdzību informācijas komisāram, ja datu subjekts uzskata, ka attiecībā uz viņa personas datiem ir pārkāpta 2018. gada DAL 4. daļa. Informācijas komisāram ir tiesības novērtēt pārziņa un apstrādātāja atbilstību 2018. gada DAL, pieprasot viņiem veikt nepieciešamos pasākumus. Turklāt saskaņā ar 2018. gada DAL 4. daļu personām ir tiesības vērsties Augstajā tiesā (Skotijā – "Court of Session"), lai saņemtu rīkojumu, ar ko pārzinim uzdod ievērot tiesības piekļūt datiem ([482]), iebilst pret apstrādi ([483]) un labot vai dzēst datus ([484]).

(262) Personām ir tiesības arī pieprasīt kompensāciju par kaitējumu, kas nodarīts tādēļ, ka pārzinis vai apstrādātājs pārkāpis 2018. gada DAL 4. daļas prasības ([485]). Kaitējums ietver gan finansiālus zaudējumus, gan kaitējumu, kas nav saistīts ar finansiāliem zaudējumiem, piemēram, spriedzi ([486]).

3.3.4.2. Tiesiskās aizsardzības mehānismi, kas pieejami saskaņā ar 2016. gada IPL

(263) Personas var saņemt kompensāciju par 2016. gada IPL pārkāpumiem, vēršoties Izmeklēšanas pilnvaru tribunālā.

(264) Izmeklēšanas pilnvaru tribunāls izveidots saskaņā ar 2000. gada IPRL, un tas ir neatkarīgs no izpildvaras ([487]). Saskaņā ar 2000. gada IPRL 65. pantu tribunāla locekļus uz pieciem gadiem amatā ieceļ Viņas Majestāte. Tribunāla locekli no amata var atbrīvot Viņas Majestāte, atbildot uz uzrunu ([488]) no abām parlamenta palātām ([489]).

([478]) Šie vispārējie pienākumi saistībā ar privātumu tagad ir noteikti 2016. gada IPL 2. panta 2. punktā, kas paredz, ka publiskajai iestādei, kas rīkojas saskaņā ar 2016. gada IPL, ir jāņem vērā, vai mērķi, ko vēlas sasniegt ar orderi, pilnvarojumu vai paziņojumu varētu pamatoti panākt ar citiem mazāk traucējošiem līdzekļiem, vai aizsardzības līmenis, kas jāpiemēro attiecībā uz informācijas iegūšanu, pamatojoties uz orderi, pilnvarojumu vai paziņojumu, ir augstāks šīs informācijas īpašās sensitivitātes dēļ, sabiedrības intereses telesakaru sistēmu un pasta pakalpojumu integritātes un drošības jomā, kā arī visi citi sabiedrības interešu aspekti privātuma aizsardzībā.

([479]) Piemēram, pēc IDK pieprasījuma dienu skaits, līdz kuram tieslietu komisāram ir jāapstiprina "steidzams" orderis, ir samazināts no piecām līdz trim darba dienām, un IDK tika piešķirtas pilnvaras nodot lietas izmeklēšanas pilnvaru komisāram izmeklēšanas nolūkiem.

([480]) *Schrems II*, 194. punkts.

([481]) *Schrems II*, 197. punkts.

([482]) 2018. gada DAL 94. panta 11. punkts.

([483]) 2018. gada DAL 99. panta 4. punkts.

([484]) 2018. gada DAL 100. panta 1. punkts.

([485]) 2018. gada DAL 169. pants, kas ļauj prasību iesniegt "personai, kurai nodarīts kaitējums datu aizsardzības tiesību aktu prasību pārkāpuma dēļ". Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju praksē prasījums vai sūdzība pret izlūkdienestiem, visticamāk, tiktu iesniegta Izmeklēšanas pilnvaru tribunālam, kuram ir plaša jurisdikcija, kas spēj noteikt kompensāciju / kaitējuma atlīdzību un kur prasījuma iesniegšana ir bez maksas.

([486]) 2018. gada DAL 169. panta 5. punkts.

([487]) Saskaņā ar 2000. gada IPRL 3. pielikumu locekļiem jābūt noteiktai tiesu pieredzei un viņiem ir tiesības tikt atkārtoti ieceltiem.

([488]) "Uzruna" ir parlamentam iesniegts priekšlikums, kura mērķis ir iepazīstināt monarhu ar parlamenta viedokli par kādu konkrētu jautājumu.

