2025/2574

23.12.2025.

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2025/2574

(2025. gada 19. decembris),

ar kuru groza Komisijas Īstenošanas lēmumu (ES) 2021/1772 par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679

(izziņots ar dokumenta numuru C(2025) 8771)

(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) ([1]), un jo īpaši tās 45. panta 3. punktu,

tā kā:

1. IEVADS

(1) Komisijas Īstenošanas lēmumā (ES) 2021/1772 ([2]) ir secināts, ka Regulas (ES) 2016/679 45. panta piemērošanas nolūkā Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni personas datiem, kas no Eiropas Savienības nosūtīti uz Apvienoto Karalisti minētās regulas darbības jomas ietvaros ([3]).

(2) Pieņemot Īstenošanas lēmumu (ES) 2021/1772, Komisija ņēma vērā, ka pēc Līgumā par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes izstāšanos no Eiropas Savienības un Eiropas Atomenerģijas kopienas ([4]) paredzētā pārejas perioda beigām un pēc tam, kad pagaidu noteikums saskaņā ar Tirdzniecības un sadarbības nolīguma starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses ([5]), 782. pantu vairs nav piemērojams, Apvienotā Karaliste pieņemtu, piemērotu un izpildītu jaunu datu aizsardzības režīmu, kas atšķiras no tā, kāds bija spēkā, kad tai bija saistoši Savienības tiesību akti.

(3) Tā kā tas varēja būt saistīts ar grozījumiem datu aizsardzības regulējumā, kas novērtēts Īstenošanas lēmumā (ES) 2021/1772, vai citām attiecīgām norisēm, tika uzskatīts par lietderīgu paredzēt, ka minēto lēmumu piemēros četrus gadus no tā spēkā stāšanās dienas. Tādēļ bija paredzēts, ka Īstenošanas lēmums (ES) 2021/1772 zaudēs spēku 2025. gada 27. jūnijā, ja vien tā darbības termiņu nepagarina saskaņā ar Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru.

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

([2]) Komisijas Īstenošanas lēmums (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 (OV L 360, 11.10.2021., 1. lpp., ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

([3]) Sk. Īstenošanas lēmuma (ES) 2021/1772 1. panta 1. punktu. Saskaņā ar minētā lēmuma 1. panta 2. punktu lēmums neattiecas uz personas datiem, kuri nosūtīti Apvienotās Karalistes imigrācijas kontroles vajadzībām, vai uz kuriem citādi attiecas atbrīvojums no konkrētām datu subjektu tiesībām efektīvas imigrācijas kontroles nodrošināšanas vajadzībām saskaņā ar Apvienotās Karalistes 2018. gada Datu aizsardzības likuma 2. pielikuma 4. punkta 1. apakšpunktu.

([4]) OV C 384 I, 12.11.2019., 1. lpp.

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

(4) Lai lemtu par Īstenošanas lēmuma (ES) 2021/1772 darbības termiņa iespējamu pagarināšanu, Komisijai ir jānovērtē, vai secinājums par to, ka Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni, joprojām ir faktiski un juridiski pamatots, ņemot vērā norises, kas kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas ir notikušas attiecībā uz Regulas (ES) 2016/679 45. panta 2. punktā uzskaitītajiem elementiem.

(5) Konkrēti – 2024. gada 23. oktobrī Apvienotās Karalistes valdība Apvienotās Karalistes parlamentā iesniedza Datu (izmantošanas un piekļuves) likumprojektu ([6]), ar kuru ierosina grozījumus Apvienotās Karalistes Vispārīgajā datu aizsardzības regulā (AK VDAR) un 2018. gada Datu aizsardzības likumā (2018. gada DAL), kas izvērtēti Īstenošanas lēmumā (ES) 2021/1772. Komisija 2025. gada 24. jūnijā pieņēma Īstenošanas lēmumu (ES) 2025/1226 ([7]), ar ko Īstenošanas lēmuma (ES) 2021/1772 darbības termiņu pagarināja par sešiem mēnešiem līdz 2025. gada 27. decembrim. Šis laika ziņā ierobežotais, tehniskais pagarinājums ļāva Komisijai pabeigt novērtējumu par to, vai Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni personas datiem, pamatojoties uz stabilu tiesisko regulējumu, t. i., pēc attiecīgā likumdošanas procesa pabeigšanas ([8]).

(6) Kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas Komisija ir pastāvīgi uzraudzījusi attiecīgās norises Apvienotajā Karalistē ([9]). Saskaņā ar Īstenošanas lēmuma (ES) 2021/1772 281. apsvērumu īpaša uzmanība tika pievērsta tam, kā Apvienotās Karalistes noteikumi par personas datu nosūtīšanu uz trešām valstīm tiek piemēroti praksē, un tam, kā tas varētu ietekmēt saskaņā ar Īstenošanas lēmumu (ES) 2021/1772 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 ņēma vērā jaunāko judikatūru un Informācijas komisāra biroja (*ICO*) un citu neatkarīgu struktūru veikto pārraudzību.

(7) Balstoties uz šo norišu novērtējumu, tostarp AK VDAR un 2018. gada DAL grozījumiem, kas tika ieviesti ar Datu (izmantošanas un piekļuves) aktu, Komisija secina, ka Apvienotā Karaliste turpina nodrošināt pietiekamu aizsardzības līmeni personas datiem, kuri nosūtīti no Eiropas Savienības uz Apvienoto Karalisti Regulas (ES) 2016/679 tvēruma ietvaros.

(8) Kā paskaidrots šā lēmuma 37. apsvērumā, Komisija arī secina, ka, ņemot vērā grozījumus attiecīgajos Apvienotās Karalistes tiesību aktu noteikumos ([10]), vairs nav pamatota tādu personas datu izslēgšana no Īstenošanas lēmuma (ES) 2021/1772 tvēruma, kuri nosūtīti Apvienotās Karalistes imigrācijas kontroles vajadzībām vai uz kuriem 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.

([6]) Pieejams šādā vietnē: https://bills.parliament.uk/bills/3825/news.

([7]) Komisijas Īstenošanas lēmums (ES) 2025/1226 (2025. gada 24. jūnijs), ar ko groza Īstenošanas lēmumu (ES) 2021/1772 par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (OV L, 2025/1226, 26.6.2025., ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) 2025. gada 19. jūnijā tika saņemta karaliskā piekrišana Datu (izmantošanas un piekļuves) aktam.

([9]) Regulas (ES) 2016/679 45. panta 4. punkts.