([489]) 2000. gada IPRL 3. pielikuma 1. punkta 5. apakšpunkts.

(265) Saskaņā ar 2000. gada IPRL 65. pantu tribunāls ir piemērota tiesu iestāde jebkuras tādas personas sūdzībai, kura cietusi sakarā ar rīcību, kas ietilpst 2016. gada IPL, 2000. gada IPRL tvērumā, vai jebkuras izlūkdienestu rīcības rezultātā ([490]).

(266) Lai iesniegtu prasību Izmeklēšanas pilnvaru tribunālā ("prasības attiecībā uz tiesībām vērsties tribunālā"), saskaņā ar 2000. gada IPRL 65. pantu personai ir jābūt pārliecībai ([491]), ka izlūkdienests ir rīkojies attiecībā uz viņu, jebkuru tās īpašumu, jebkuru tai vai tās nosūtītu saziņu, vai tai paredzētu saziņu, vai tās jebkuru pasta pakalpojumu, telesakaru pakalpojumu vai telesakaru sistēmu izmantojumu" ([492]). Turklāt sūdzības iesniedzējam ir jābūt pārliecinātam, ka rīcība ir notikusi "apstrīdamos apstākļos" ([493]) vai "to ir veikuši izlūkdienesti vai tā ir notikusi viņu uzdevumā" ([494]). Tā kā šis "pārliecības" standarts ir interpretēts salīdzinoši plaši ([495]), prasības attiecībā uz tiesībām vērsties tribunālā ir relatīvi zemas.

(267) Ja Izmeklēšanas pilnvaru tribunāls izskata tam iesniegtu sūdzību, tribunāla pienākums ir izmeklēt, vai personas, par kurām sūdzībā ir izvirzīti kādi apgalvojumi, ir rīkojušās attiecībā uz sūdzības iesniedzēju, kā arī izmeklēt iestādi, kas, iespējams, varētu būt iesaistījusies pārkāpumos, un to, vai apgalvotā rīcība vispār ir notikusi ([496]). Ja tribunāls izskata kādu lietu, tam, pieņemot nolēmumu šajā lietā, ir jāpiemēro tie paši principi, kas tiktu piemēroti tiesā, izskatot pieteikumu par pārskatīšanu tiesā ([497]). Turklāt orderu vai paziņojumu adresātiem saskaņā ar 2016. gada IPL, kā arī visām pārējām personām, kuras ieņem amatu valsts uzdevumā, kuras strādā policijas vienībā vai pie policijas izmeklēšanas un pārbaudes komisāra, ir pienākums izpaust vai iesniegt šim tribunālam jebkādus tādus dokumentus un informāciju, ko tribunāls var pieprasīt tā jurisdikcijas īstenošanas nolūkos ([498]).

(268) Izmeklēšanas pilnvaru tribunālam ir jāinformē sūdzības iesniedzējs par to, vai ir pieņemts tam labvēlīgs lēmums vai nē ([499]). Saskaņā ar 2000. gada IPRL 67. panta 6. un 7. punktu tribunālam ir pilnvaras izdot pagaidu rīkojumus un paredzēt atlīdzināšanu vai izdot citu rīkojumu, ko tas uzskata par piemērotu. Tas var ietvert rīkojumu par jebkura ordera vai pilnvarojuma atcelšanu vai atsaukšanu, kā arī rīkojumu, ar ko pieprasa iznīcināt jebkādus informācijas

([490]) 2000. gada IPRL 65. panta 5. punkts.

([491]) Attiecībā uz "pārliecības" standartu sk. lietu *Human Rights Watch v Secretary of State* [2016], UKIPTrib15_165-CH, 41. punkts. Šajā gadījumā Izmeklēšanas pilnvaru tribunāls, atsaucoties uz Eiropas Cilvēktiesību tiesas judikatūru, sprieda, ka atbilstošais kritērijs attiecībā uz pārliecību, ka rīcību, uz kuru attiecas 2000. gada IPRL 68. panta 5. punkts, ir veicis kāds no izlūkdienestiem vai tā veikta tā vārdā, ir tas, vai šādai pārliecībai ir pamats, persona var apgalvot, ka ir cietusi no tāda pārkāpuma, ko izraisījusi jau tikai pati slepenu pasākumu vai tiesību aktu, kas atļauj slepenus pasākumus, esamība, tikai tad, ja tā spēj pierādīt, ka tās personīgās situācijas dēļ viņai potenciāli draud šādu pasākumu veikšana pret to.

([492]) 2000. gada IPRL 65. panta 4. punkta a) apakšpunkts.

([493]) Šādi apstākļi attiecas uz publisko iestāžu rīcību, kas notiek uz pilnvarojuma pamata (piemēram, orderis, atļauja/paziņojums saziņas datu iegūšanai utt.), vai ja apstākļi ir tādi, ka (neatkarīgi no tā, vai šāds pilnvarojums ir vai nav) nebūtu bijis lietderīgi rīkoties bez šāda pilnvarojuma vai vismaz pienācīgi neizvērtējot, vai šāds pilnvarojums būtu jāpieprasa. Tiek uzskatīts, ka rīcība, ko atļāvis tiesas komisārs, ir notikusi apstrīdamos apstākļos (2000. gada IPRL 65. panta 7.ZA punkts), savukārt citas rīcības, kas notiek ar tiesu iestādes amatā esošas personas atļauju, netiek uzskatītas par tādām, kas notikušas apstrīdamos apstākļos (2000. gada IPRL 65. panta 7. un 8. punkts).

([494]) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju, no zemā sliekšņa sūdzības iesniegšanai izriet, ka tribunāla izmeklēšanas gaitā bieži vien tiek konstatēts, ka sūdzības iesniedzējs faktiski nekad nav bijis pakļauts publiskās iestādes veiktai izmeklēšanai. Izmeklēšanas pilnvaru tribunāla jaunākajā statistikas pārskatā norādīts, ka 2016. gadā tribunāls saņēmis 209 sūdzības, no kurām 52 % tika atzītas par nepamatotām vai kaitnieciskām, bet 25 % noslēdzās "bez rezultāta". Apvienotās Karalistes iestādes paskaidroja, ka tas nozīmē, ka attiecībā uz sūdzības iesniedzēju vai nu netika izmantotas slēptas darbības vai pilnvaras, vai arī tika izmantotas slēptas metodes, taču tribunāls atzinis šīs darbības par likumīgām. Līdztekus tam 11 % sūdzību tika atzītas par nepiekritīgām, atsauktām vai spēkā neesošām, 5 % gadījumu tika konstatēts nokavējums, bet 7 % sūdzību tika izlemtas par labu sūdzības iesniedzējam. Izmeklēšanas pilnvaru tribunāla 2016. gada statistikas pārskats, pieejams vietnē https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([495]) Sk. spriedumu lietā *Human Rights Watch v Secretary of State*, [2016] UKIPTrib15_165-CH. Šajā lietā Izmeklēšanas pilnvaru tribunāls, atsaucoties uz Eiropas Cilvēktiesību tiesas judikatūru, uzskatīja, ka atbilstošais kritērijs attiecībā uz pārliecību, ka rīcību, uz kuru attiecas 2000. gada IPRL 68. panta 5. punkts, ir veicis kāds no izlūkdienestiem vai tā veikta tā vārdā, ir tas, vai šādai pārliecībai ir pamats, tostarp persona var apgalvot, ka ir cietusi no tāda pārkāpuma, ko izraisījusi jau tikai pati slepenu pasākumu vai tiesību aktu, kas atļauj slepenus pasākumus, esamība, tikai tad, ja tā spēj pierādīt, ka tās personīgās situācijas dēļ viņai potenciāli draud šādu pasākumu veikšana pret to (sk. spriedumu lietā *Human Rights Watch v Secretary of State*, 41. punkts).

([496]) 2000. gada IPRL 67. panta 3. punkts.

([497]) 2000. gada IPRL 67. panta 2. punkts.

([498]) 2000. gada IPRL 68. panta 6.–7. punkts.

([499]) 2000. gada IPRL 68. panta 4. punkts.

ierakstus, kas iegūti, izmantojot ar orderi, pilnvarojumu vai paziņojumu piešķirtās pilnvaras, vai citādi ir kādas publiskās iestādes rīcībā saistībā ar jebkuru personu ([500]). Saskaņā ar 2000. gada IPRL 67.A pantu tribunāla nolēmumu var pārsūdzēt, ja tribunāls vai attiecīgā apelācijas tiesa ir to atļāvusi.