([10]) Anglijas un Velsas Apelācijas tiesa 2021. gada maijā bija konstatējusi, ka Apvienotās Karalistes Datu aizsardzības likuma 2. pielikuma 4. punkta 1. apakšpunktā tobrīd formulētais imigrācijas atbrīvojums nebija saderīgs ar Apvienotās Karalistes tiesību aktiem, jo likumdošanas instrumentam nebija konkrētu noteikumu, kuros būtu izklāstīti AK VDAR 23. panta 2. punktā uzskaitītie aizsardzības pasākumi. Lai panāktu atbilstību spiedumam, Apvienotās Karalistes valdība pārskatīja imigrācijas atbrīvojumu, pieņemot 2018. gada Datu aizsardzības likuma (2. pielikumā paredzēto atbrīvojumu) 2022. gada noteikumus. Taču pārskatītais atbrīvojums atkal tika apstrīdēts, pamatojoties uz to, ka tas neatbilda visām AK VDAR 23. panta 2. punkta prasībām. Apelācijas tiesa 2023. gada 11. decembra spriedumā pasludināja, ka pārskatītais imigrācijas atbrīvojums atkal nav saderīgs ar AK VDAR 23. panta 2. punktu. Lai panāktu atbilstību, Apvienotās Karalistes valdība pēc tam pieņēma 2018. gada Datu aizsardzības likuma (2. pielikumā paredzēto atbrīvojumu grozījuma) 2024. gada noteikumus, kas stājās spēkā 2024. gada 8. martā.

2. ATTIECĪGĀS NORISES SAISTĪBĀ AR NOTEIKUMIEM, KURUS PIEMĒRO PERSONAS DATU APSTRĀDEI

2.1. Apvienotās Karalistes datu aizsardzības regulējums

(9) Brīdī, kad tika pieņemts Īstenošanas lēmums (ES) 2021/1772, tiesisko regulējumu personas datu aizsardzībai Apvienotajā Karalistē veidoja šādi elementi:

— AK VDAR ([11]), kas iestrādāta Apvienotās Karalistes tiesībās saskaņā ar 2018. gada Likumu par izstāšanos no Eiropas Savienības ([12]) un grozīta ar 2019. gada Datu aizsardzības, privātuma un elektronisko sakaru (grozījumi utt.) (izstāšanās no ES) noteikumiem (DAPES noteikumi) ([13]),

— 2018. gada DAL ([14]), kas grozīts ar DAPES noteikumiem.

(10) Kaut arī šie abi akti, ar kuriem cieši atspoguļo atbilstošos, Eiropas Savienībā piemērojamos noteikumus, vēl aizvien ir Apvienotās Karalistes datu aizsardzības tiesību akti, tomēr kopš tā laika tajos ir izdarīti nelieli grozījumi, kas atspoguļo faktu, ka uz Apvienoto Karalisti vairs neattiecas Eiropas Savienības tiesību akti.

(11) Pirmkārt, 2023. gada saglabāto ES tiesību (atcelšanas un reformu) likumā (SEST likums) ([15]) ir precizēts, ka pēc 2023. gada beigām ES tiesību vispārējie principi vairs nebija daļa no Apvienotās Karalistes valsts tiesību aktiem ([16]). Turklāt Apvienotās Karalistes tiesām vairs nav pienākuma interpretēt negrozītos "asimilētos tiesību aktus" (kas iepriekš tika dēvēti par "saglabātiem ES tiesību aktiem") atbilstīgi ES tiesību vispārējiem principiem, bet gan šādi tiesību akti ir jālasa saskanīgi ar Apvienotās Karalistes valsts tiesību aktiem ([17]). Taču attiecīgajām Apvienotās Karalistes tiesām joprojām jāinterpretē negrozītie asimilētie tiesību akti saskaņā ar Eiropas Savienības Tiesas attiecīgo judikatūru, kas pieņemta pirms pārejas perioda beigām ([18]), kā minēts arī Īstenošanas lēmuma (ES) 2021/1772 13. apsvērumā. 2018. gada DAL ir grozīts ar Datu (izmantošanas un piekļuves) aktu, lai precizētu SEST likuma ietekmi uz Apvienotās Karalistes tiesību aktiem datu aizsardzības jomā. Piemēram, 2018. gada DAL 183.A panta 1. punktā ir paredzēts vispārējs noteikums, saskaņā ar kuru visi jaunie tiesību akti (kas pieņemti 2025. gada 20. augustā vai vēlāk), ar kuriem ievieš jaunus pienākumus vai pilnvaras apstrādāt personas datus, tiek uzskatīti par tādiem, uz kuriem attiecas Apvienotās Karalistes tiesību akti datu aizsardzības jomā. Tas nozīmē, ka Apvienotās Karalistes datu aizsardzības regulējums joprojām prevalē pār citiem tiesību aktiem. Saskaņā ar

([11]) Vispārīgā datu aizsardzības regula, pieejama šādā vietnē: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) 2018. gada Likums par izstāšanos no Eiropas Savienības, pieejams šādā vietnē: https://www.legislation.gov.uk/ukpga/2018/16/contents, kas iestrādāts Savienības tiesību aktos, kuri bija tieši piemērojami Apvienotajā Karalistē pārejas perioda beigās uz attiecībā uz Apvienotās Karalistes tiesību aktiem. Šie tā dēvētie "saglabātie ES tiesību akti" ietvēra Regulu (ES) 2016/679 pilnā apjomā, ieskaitot tās apsvērumus (sk. 2018. gada Likuma par izstāšanos no Eiropas Savienības paskaidrojuma raksta 83. punktu, pieejams šādā tīmekļa vietnē: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Minētajā likumā ir paredzēts, ka Apvienotās Karalistes tiesām negrozītie saglabātie ES tiesību akti bija jāinterpretē saskaņā ar Eiropas Savienības Tiesas attiecīgo judikatūru un Savienības tiesību aktu vispārējiem principiem, kā tie bija piemērojami tieši pirms pārejas perioda beigām (attiecīgi – "saglabātā ES judikatūra" un "saglabātie ES tiesību aktu vispārējie principi").

([13]) 2019. gada Datu aizsardzības, privātuma un elektronisko sakaru (grozījumi utt.) (izstāšanās no ES) noteikumi, pieejami šādā vietnē: https://www.legislation.gov.uk/uksi/2019/419/contents/made, kas grozīti ar 2020. gada DAPES noteikumiem; pieejami šādā tīmekļa vietnē: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. 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.

([14]) 2018. gada Datu aizsardzības likums, pieejams šādā vietnē: https://www.legislation.gov.uk/ukpga/2018/12/contents. Pirms Apvienotās Karalistes izstāšanās no Eiropas Savienības un pārejas perioda laikā 2018. gada Datu aizsardzības likumā tika izklāstīti valsts līmeņa noteikumi, ar kuriem gadījumos, kad to atļāva Regula (ES) 2016/679, precizēja un ierobežoja Regulas (ES) 2016/679 noteikumu piemērošanu un transponēja Eiropas Parlamenta un Padomes Direktīvu (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 krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp., ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Pieejams šādā vietnē: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) 5. pants 2018. gada Likumā par izstāšanos no Eiropas Savienības, kas grozīts ar SEST likumu.

([17]) 5. panta A2. punkts 2018. gada Likumā par izstāšanos no Eiropas Savienības, kas grozīts ar SEST likumu.

([18]) 6. panta 3. punkts un 7. pants 2018. gada Likumā par izstāšanos no Eiropas Savienības, kas grozīts ar SEST likumu.