(269) Visbeidzot, ir vērts minēt, ka Izmeklēšanas pilnvaru tribunāla loma vairākkārt ir apspriesta saistībā ar tiesvedību Eiropas Cilvēktiesību tiesā, īpaši lietā *Kennedy v. the United Kingdom* ([501]) un nesenajā lietā *Big Brother Watch and others v. United Kingdom* ([502]), kur Tiesa paziņoja, ka "IPT piedāvāja spēcīgu tiesiskās aizsardzības līdzekli ikvienam, kam bija aizdomas, ka tā saziņu pārtvēruši izlūkdienesti" ([503]).

3.3.4.3. Citi pieejamie tiesiskās aizsardzības mehānismi

(270) Kā paskaidrots 109.–111. apsvērumā, valsts drošības jomā ir pieejami arī tiesiskās aizsardzības līdzekļi saskaņā ar 1998. gada Cilvēktiesību likumu, kā arī Eiropas Cilvēktiesību tiesā ([504]). 2000. gada IPRL 65. panta 2. punkts paredz Izmeklēšanas pilnvaru tribunāla ekskluzīvu jurisdikciju attiecībā uz visām Cilvēktiesību likuma prasībām, kas saistītas ar izlūkošanas aģentūrām ([505]). Tas, kā norādījusi Augstā tiesa, nozīmē, ka "jautājumu par to, vai saskaņā ar konkrētās lietas faktiem ir noticis Cilvēktiesību likuma pārkāpums, principā var izvirzīt un izskatīt neatkarīga tiesa, kurai ir pieejami visi attiecīgie materiāli, tostarp slepeni materiāli. (..) Šajā kontekstā mēs arī paturam prātā, ka tagad ir paredzēta iespēja pārsūdzēt tribunāla lēmumu attiecīgajā apelācijas tiesā (Anglijā un Velsā tā būtu Apelācijas tiesa); un ka Augstākā tiesa nesen nolēma, ka tribunāls principā ir pakļauts tiesas kontrolei: sk. *R (Privacy International) v Investigatory Powers Tribunal* [2019], UKSC 22; [2019] 2 WLR 1219" ([506]).

(271) No iepriekš minētā izriet, ka tad, ja Apvienotās Karalistes tiesībaizsardzības vai valsts drošības iestādes piekļūst personas datiem, uz kuriem attiecas šis lēmums, šādu piekļuvi reglamentē tiesību akti, kuros izklāstīti nosacījumi, saskaņā ar kuriem šāda piekļuve var notikt, un nodrošina, ka piekļuve un turpmāka datu izmantošana aprobežojas ar to, kas ir nepieciešams un samērīgs izvirzītajiem tiesībaizsardzības vai valsts drošības mērķiem. Turklāt šādai piekļuvei vairumā gadījumu ir vajadzīga iepriekšēja tiesu iestādes atļauja, apstiprinot orderi vai pierādījumu sniegšanas orderi, un jebkurā gadījumā neatkarīga pārraudzība. Pēc tam, kad publiskās iestādes ir piekļuvušas datiem, uz to apstrādi, tostarp tālāku apmaiņu un tālāku nosūtīšanu, attiecas konkrētas datu aizsardzības garantijas saskaņā ar 2018. gada DAL 3. daļu, atspoguļojot Direktīvā (ES) 2016/680 paredzētās garantijas tiesībaizsardzības iestāžu veiktajai apstrādei un 2018. gada DAL 4. daļu izlūkošanas aģentūru veiktajai apstrādei. Visbeidzot, datu subjektiem šajā jomā ir efektīva tiesību aizsardzība administratīvā kārtā vai tiesā, tostarp piekļuve saviem datiem vai šādu datu labošanas vai dzēšanas tiesības.

(272) Ņemot vērā šādu nosacījumu, ierobežojumu un garantiju nozīmi šajā lēmumā, Komisija cieši uzraudzīs to Apvienotās Karalistes noteikumu piemērošanu un interpretāciju, ar ko paredz valdības piekļuvi datiem. Tas ietvers attiecīgās norises likumdošanas, regulatīvajā un judikatūras jomā, kā arī IKB un citu pārraudzības iestāžu

([500]) Šādu pilnvaru piemērošanas piemērs ir lieta *Liberty & Others v the Security Service, SIS, GCHQ* [2015], UKIP Trib 13_77-H_2. Tribunāls pieņēma lēmumu par labu diviem sūdzības iesniedzējiem, jo vienā gadījumā viņu saziņa tika glabāta, pārsniedzot noteiktos ierobežojumus, bet otrā tāpēc, ka netika ievērota pārbaudes procedūra, kā noteikts *GCHQ* iekšējos noteikumos. Pirmajā gadījumā Tiesa lika izlūkdienestiem iznīcināt saziņu, kas tika glabāta ilgāk par attiecīgo termiņu. Otrajā gadījumā rīkojums par iznīcināšanu netika izsniegts, jo saziņa netika glabāta.

([501]) *Kennedy*, sk. 129. zemsvītras piezīmi.

([502]) Eiropas Cilvēktiesību tiesa , *Big Brother Watch and others v United Kingdom* (sk. iepriekš 268. zemsvītras piezīmi), 413.–415. punkts.

([503]) Eiropas Cilvēktiesību tiesa, *Big Brother Watch*, 425. punkts.

([504]) Kā ilustrēts, piemēram, Eiropas Cilvēktiesību tiesas virspalātas nesen pieņemtajā spriedumā lietā *Big Brother Watch and others v United Kingdom* (sk. iepriekš 279. zemsvītras piezīmi), tas ļauj īstenot efektīvu tiesas kontroli (līdzīgu tai, kurai pakļautas ES dalībvalstis), kuru veic starptautiska tiesa un ar kuru pārbauda pamattiesību ievērošanu publiskās iestādēs attiecībā uz piekļuvi personas datiem. Turklāt Eiropas Cilvēktiesību tiesas spriedumu izpildi īpaši uzrauga Eiropas Padome.

([505]) Lietā *Belhaj & others* [2017], UKSC 3, materiāla, uz ko attiecas advokāta un klienta saziņas konfidencialitāte, pārtveršanas nelikumīguma noteikšana tieši balstījās uz ECTK 8. pantu (sk. 11. punktu).

([506]) Augstā tiesa, *Liberty* [2019], EWHC 2057 (Admin), 170. punkts.

pasākumus šajā jomā. Īpaša uzmanība tiks pievērsta arī tam, kā Apvienotā Karaliste izpilde attiecīgos Eiropas Cilvēktiesību tiesas spriedumus, ietverot tādos rīcības plānos un rīcības ziņojumos noteiktos pasākumus, kas iesniegti Ministru komitejai saistībā ar tiesas nolēmumu ievērošanas uzraudzību.

4. **SECINĀJUMS**

(273) Komisija uzskata, ka Apvienotās Karalistes VDAR un 2018. gada DAL nodrošina no Eiropas Savienības nosūtīto personas datu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 garantētajam līmenim.

(274) Komisija arī uzskata, ka kopumā pārraudzības mehānismi un tiesiskās aizsardzības līdzekļi, kas paredzēti Apvienotās Karalistes tiesību aktos, ļauj apzināt pārkāpumus un piemērot praksē attiecīgus sodus, kā arī sniedz datu subjektam tiesisko aizsardzību, ļaujot piekļūt viņa personas datiem un galu galā – labot vai dzēst šādus datus.

(275) Visbeidzot, pamatojoties uz pieejamo informāciju par Apvienotās Karalistes tiesību sistēmu, Komisija uzskata, ka jebkurš ierobežojums to personu pamattiesībām, kuru personas datus Apvienotās Karalistes publiskās iestādes sabiedrības interesēs nosūta no Eiropas Savienības uz Apvienoto Karalisti, jo īpaši tiesībaizsardzības un valsts drošības nolūkos, būs tikai tāds, kas ir absolūti nepieciešams attiecīgā leģitīmā mērķa sasniegšanai, un ka pastāv efektīva tiesiskā aizsardzība pret šādu ierobežošanu.

(276) Tādēļ, ņemot vērā šā lēmuma konstatējumus, būtu jāpieņem lēmums, ka Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni Regulas (ES) 2016/679 45. panta nozīmē, kas interpretēts, ņemot vērā Eiropas Savienības Pamattiesību hartu.

(277) Šis secinājums ir balstīts gan uz attiecīgo Apvienotās Karalistes iekšējo režīmu, gan tās starptautiskajām saistībām, jo īpaši Eiropas Cilvēktiesību konvencijas ievērošanu un pakļaušanos Eiropas Cilvēktiesību tiesas jurisdikcijai. Tādēļ šā lēmuma pamatā esošajā novērtējumā šādu starptautisku saistību pastāvīga ievērošana ir īpaši svarīgs elements.