2018. gada DAL 183.A panta 2. punkta b) apakšpunktu šo prezumpciju var nepiemērot tad, ja Apvienotās Karalistes parlaments apzināti nolemj šādi rīkoties tiesību aktos, saglabājot parlamentāro suverenitāti. Turklāt 2018. gada DAL 186. panta 2.A punktā ir precizēts, ka 2018. gada DAL 186. panta 3. punktā uzskaitītos datu subjektu tiesību ierobežojumus neatceļ 2018. gada DAL 186. panta 1. punkts, kurā noteikts, ka normatīvie akti, ar kuriem aizliedz vai ierobežo informācijas izpaušanu, neprevalē pār konkrētām datu aizsardzības tiesībām. Tādējādi, piemēram, tiek nodrošināts, ka uz 2018. gada Datu aizsardzības likumā izklāstītajiem datu subjektu tiesību ierobežojumiem pašiem par sevi neattiecas 2018. gada DAL 186. panta 1. punktā paredzētā vispārējā "datu aizsardzības prioritāte".

(12) Otrkārt, kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas Apvienotās Karalistes datu aizsardzības tiesību akti ir tikuši grozīti ar 2023. gada Datu aizsardzības (pamattiesības un brīvības) grozījumu noteikumiem ([19]). Šajos noteikumos tās atsauces uz pamattiesībām vai pamatbrīvībām, kuras ietvertas AK VDAR un 2018. gada Datu aizsardzības likumā (kuras iepriekš tika definētas ar nolūku aptvert ES pamattiesības un pamatbrīvības ([20])), ir definētas kā atsauces uz tiesībām atbilstīgi Eiropas Cilvēktiesību konvencijai, kas Apvienotās Karalistes valsts tiesību aktos ir spēkā saskaņā ar 1998. gada Cilvēktiesību likumu ([21]). 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 minētās konvencijas 16., 17. un 18. pantu. Tas ietver tiesības uz privātās un ģimenes dzīves neaizskaramību (un datu aizsardzību minēto tiesību ietvaros) un tiesības uz lietas taisnīgu izskatīšanu ([22]).

(13) Visbeidzot, attiecībā uz AK VDAR un 2018. gada DAL ir veiktas mērķorientētas reformas, kas izklāstītas Datu (izmantošanas un piekļuves) akta piektajā un sestajā daļā. Lai gan Datu (izmantošanas un piekļuves) akta tvērums ievērojami pārsniedz personas datu aizsardzību, tajā ir paredzēti nelieli grozījumi vairākos datu aizsardzības režīma aspektos, piemēram, cita starpā tādos kā datu apstrāde zinātniskās pētniecības nolūkos, datu apstrādes juridiskie pamati, noteikumi par mērķa ierobežojuma principu un nosacījumi automatizētai lēmumu pieņemšanai. Turklāt ar Datu (izmantošanas un piekļuves) aktu veic grozījumus *ICO* pārvaldības struktūrā. Pēc šo pasākumu īstenošanas *ICO* tiks aizstāts ar jaunu struktūru – Informācijas komisiju. Regulatora kā neatkarīgas datu aizsardzības uzraudzības iestādes Apvienotajā Karalistē loma un funkcijas nemainīsies. Ar minēto aktu arī ievieš regulatora jaunas izpildes pilnvaras.

(14) Šajā lēmumā ir novērtētas likumdošanas, regulatīvās un citas norises, kuras ir būtiskas Īstenošanas lēmumā (ES) 2021/1772 izdarītajam secinājumam par Apvienotās Karalistes garantēto aizsardzības līmeni. Īstenošanas lēmumā (ES) 2021/1772 veiktais novērtējums joprojām ir spēkā attiecībā uz tiem Apvienotās Karalistes datu aizsardzības regulējuma aspektiem, kuri kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas nav tikuši grozīti vai kurus nav ietekmējušas citas norises.

(15) Turpmākajās iedaļās ir sīki analizētas likumdošanas, regulatīvās un citas būtiskas norises, pamatojoties uz pietiekamības standartu, saskaņā ar kuru Komisijai jānosaka, vai attiecīgā trešā valsts garantē aizsardzības līmeni, kas "pēc būtības ir līdzvērtīgs" Eiropas Savienībā nodrošinātajam aizsardzības līmenim ([23]). Kā precizējusi Eiropas Savienības Tiesa, tas nenozīmē, ka ir jākonstatē identisks aizsardzības līmenis ([24]). Konkrēti – attiecīgās trešās valsts izmantotie līdzekļi personas datu aizsardzībai var atšķirties no Eiropas Savienībā izmantotajiem līdzekļiem, kamēr vien tie praksē efektīvi nodrošina pietiekamu aizsardzības līmeni ([25]). Tāpēc aizsardzības līmeņa pietiekamības standarts neparedz Savienības noteikumu precīzu replicēšanu. Pārbaude drīzāk atklāj to, vai attiecīgās valsts tiesību sistēma kopumā spēj nodrošināt nepieciešamo aizsardzības līmeni, ņemot vērā tiesību uz datu aizsardzību būtību un to efektīvu īstenošanu, uzraudzību un izpildi ([26]).

([19]) Pieejami šādā vietnē: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) ES pamattiesības un pamatbrīvības Apvienotās Karalistes tiesību aktos bija saglabātas ar 4. pantu 2018. gada Likumā par izstāšanos no Eiropas Savienības, kas 2023. gada beigās tika atcelts ar SEST likumu.

([21]) 2023. gada Datu aizsardzības (pamattiesības un brīvības) grozījumu noteikumu 2. panta 3. punkts.

([22]) Eiropas Cilvēktiesību konvencijas (ECTK) 6., 8., 10. un 13. pants (sk. arī 1998. gada Cilvēktiesību likuma 1. pielikumu).

([23]) Regulas (ES) 2016/679 104. apsvērums.

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

([25]) Lieta *Schrems I*, 74. punkts.

([26]) 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.

2.1.1. *Definīcijas*

(16) Apvienotās Karalistes datu aizsardzības režīmā joprojām piemēro datu aizsardzības pamatjēdzienus, ar kuriem atspoguļo Regulā (ES) 2016/679 izmantoto terminoloģiju. Šie jēdzieni ir tikuši novērtēti Īstenošanas lēmuma (ES) 2021/1772 23. apsvērumā.