5. **ŠĀ LĒMUMA SEKAS UN DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA**

(278) Dalībvalstīm un to struktūrām ir pienākums veikt nepieciešamos pasākumus, lai izpildītu Savienības iestāžu tiesību aktus, jo tie tiek uzskatīti par likumīgiem un attiecīgi paredz juridiskās sekas līdz brīdim, kad tie zaudē spēku, tiek atcelti, anulēti saskaņā ar prasību atcelt tiesību aktu vai pasludināti par spēkā neesošiem pēc lūguma sniegt prejudiciālu nolēmumu vai iebildes par prettiesiskumu.

(279) Tādējādi lēmums par aizsardzības līmeņa pietiekamību, ko Komisija pieņēmusi saskaņā ar Regulas (ES) 2016/679 45. panta 3. punktu, ir saistošs visām dalībvalstu struktūrām, kurām tas adresēts, tostarp to neatkarīgajām uzraudzības iestādēm. Konkrēti, šā lēmuma piemērošanas laikā nosūtīšana no pārziņa vai apstrādātāja Eiropas Savienībā pārziņiem vai apstrādātājiem Apvienotajā Karalistē var notikt bez nepieciešamības saņemt jebkādu turpmāku atļauju.

(280) Vienlaikus būtu jāatgādina, ka saskaņā ar Regulas (ES) 2016/679 58. panta 5. punktu un kā Tiesa paskaidrojusi spriedumā *Schrems* lietā ([507]), ja valsts datu aizsardzības iestāde, tostarp pēc sūdzības saņemšanas, apšauba Komisijas lēmuma par aizsardzības līmeņa pietiekamību atbilstību personas pamattiesībām uz privātuma neaizskaramību un datu aizsardzību, tai valsts tiesību aktos ir jānodrošina tiesiskās aizsardzības līdzeklis, kas ļauj celt šādus iebildumus valsts tiesā, kurai var būt pienākums lūgt Tiesai sniegt prejudiciālu nolēmumu ([508]).

([507]) *Schrems*, 65. punkts.

([508]) *Schrems*, 65. punkts: "Šajā ziņā valsts likumdevēja ziņā ir paredzēt tiesiskās aizsardzības līdzekļus, kas valsts uzraudzības iestādei ļauj valstu tiesās izvirzīt iebildes, ko tā uzskata par pamatotām, lai šīs tiesas – ja arī tās piekrīt šīs iestādes šaubām par Komisijas lēmuma spēkā esamību – iesniegtu lūgumu sniegt prejudiciālu nolēmumu šā lēmuma spēkā esamības izvērtēšanas nolūkos."

6. ŠĀ LĒMUMA UZRAUDZĪBA, APTURĒŠANA, ATCELŠANA VAI GROZĪŠANA

(281) Saskaņā ar Regulas (ES) 2016/679 45. panta 4. punktu Komisijai pēc šā lēmuma pieņemšanas pastāvīgi jāuzrauga attiecīgās norises Apvienotajā Karalistē, lai izvērtētu, vai tā joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Šāda uzraudzība šajā gadījumā ir īpaši svarīga, jo Apvienotā Karaliste pārvaldīs, piemēros un īstenos jaunu datu aizsardzības režīmu, uz kuru vairs neattiecas Savienības tiesību akti un kurš varētu attīstīties. Šajā saistībā īpaša uzmanība tiks pievērsta tam, kā Apvienotās Karalistes noteikumi par personas datu nosūtīšanu uz trešām valstīm tiek piemēroti praksē, un tam, kā tas varētu ietekmēt saskaņā ar šo lēmumu nosūtīto datu aizsardzības līmeni, individuālo tiesību izmantošanas efektivitātei, ietverot jebkādas nesenas norises tiesību aktos un praksē saistībā ar šādu tiesību izņēmumiem vai ierobežojumiem (jo īpaši saistībā ar efektīvas imigrācijas kontroles uzturēšanu), kā arī ierobežojumu un garantiju ievērošanai attiecībā uz valdības piekļuvi. Komisija, īstenojot uzraudzību, cita starpā ņems vērā jaunāko judikatūru un IKB un citu neatkarīgu struktūru veikto pārraudzību.

(282) Lai sekmētu šo uzraudzību, Apvienotās Karalistes iestādēm būtu bez kavēšanās jāinformē Komisija par visām būtiskajām Apvienotās Karalistes tiesiskās kārtības izmaiņām, kas ietekmē tiesisko regulējumu, uz kuru attiecas šis lēmums, kā arī par šajā lēmumā novērtētās personas datu apstrādes prakses maiņu gan attiecībā uz pārziņu un apstrādātāju veiktu personas datu apstrādi saskaņā ar Apvienotās Karalistes VDAR, gan attiecībā uz ierobežojumiem un garantijām, ko piemēro publiskām iestādēm nodrošinātai piekļuvei personas datiem. Tam būtu jāietver norises, kas attiecas uz 281. apsvērumā minētajiem elementiem.