(17) Kaut arī Datu (izmantošanas un piekļuves) aktā lielākā daļa definīciju ir palikušas nemainīgas, tomēr ar to ir ieviestas tādas konkrētas definīcijas AK VDAR 4. panta 2., 3., 4. un 5. punktā, kuras attiecas uz personas datu apstrādi zinātniskos, vēsturiskos un statistikas nolūkos. 2. punktā "apstrāde zinātniskos nolūkos" ir definēta kā personas datu apstrāde, ko veic jebkādas tādas pētniecības nolūkos, kuru var pamatoti raksturot kā zinātnisku. Šo pētniecību var finansēt publiski vai privāti, un to var veikt vai nu kā komerciālu, vai nekomerciālu darbību. Atspoguļojot Regulas (ES) 2016/679 159. apsvēruma saturu, 3. punktā ir sniegts neizsmeļošs saraksts ar tādu pētniecības darbību piemēriem, kuras uzskatāmas par darbībām ar zinātniskiem mērķiem, tostarp tehniskā izstrāde, demonstrējumi, fundamentālie pētījumi un lietišķie pētījumi. 4. punktā ir precizēts, ka "vēsturiskie pētījumi" ietver ģenealoģisko pētniecību, kas Regulas (ES) 2016/679 160. apsvērumā arī atzīta par vēstures pētniecības nolūku. Visbeidzot, 5. punktā apstrāde, ko veic statistiskos nolūkos, ir definēta kā datu apstrāde statistikas apsekojumu veikšanai vai statistikas rezultātu iegūšanai gadījumos, kad dati tiek apkopoti tādā pakāpē, ka tie vairs nav personas dati. Turklāt apstrādātos datus vai no tiem izrietošo informāciju nedrīkst izmantot, lai pieņemtu lēmumus vai veiktu darbības, kuras attiecas uz kādu konkrētu fizisku personu. Šī definīcija atbilst Regulas (ES) 2016/679 162. apsvērumā izklāstītajai izpratnei par statistikas nolūkiem.

(18) Visbeidzot – kaut arī ar AK VDAR 4. panta grozījumiem tiek pievienotas konkrētas definīcijas par datu apstrādi zinātniskos, vēsturiskos un statistikas nolūkos, tomēr šādas definīcijas ir saskanīgas ar Regulas (ES) 2016/679 burtu un garu, kā atspoguļots iepriekš minētajā 159., 160. un 162. apsvērumā.

(19) Pievienojot AK VDAR 4. pantam 6. punktu, ar Datu (izmantošanas un piekļuves) aktu ir arī izveidots īpašs regulējums, kura mērķis ir saņemt datu subjekta piekrišanu personas datu apstrādei zinātniskos nolūkos. Ļoti līdzīgi kā Regulas (ES) 2016/679 33. apsvērumā, kurā atzīts, ka zinātniskās pētniecības jomā piekrišanu ne vienmēr var iegūt attiecībā uz konkrētu apstrādes nolūku, ar jauno noteikumu tiek pieļauti plašāki piekrišanas veidi, atļaujot datu subjektiem sniegt derīgu piekrišanu pat tad, ja datu vākšanas laikā nav iespējams pilnībā identificēt precīzus pētniecības nolūkus – ar nosacījumu, ka piekrišanas iegūšana atbilst vispāratzītiem ētikas standartiem, kas ir būtiski konkrētajā pētniecības jomā. Datu subjektiem jebkurā gadījumā ir jābūt iespējai piekrist personas datu apstrādei tikai attiecībā uz konkrētām pētniecības daļām, ja tas ir iespējams.

(20) Visbeidzot, Datu (izmantošanas un piekļuves) aktā ir sīkāk izklāstīti (jaunajā AK VDAR 8.A nodaļā) ([27]) aizsardzības pasākumi, kas līdz šim bija noteikti AK VDAR 89. pantā un 2018. gada DAL 19. pantā attiecībā uz datu apstrādi arhivēšanas vajadzībām sabiedrības interesēs un zinātniskās, vēsturiskās un statistiskās pētniecības nolūkos. Šie aizsardzības pasākumi ir līdzīgi tiem, kas ir noteikti saskaņā ar Regulas (ES) 2016/679 89. pantu, un tie ietver prasību paredzēt tehniskus un organizatoriskus pasākumus, lai nodrošinātu datu minimizēšanas principa ievērošanu.

2.2. **Garantijas, tiesības un pienākumi**

2.2.1. *Apstrādes likumīgums un godprātība*

(21) Apvienotās Karalistes datu aizsardzības regulējumā joprojām ir noteikts, ka dati jāapstrādā likumīgi, godprātīgi un leģitīmi, kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 24.–26. apsvērumā.

([27]) AK VDAR 84.A–84.D pants, kas ieviests ar Datu (izmantošanas un piekļuves) akta 86. pantu.

(22) Likumīguma un godprātības principi un likumīgas apstrādes pamats Apvienotās Karalistes tiesību aktos joprojām tiek garantēts ar AK VDAR 5. panta 1. punkta a) apakšpunktu un 6. panta 1. punktu, kas novērtēts Īstenošanas lēmumā (ES) 2021/1772. Kaut arī minētie noteikumi lielā mērā joprojām ir identiski ([28]) ar attiecīgajiem noteikumiem Regulā (ES) 2016/679, ar Datu (izmantošanas un piekļuves) aktu vispirms groza AK VDAR 6. panta 1. punktu, ieviešot papildu likumīgu pamatu personas datu apstrādei saskaņā ar 6. panta 1. punkta ea) apakšpunktu ([29]). Saskaņā ar minēto noteikumu apstrāde ir likumīga tad, ja un ciktāl tā ir "vajadzīga atzītu leģitīmu interešu ievērošanai". Atšķirībā no leģitīmo interešu juridiskā pamata, kas paredzēts AK VDAR 6. panta 1. punkta f) apakšpunktā, atbilstīgi jaunievieštajam atzītu leģitīmu interešu juridiskajam pamatam nav nepieciešams katrā atsevišķā gadījumā samērot datu pārziņa leģitīmās intereses ar datu subjekta interesēm vai tā pamattiesībām un brīvībām; tas ir tādēļ, lai nodrošinātu lielāku juridisko noteiktību datu pārziņiem, kuri nav publiska struktūra. Jaunievieštajā AK VDAR 6. panta 5. punktā ir precizēts, ka datu apstrāde ir vajadzīga atzītu leģitīmu interešu ievērošanai tikai tad, ja tā atbilst nosacījumam, kas izklāstīts 1. pielikumā ([30]), kurā uzskaitītas situācijas, kādās apstrāde tiek uzskatīta par vajadzīgu atzītu leģitīmu interešu ievērošanai, piemēram, tad, ja apstrāde tiek veikta, atbildot uz pieprasījumu, ko saņēmusi publiska iestāde, kurai dati ir nepieciešami, lai pildītu uzdevumu sabiedrības interesēs, kuru juridiskais pamats atbilst AK VDAR 6. panta 3. punktam; ja apstrāde ir vajadzīga, lai garantētu valsts drošību un aizsargātu sabiedrisko drošību, vai tā ir vajadzīga aizsardzības nolūkos, lai reaģētu uz ārkārtas situāciju, atklātu, izmeklētu vai novērstu noziegumu vai aizsargātu neaizsargātas personas ([31]).