(283) Turklāt, lai Komisija varētu efektīvi pildīt savu uzraudzības funkciju, dalībvalstīm būtu jāinformē Komisija par visām būtiskajām darbībām, ko veikušas valstu datu aizsardzības iestādes, jo īpaši attiecībā uz ES datu subjektu vaicājumiem un sūdzībām par personas datu nosūtīšanu no Savienības pārziņiem un apstrādātājiem Apvienotajā Karalistē. Komisiju vajadzētu informēt arī par visām pazīmēm, kas liecina, ka darbības, kuras veic Apvienotās Karalistes publiskās iestādes, kas atbild par noziedzīgu nodarījumu novēršanu, izmeklēšanu vai atklāšanu vai saukšanu pie atbildības par tiem, tostarp jebkādas pārraudzības struktūras, nenodrošina vajadzīgo aizsardzības līmeni.

(284) Ja pieejamā informācija, jo īpaši informācija, kas iegūta, uzraugot šo lēmumu, vai informācija, ko sniedz Apvienotās Karalistes vai dalībvalstu iestādes, atklāj, ka Apvienotās Karalistes nodrošinātais aizsardzības līmenis, iespējams, vairs nav pietiekams, Komisijai par to būtu nekavējoties jāinformē Apvienotās Karalistes kompetentās iestādes un jāpieprasa, lai noteiktā termiņā, kas nav garāks par trim mēnešiem, tiktu veikti attiecīgi pasākumi. Nepieciešamības gadījumā minēto termiņu var pagarināt par noteiktu laiku, ņemot vērā attiecīgās problēmas un/vai veicamo pasākumu būtību. Piemēram, šāda procedūra tiktu izraisīta gadījumos, kad tālāku nosūtīšanu, arī balstoties uz jauniem ministra pieņemtiem noteikumiem par aizsardzības līmeņa pietiekamību vai Apvienotās Karalistes noslēgtiem starptautiskiem nolīgumiem, vairs neveiktu saskaņā ar garantijām, kas nodrošina aizsardzības nepārtrauktību Regulas (ES) 2016/679 44. panta nozīmē.

(285) Ja līdz minētā termiņa beigām Apvienotās Karalistes kompetentās iestādes neveiks minētos pasākumus vai kā citādi apmierinoši neparādīs, ka šā lēmuma pamatā joprojām ir pietiekams aizsardzības līmenis, Komisija uzsāks Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru, lai daļēji vai pilnībā apturētu vai atceltu šo lēmumu.

(286) Alternatīvi Komisija uzsāks šo procedūru, lai grozītu šo lēmumu, jo īpaši piemērojot papildu nosacījumus datu nosūtīšanai vai ierobežojot aizsardzības līmeņa pietiekamības konstatējuma darbības jomu tikai attiecībā uz tādu datu nosūtīšanu, kam joprojām tiek nodrošināts pietiekams aizsardzības līmenis.

(287) Pienācīgi pamatotu nenovēršamu steidzamu iemeslu dēļ Komisija izmantos iespēju saskaņā ar Regulas (ES) 2016/679 93. panta 3. punktā minēto procedūru pieņemt nekavējoties piemērojamus īstenošanas aktus, ar kuriem aptur, atceļ vai groza lēmumu.

7. ŠĀ LĒMUMA DARBĪBAS TERMIŅŠ UN ATJAUNOŠANA

(288) Komisijai jāņem vērā, ka, beidzoties Izstāšanās līgumā paredzētajam pārejas periodam, tiklīdz vairs nepiemēros ES un Apvienotās Karalistes Tirdzniecības un sadarbības nolīguma 782. pantā paredzēto pagaidu noteikumu, Apvienotā Karaliste pārvaldīs, piemēros un īstenos jaunu datu aizsardzības regulējumu salīdzināmā ar to, kas bija spēkā, kad tai bija saistoši ES tiesību akti. Tas jo īpaši var ietvert grozījumus vai izmaiņas šajā lēmumā izvērtētajā datu aizsardzības regulējumā, kā arī citas attiecīgās norises.