(23) Kaut arī ar Datu (izmantošanas un piekļuves) aktu tādējādi tiek paplašināts to personas datu apstrādes juridisko pamatu saraksts, kuri pieejami datu pārzinim, tomēr jaunievieštais atzītu leģitīmu interešu juridiskais pamats ir pakļauts vairākiem būtiskiem ierobežojumiem. Pirmkārt, atzītās leģitīmās intereses aprobežojas tikai ar konkrētām situācijām, kuras ir izsmeļoši uzskaitītas minētajā tiesību aktā. Otrkārt, publiskās iestādes, pildot savus uzdevumus, nevar atsaukties uz šo juridisko pamatu ([32]). Treškārt, minētais juridiskais pamats attiecas tikai uz jomām, kurās pastāv nepārprotama sabiedrības interese par datu apstrādes darbību (saskaņā ar 1. pielikumā izklāstītajiem nosacījumiem), t. i., jomās, kurās apstrāde kalpo mērķiem, kas uzskaitīti AK VDAR 23. pantā (kurš atbilst Regulas (ES) 2016/679 23. pantam), un tādējādi minēto juridisko pamatu nevar izmantot komerciālos nolūkos. Ceturtkārt, lai gan ar Datu (izmantošanas un piekļuves) aktu valsts sekretāram tiek piešķirtas tiesības grozīt 1. pielikumā

([28]) Precizēšanas nolūkā ar Datu (izmantošanas un piekļuves) aktu AK VDAR 6. pantā arī ievieš jaunu punktu, kurā sniegti piemēri apstrādes veidiem, kurus var uzskatīt par nepieciešamiem leģitīmu interešu ievērošanai AK VDAR 6. panta 1. punkta f) apakšpunkta nozīmē. Šie piemēri (tiešā tirgvedība, datu nosūtīšana grupas iekšienē administratīvos nolūkos, kā arī tīklu un informācijas sistēmu drošība) ir arī minēti Regulas (ES) 2016/679 47. un 48. apsvērumā, proti, kā situācijas, kurās apstrāde tiktu uzskatīta par datu pārziņa leģitīmām interesēm.

([29]) Datu (izmantošanas un piekļuves) akta 70. panta 2. punkta b) apakšpunkts. Ar Datu (izmantošanas un piekļuves) akta 70. panta 5. punktu tiesības iebilst, kas ir noteiktas AK VDAR 21. pantā, ir paplašinātas, paredzot tās arī saskaņā ar jauno AK VDAR 6. panta 1. punkta ea) apakšpunktu.

([30]) Datu (izmantošanas un piekļuves) akta 70. panta 4. punkts.

([31]) Sk. Datu (izmantošanas un piekļuves) akta 4. pielikumu. Saskaņā ar informāciju, ko sniegušas Apvienotās Karalistes iestādes, piemēri situācijām, kurās nepubliskām struktūrām var būt nepieciešams apstrādāt personas datus, lai novērstu vai atklātu noziegumus, cita starpā ir tad, kad kāds uzņēmums uzzina par mēģinājumiem nelikumīgi uzlauzt tā datorsistēmas vai kad banka vai finanšu iestāde uzzina par krāpnieciskiem mēģinājumiem atvērt bankas kontu. Personas datu apstrāde, ko veic nepubliska struktūra, var būt nepieciešama, piemēram, lai garantētu valsts drošību vai aizsardzību gadījumos, kad komerciālai organizācijai ir aizdomas par to, ka klienta darbības tiešsaistē norāda uz dalību teroristiskā darbībā. *ICO* strādā pie konkrētiem norādījumiem šajā jautājumā, tostarp pie attiecīgo jēdzienu definīcijas. Piemēram, tajos ir minēts, ka "valsts drošība", visticamāk, attieksies uz Apvienotās Karalistes drošību un labklājību kopumā, kā arī uz tās iedzīvotājiem, iestādēm un valdības sistēmu. Sk. *ICO* norādījumu projektu par atzītām leģitīmām interesēm, kas publicēts sabiedriskas apspriešanas nolūkā un ir pieejams šādā vietnē: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) 6. panta 1. punkta pēdējā daļa, kas grozīta ar Datu (izmantošanas un piekļuves) akta 70. panta 2. punkta c) apakšpunktu.

ietverto sarakstu, pieņemot attiecīgus noteikumus ([33]), valsts sekretārs var pieņemt šādus noteikumus tikai pēc apspriešanās ar *ICO* ([34]) un minētajam sarakstam pievienot atzītas leģitīmas intereses tikai tad, ja šāda datu apstrāde ir vajadzīga, lai aizsargātu sabiedrības interešu mērķi, kurš uzskaitīts AK VDAR 23. panta 1. punkta c)–j) apakšpunktā ([35]). Visbeidzot, kā apstiprināts arī *ICO* norādījumos ([36]), datu pārziņiem, kuri kā juridisko pamatu izmanto atzītas leģitīmās intereses, ir jāievēro visas pārējās prasības saskaņā ar AK VDAR, tostarp jānodrošina, ka datu apstrāde ir nepieciešama un samērīga, lai sasniegtu leģitīmās intereses.

(24) Otrkārt, AK VDAR 6. panta 3. punktā, 9. panta 2. punkta g) apakšpunktā un 10. panta 1. punktā (kas atbilst attiecīgajiem Regulas (ES) 2016/679 noteikumiem) ar Datu (izmantošanas un piekļuves) aktu tiek precizēts, ka personas datu, īpašu kategoriju personas datu un personas datu, kuri attiecas uz sodāmību un noziedzīgiem nodarījumiem saskaņā ar juridiskām saistībām vai uzdevuma veikšanai sabiedrības interesēs, apstrādes pamats var būt ne tikai valsts tiesību akti, bet arī attiecīgās starptautiskās tiesības ([37]). Saskaņā ar jaunieviesto AK VDAR 9.A pantu (kopā ar A1. pielikumu) attiecīgās starptautiskās tiesības savukārt aprobežojas ar vienu nolīgumu, proti, ar 2019. gada 3. oktobrī parakstīto Nolīgumu starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā (AK un ASV nolīgums) ([38]). Minētajā nolīgumā paredzētie aizsardzības pasākumi ir tikuši novērtēti Īstenošanas lēmuma (ES) 2021/1772 153.–155. apsvērumā, un to īstenošana ir analizēta šā lēmuma 87.–93. apsvērumā.

2.2.2. *Īpašu kategoriju personas datu apstrāde*

(25) Apvienotās Karalistes datu aizsardzības regulējumā joprojām ir paredzēti specifiski aizsardzības pasākumi gadījumos, kad tiek apstrādāti īpašu kategoriju personas dati, kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 27.–42. apsvērumā.

(26) Joprojām ir spēkā gan īpašu kategoriju personas datu definīcija, gan īpašie noteikumi, kurus piemēro šo kategoriju datu apstrādei un kuri izklāstīti AK VDAR un 2018. gada Datu aizsardzības likumā. Vienlaikus ar Datu (izmantošanas un piekļuves) aktu valsts sekretāram tiek piešķirtas jaunas noteikumu izstrādes pilnvaras, proti, pilnvaras pievienot īpašas datu kategorijas, pielāgot to izmantošanai piemērojamos nosacījumus un vajadzības gadījumā pievienot jaunas definīcijas ([39]). Svarīgi ir tas, ka ar minēto aktu valsts sekretāram nav atļauts svītrot vai grozīt esošās īpašās datu kategorijas vai arī mainīt šo kategoriju apstrādes nosacījumus ([40]). Tādējādi jaunieviestās noteikumu izstrādes pilnvaras ļauj valdībai vienīgi pievienot jaunas sensitīvo datu kategorijas un noteikt šo kategoriju apstrādes nosacījumus, kā mērķis ir nodrošināt to, ka valdība vajadzības gadījumā varētu reaģēt uz tehnoloģiju un sabiedrības attīstību nākotnē.