(289) Tādēļ ir lietderīgi noteikt, ka šo lēmumu piemēro četrus gadus pēc tā stāšanās spēkā.

(290) Jo īpaši tad, ja informācija, kas iegūta, uzraugot šo lēmumu, liecina, ka konstatējumi par Apvienotās Karalistes nodrošinātā aizsardzības līmeņa pietiekamību joprojām ir faktiski un juridiski pamatoti, Komisijai ne vēlāk kā sešus mēnešus pirms šā lēmuma piemērošanas pārtraukšanas būtu jāsāk šā lēmuma grozīšanas procedūra, principā pagarinot tā darbības termiņu uz vēl četriem gadiem. Jebkurš šāds īstenošanas akts, ar kuru groza šo lēmumu, jāpieņem saskaņā ar Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru. Jebkurš šāds īstenošanas akts, ar kuru groza šo lēmumu, jāpieņem saskaņā ar Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru.

8. **NOSLĒGUMA APSVĒRUMI**

(291) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([509]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(292) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) 2016/679 93. pantu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

1. Apvienotā Karaliste Regulas (ES) 2016/679 45. panta mērķiem nodrošina pietiekamu aizsardzības līmeni tādiem personas datiem, ko Regulas (ES) 2016/679 piemērošanas jomas ietvaros nosūta no Eiropas Savienības uz Apvienoto Karalisti.

2. Šis lēmums neattiecas uz personas datiem, kas nosūtīti Apvienotās Karalistes imigrācijas kontroles vajadzībām vai uz ko citādi attiecas atbrīvojums no konkrētām datu subjektu tiesībām efektīvas imigrācijas kontroles nodrošināšanas vajadzībām saskaņā ar 2018. gada DAL 2. pielikuma 4. punkta 1. apakšpunktu.

2. pants

Lai aizsargātu personas attiecībā uz viņu personas datu apstrādi, ikreiz, kad kompetentās uzraudzības iestādes dalībvalstīs īsteno savas pilnvaras atbilstoši Regulas (ES) 2016/679 58. pantam attiecībā uz datu nosūtīšanu 1. pantā noteiktajā piemērošanas jomā, attiecīgā dalībvalsts nekavējoties informē Komisiju.

3. pants

1. Komisija nepārtraukti uzrauga to, kā tiek piemērots tiesiskais regulējums, kas ir šā lēmuma pamatā, tai skaitā nosacījumi, ar kādiem tiek veikta datu tālāka nosūtīšana, tiek īstenotas individuālās tiesības un Apvienotās Karalistes publiskajām iestādēm ir piekļuve datiem, kuri nosūtīti, balstoties uz šo lēmumu, lai novērtētu, vai Apvienotā Karaliste turpina nodrošināt pietiekamu aizsardzības līmeni 1. panta nozīmē.

2. Dalībvalstis un Komisija informē viena otru par gadījumiem, kad informācijas komisārs vai jebkura cita Apvienotās Karalistes kompetentā iestāde nespēj nodrošināt atbilstību tiesiskajam regulējumam, kas ir šā lēmuma pamatā.

3. Dalībvalstis un Komisija informē viena otru par visām pazīmēm, kas liecina, ka Apvienotās Karalistes publisko iestāžu ierobežojumi personu tiesībām uz viņu personas datu aizsardzību pārsniedz absolūti nepieciešamo vai ka nav efektīvas tiesiskās aizsardzības pret šādu ierobežošanu.

4. Ja Komisija ir saņēmusi norādes, ka vairs netiek nodrošināts pietiekams aizsardzības līmenis, Komisija informē Apvienotās Karalistes kompetentās iestādes un var apturēt, atcelt vai grozīt šo lēmumu.

([509]) Atzinums 14/2021 par Eiropas Komisijas Īstenošanas lēmuma projektu saskaņā ar Regulu (ES) 2016/679 par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, pieejams vietnē https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komisija var apturēt, atcelt vai grozīt šo lēmumu, ja Apvienotās Karalistes valdības nesadarbošanās liedz Komisijai noteikt, vai ir skarts 1. panta 1. punktā ietvertais konstatējums.

4. pants

Šis lēmums zaudē spēku 2025. gada 27. jūnijā, ja vien tā termiņš netiek pagarināts saskaņā ar Direktīvas (ES) 2016/679 93. panta 2. punktā minēto procedūru.

5. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2021. gada 28. jūnijā

Komisijas vārdā –
Komisijas loceklis
Didier REYNDERS