(27) Tādēļ šie grozījumi neietekmē īpašu kategoriju personas datu aizsardzības līmeni, kurš, kā konstatēts Īstenošanas lēmumā (ES) 2021/1772, pēc būtības ir līdzvērtīgs Eiropas Savienībā nodrošinātajai aizsardzībai.

([33]) Pirms iepriekš minēto noteikumu pieņemšanas valsts sekretāram jāņem vērā jebkādu izmaiņu ietekme uz datu subjektu interesēm, pamattiesībām un brīvībām, kā arī tas, ka bērniem (attiecīgā gadījumā) pienākas īpaša aizsardzība attiecībā uz viņu personas datiem. Noteikumi jāpieņem ar normatīvu aktu, un tie jāapstiprina ar apstiprinošas rezolūcijas procedūru, kas nozīmē to, ka tie ir aktīvi jāapstiprina Apvienotās Karalistes parlamentā. Datu (izmantošanas un piekļuves) akta 70. panta 4. punkta 8. apakšpunkts.

([34]) 2018. gada DAL 182. panta 2. punkts.

([35]) Datu (izmantošanas un piekļuves) akta 70. panta 4. punkta 9. apakšpunkts.

([36]) Sk. *ICO* norādījumus par leģitīmām interesēm, pieejami šādā vietnē: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Datu (izmantošanas un piekļuves) akta 72. pants.

([38]) Nolīgums starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā, pieejams šādā 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.

([39]) Datu (izmantošanas un piekļuves) akta 74. pants. Šādi noteikumi jāapstiprina ar apstiprinošas rezolūcijas procedūru, kas nozīmē to, ka tie ir aktīvi jāapstiprina Apvienotās Karalistes parlamentā.

([40]) Sk. AK VDAR 11.A panta 1. punkta b) apakšpunktu un 2. punktu, kā arī Datu (izmantošanas un piekļuves) akta paskaidrojuma raksta 571. punktu; pieejami šādā vietnē: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Nolūka ierobežojums*

(28) Apvienotās Karalistes personas datu aizsardzības režīmā joprojām tiek prasīts, ka dati ir jāapstrādā konkrētā nolūkā, un pēc tam tos var izmantot tikai, ciktāl tas nav pretrunā sākotnējam apstrādes nolūkam, kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 43.–48. apsvērumā.

(29) Pirmkārt, ar Datu (izmantošanas un piekļuves) aktu tiek veikti nedaudzi mērķorientēti grozījumi nolūka ierobežojuma principā, kas izklāstīts AK VDAR 5. panta 1. punkta b) apakšpunktā. Šie grozījumi precizē šā principa piemērošanu, nemainot būtību. Datu (izmantošanas un piekļuves) akta 71. panta 1., 2. un 3. punktā ir precizēts, ka nolūka ierobežojuma principu piemēro gadījumos, kad datus vāc no datu subjekta vai citādi, ka šo principu piemēro tikai tad, ja personas datus turpmāk apstrādā viens un tas pats datu pārzinis vai tos apstrādā viņa vārdā (t. i., minēto principu nepiemēro datu pārziņa maiņas gadījumā), un ka apstrāde nekļūst likumīga tādēļ vien, ka tā ir saderīga ar nolūkiem, kādos personas dati tika vākti.

(30) Otrkārt, Datu (izmantošanas un piekļuves) aktā ir precizēti noteikumi par personas datu turpmāku apstrādi, pārgrupējot tos jaunpievienotajā AK VDAR 8.A pantā, kurā ir noteikts pilnīgs režīms personas datu turpmākai apstrādei. AK VDAR 8.A panta 2. punktā ir uzskaitīti elementi, kas jāņem vērā, nosakot to, vai jauns apstrādes nolūks ir saderīgs ar sākotnējo nolūku. Līdz šim šie elementi bija uzskaitīti AK VDAR 6. panta 4. punktā, kas atbilst Regulas (ES) 2016/679 6. panta 4. punktam ([41]). Ar AK VDAR 8.A panta 3. punktu apvieno vienā noteikumā situācijas, kurās personas datu apstrāde jaunā nolūkā ir uzskatāma par saderīgu ar sākotnējo nolūku. Tas attiecas uz situācijām, kurās datu subjekts piekrīt personas datu apstrādei jaunajā nolūkā, vai uz gadījumiem, kad apstrāde ir vajadzīga, lai aizsargātu kādu no 23. panta 1. punktā uzskaitītajiem mērķiem ([42]), vai kad apstrādi veic zinātniskās vai vēstures pētniecības nolūkā, arhivēšanas nolūkos sabiedrības interesēs vai statistikas nolūkos ([43]). Visbeidzot, Datu (izmantošanas un piekļuves) aktā ir precizēts, ka jebkura apstrāde, ko veic, lai nodrošinātu to, ka apstrāde atbilst AK VDAR 5. panta 1. punktā izklāstītajiem datu aizsardzības principiem, vai ar kuru apliecina, ka tas ir panākts, tiek uzskatīta par saderīgu ar sākotnējo nolūku. Iepriekš minētās situācijas joprojām atbilst tam, kas arī Regulā (ES) 2016/679 tiek uzskatīts par saderīgu turpmāku apstrādi.

(31) Treškārt, AK VDAR 8.A panta 3. punkta d) apakšpunktā ar Datu (izmantošanas un piekļuves) aktu tiek ieviestas arī jaunas papildu situācijas, kurās personas datu turpmāka apstrāde jaunā nolūkā tiek uzskatīta par saderīgu ar sākotnējo nolūku. Šīs situācijas ir uzskaitītas AK VDAR 2. pielikumā ([44]) un ietver, piemēram, gadījumus, kad datu apstrāde notiek, atbildot uz pieprasījumu, ko saņēmusi publiska iestāde, kurai dati ir vajadzīgi, lai pildītu uzdevumu sabiedrības interesēs, kuru juridiskais pamats atbilst AK VDAR 6. panta 3. punktam, gadījumus, kad apstrāde ir vajadzīga, lai aizsargātu sabiedrisko drošību, reaģētu uz ārkārtas situāciju, atklātu, izmeklētu vai novērstu noziegumu, aizsargātu datu subjekta un citu personu vitālas intereses un aizsargātu neaizsargātas personas, gadījumus, kad apstrāde ir vajadzīga nodokļu nolūkos, vai tā ir vajadzīga, lai izpildītu juridiskas saistības ([45]).

(32) Kaut gan ar Datu (izmantošanas un piekļuves) aktu tādējādi paplašina to situāciju sarakstu, kurās datu turpmāka apstrāde citā nolūkā tiek uzskatīta par saderīgu ar sākotnējo apstrādes nolūku, tomēr uz šo paplašinājumu attiecas būtiski ierobežojumi. Pirmkārt, tas aprobežojas tikai ar konkrētām situācijām, kuras ir izsmeļoši uzskaitītas minētajā tiesību aktā. Otrkārt, minētais paplašinājums attiecas tikai uz jomām, kurās pastāv nepārprotama sabiedrības interese par datu apstrādes darbību, t. i., jomās, kurās turpmāka apstrāde kalpo mērķiem, kas uzskaitīti

([41]) Tāpat, kā tas ir Regulas (ES) 2016/679 gadījumā, arī šie elementi ietver jebkuru saikni starp sākotnējo un jauno nolūku, kontekstu, kādā personas dati tika vākti, tostarp attiecības starp datu subjektu un pārzini, apstrādes raksturu un to, vai apstrāde attiecas uz īpašām datu kategorijām, paredzētās turpmākās apstrādes iespējamās sekas datu subjektam un atbilstošu garantiju esamību.

([42]) Sk. arī Regulas (ES) 2016/679 6. panta 4. punktu.

([43]) Regulas (ES) 2016/679 50. apsvērums.

([44]) AK VDAR 2. pielikums ir ieviests ar Datu (izmantošanas un piekļuves) akta 5. pielikumu, sk. minētā akta 71. panta 6. punktu.

([45]) Sk. Datu (izmantošanas un piekļuves) akta 5. pielikumu.

AK VDAR 23. pantā (kurš atbilst Regulas (ES) 2016/679 23. pantam). Tādējādi minēto paplašinājumu nevar izmantot komerciālos nolūkos. Treškārt, lai gan ar Datu (izmantošanas un piekļuves) aktu valsts sekretāram tiek piešķirtas tiesības grozīt 2. pielikumā ietverto sarakstu, pieņemot attiecīgus noteikumus ([46]), valsts sekretārs minētajam sarakstam var pievienot datu apstrādes veidus tikai tad, ja šāda apstrāde ir vajadzīga, lai aizsargātu sabiedrības interešu mērķi, kurš uzskaitīts AK VDAR 23. panta 1. punkta c)–j) apakšpunktā ([47]). Ceturtkārt, gadījumos, kad datu pārziņa veiktā personas datu vākšana pamatojas uz datu subjekta piekrišanu, apstrādi, kas 2. pielikumā uzskaitītajās situācijās tiek veikta jaunā nolūkā, uzskata par saderīgu ar sākotnējo nolūku tikai tad, ja no pārziņa nevar pamatoti gaidīt, ka tas iegūs datu subjekta jaunu piekrišanu ([48]).

2.2.4. *Individuālās tiesības*

(33) Atbilstīgi Apvienotās Karalistes personas datu aizsardzības regulējumam datu subjekti joprojām izmanto tādas pašas – kā Regulā (ES) 2016/679 noteiktās – individuālās tiesības, kurās nav veiktas nekādas būtiskas izmaiņas ([49]) un kuras var tikt īstenotas attiecībā pret datu pārzini vai apstrādātāju, jo īpaši tiesības piekļūt datiem, tiesības iebilst pret apstrādi un tiesības panākt datu labošanu vai dzēšanu, kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 51.–54. apsvērumā.

(34) Pirmkārt, Datu (izmantošanas un piekļuves) aktā ir precizēta konkrēta kārtība, kādā šīs tiesības var izmantot. No vienas puses, grozot AK VDAR 12. pantu un ieviešot jaunu 12.A pantu ([50]), ar iepriekš minēto aktu tiek precizēti termiņi, kuros pārziņiem jāatbild uz datu subjekta pieprasījumiem. Konkrētāk – AK VDAR 12. pants ir grozīts tādā veidā, ka datu pārziņa pienākumos vairs nav sniegt informāciju par rīcību, kas veikta (vai par iemesliem, kādēļ nav veikta rīcība), lai saskaņā ar AK VDAR 15.–22. pantu "viena mēneša laikā pēc pieprasījuma saņemšanas", taču drīzāk "pirms piemērojamā laikposma beigām" reaģētu uz datu subjekta pieprasījumu. Piemērojamais laikposms ir sīkāk definēts jaunieviestajā AK VDAR 12.A pantā, proti, tas ir viena mēneša laikposms, to skaitot no attiecīgā brīža, kas ir laiks, kad datu pārzinis saņem pieprasījumu, vai laiks, kad pārzinis saņem informāciju saistībā ar pieprasījumu saskaņā ar AK VDAR 12. panta 6. punktu, vai laiks, kad ir samaksāta maksa, kas iekasēta saistībā ar pieprasījumu saskaņā ar AK VDAR 12. panta 5. punktu – atkarībā no tā, kurš datums ir vēlāk ([51]). Turklāt saskaņā ar 12.A panta 3. punktu datu pārzinim ir atļauts pagarināt piemērojamo laikposmu vēl par diviem mēnešiem gadījumos, kad tas ir vajadzīgs datu subjekta iesniegto pieprasījumu sarežģītības vai šādu pieprasījumu skaita dēļ. No otras puses – vienīgi attiecībā uz tiesībām piekļūt informācijai un personas datiem ar Datu (izmantošanas un piekļuves) aktu tiek grozīts AK VDAR 15. pants, lai iekļautu atbilstīgi esošajai valsts judikatūrai izstrādātu precizējumu (kura pamatā ir ES tiesību aktos noteiktais samērīguma princips), ka datu pārziņiem jāveic tikai saprātīga un samērīga pieprasītās informācijas un personas datu meklēšana ([52]). Paredzams, ka jaunais noteikums tiks interpretēts saskaņā ar esošo judikatūru, kurā noteikts, ka "[..] veicot samērīguma pārbaudi, tiek izsvērts meklēšanas galīgais mērķis, proti, potenciālais ieguvums, ko datu subjektam varētu dot informācijas sniegšana, attiecībā pret līdzekļiem, ar kādiem minētā informācija ir iegūta. Katrā konkrētā gadījumā būs jāizvērtē, vai informācijas atrašana un sniegšana prasītu nesamērīgas pūles attiecībā pret ieguvumiem, kurus tā varētu dot datu subjektam." ([53])

([46]) AK VDAR 8.A panta 5. punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 71. panta 1. punktu.
([47]) AK VDAR 8.A panta 6. punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 71. panta 1. punktu.
([48]) AK VDAR 8.A panta 4. punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 71. panta 1. punktu.
([49]) Ar 2024. gada Likuma par cietušajiem un ieslodzītajiem (*VAP* likums) 31. pantu tika iekļauts papildu pamatojums saistībā ar AK VDAR 17. pantā noteiktajām tiesībām uz datu dzēšanu, piešķirot datu subjektiem tiesības pieprasīt, lai datu pārziņi dzēstu viņu personas datus gadījumos, kad tie tikuši apstrādāti tāda nepamatota apgalvojuma rezultātā, kuru par datu subjektu izteikusi ļaunprātīga persona. Personu uzskata par "ļaunprātīgu", ja tā ir notiesāta par kādu no *VAP* likuma 31. panta 3. punktā uzskaitītajiem noziedzīgajiem nodarījumiem (piemēram, par aizskaršanu) vai ja attiecībā uz to ir izdots aizliegums vajāt kādu personu. *VAP* likums ir pieejams šādā tīmekļa vietnē: https://www.legislation.gov.uk/ukpga/2024/21/contents. Turklāt ar Datu (izmantošanas un piekļuves) akta 77. pantu tiek grozītas AK VDAR 13. pantā paredzētās tiesības uz informāciju tādā veidā, ka datu pārziņa pienākumos vairs nav informēt datu subjektu par viņa personas datu turpmāku apstrādi jaunā nolūkā tad, ja minētais nolūks ir zinātniskā vai vēstures pētniecība, arhivēšana sabiedrības interesēs vai statistikas nolūks, ja apstrāde tiek veikta saskaņā ar īpašajām garantijām, kas izklāstītas AK VDAR jaunajā 84.B pantā, un ja informācijas sniegšana būtu neiespējama vai nesamērīga.
([50]) Datu (izmantošanas un piekļuves) akta 76. pants.
([51]) AK VDAR 12.A panta 1. un 2. punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 76. pantu.
([52]) AK VDAR 15. panta 1.A punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 78. pantu.
([53]) Lieta *Dawson-Damer* pret *Taylor Wessing LLP,* (2017) *EWCA Civ* 74.

(35) Tādēļ, kaut arī uz termiņiem, kādos jāatbild uz datu subjektu pieprasījumiem, un uz konkrētajiem datu pārziņu pienākumiem saistībā ar piekļuves tiesībām attiecas sīkāk izstrādāti noteikumi, Apvienotās Karalistes sistēma turpina nodrošināt to, ka datu subjektu pieprasījumi jāizskata samērīgos laikposmos, kas ir noteikti uz objektīvu faktoru pamata. Turklāt datu pārziņa būtiskie pienākumi, kas viņam jāpilda, atbildot uz piekļuves pieprasījumiem, ir noteikti uz tādu iedibinātu juridisko standartu pamata, kuros ņemtas vērā arī datu subjekta intereses. Visbeidzot, jau pašreizējos *ICO* norādījumos ir noteikts, ka datu pārzinim nav jāveic meklēšana, kas būtu nepamatota vai nesamērīga ar to, cik svarīgi būtu nodrošināt piekļuvi informācijai ([54]).

(36) Šo individuālo tiesību ierobežojumi, kas izklāstīti 2018. gada Datu aizsardzības likumā un atbilst AK VDAR 23. pantam, kā arī ierobežojumi un garantijas, uz kuru pamata nosaka šo ierobežojumu piemērošanu, vēl aizvien ir spēkā Apvienotās Karalistes regulējumā ([55]), kā sīki aprakstīts Īstenošanas lēmuma (ES) 2021/1772 55.–67. apsvērumā.

(37) Konkrēti – attiecībā uz ierobežojumu saistībā ar personas datiem, kurus apstrādā efektīvas imigrācijas kontroles nodrošināšanas nolūkos, vai tādu darbību izmeklēšanu vai atklāšanu, kas varētu apdraudēt efektīvas imigrācijas kontroles saglabāšanu (ciktāl minēto noteikumu piemērošana, iespējams, varētu apdraudēt kādu no minētajiem jautājumiem) (imigrācijas atbrīvojums) ([56]), Apvienotās Karalistes valdība ir grozījusi 2018. gada DAL 2. pielikuma 4. punktu, pieņemot 2018. gada Datu aizsardzības likuma (2. pielikumā paredzēto atbrīvojumu) 2022. gada noteikumus ([57]) un 2018. gada Datu aizsardzības likuma (2. pielikumā paredzēto atbrīvojumu) 2024. gada noteikumus ([58]), kas papildina 2022. gada noteikumus ([59]). 2018. gada DAL 2. pielikuma 4.A un 4.B punktā ar minētajiem grozījumiem tiek iestrādātas tās garantijas imigrācijas atbrīvojuma īstenošanai, kuras nepieciešamas saskaņā ar AK VDAR 23. panta 2. punktu. Konkrēti – ar minētajiem grozījumiem tiek noteikts, i) ka imigrācijas atbrīvojums jāizmanto tikai katrā gadījumā individuāli, atsevišķi attiecībā uz katru būtisko AK VDAR noteikumu un no jauna katrā tādā gadījumā, kad valsts sekretārs apsver iespēju nepiemērot vai ierobežot kādu no attiecīgajiem AK VDAR noteikumiem ([60]), ii) ka, izmantojot imigrācijas atbrīvojumu, ir jāņem vērā datu subjekta tiesības un brīvības un iespējamā neaizsargātība ([61]), iii) ka valsts sekretāram jāveic uzskaite par imigrācijas atbrīvojuma izmantošanu un jāinformē datu subjekts par šāda atbrīvojuma izmantošanu (izņemot īpašos apstākļos, kad informācija apdraudētu atbrīvojuma mērķi) ([62]) un iv) ka jāprecizē, ka imigrācijas atbrīvojuma izmantošana aprobežojas ar personas datu apstrādi, ko veic valsts sekretārs ([63]), t. i., praksē – Iekšlietu ministrija, lai pildītu savus uzdevumus saskaņā ar 2018. gada DAL 2. pielikuma 4. punkta 1. apakšpunktu. Turklāt ar minētajiem grozījumiem ir arī izskaidrota samēra pārbaude, kas jāveic, nosakot to, vai datu subjekta tiesību īstenošana varētu apdraudēt efektīvu imigrācijas kontroli un vai tā rezultātā ir nepieciešami un samērīgi ierobežot šādas tiesības.

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

([55]) Ar Datu (izmantošanas un piekļuves) akta 88. panta 2. punktu tiek nedaudz grozīts 2018. gada DAL 26. panta 2. punkta f) apakšpunkts (atbrīvojums valsts drošības un aizsardzības jomā), precizējot to, ka tiesības iesniegt sūdzību Informācijas komisāram saskaņā ar AK VDAR 77. pantu nav daļa no tiem noteikumiem, kuru piemērošanu var ierobežot valsts drošības vai aizsardzības nolūkos.

([56]) Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas brīdī nebija atrisināts jautājums par imigrācijas atbrīvojuma spēkā esamību un interpretāciju saskaņā ar Apvienotās Karalistes tiesību aktiem, jo Anglijas un Velsas Apelācijas tiesa 2021. gada 26. maijā bija pieņēmusi lēmumu, kurā konstatēts, ka 2018. gada Datu aizsardzības likumā tobrīd formulētais imigrācijas atbrīvojums nebija saderīgs ar Apvienotās Karalistes tiesību aktiem, jo tajā nebija konkrētu noteikumu, kuros būtu izklāstītas garantijas, kas izklāstītas AK VDAR 23. panta 2. punktā, kurš atspoguļo Regulas (ES) 2016/679 23. panta 2. punktu. Minētā iemesla dēļ personas dati, kas nosūtīti Apvienotās Karalistes imigrācijas kontroles vajadzībām vai uz kuriem citādi attiecas imigrācijas atbrīvojuma tvērums, bija izslēgti no Īstenošanas lēmuma (ES) 2021/1772 tvēruma.

([57]) Noteikumi stājās spēkā 2022. gada 31. janvārī un ir pieejami šādā vietnē: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Noteikumi stājās spēkā 2024. gada 8. martā un ir pieejami šādā vietnē: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) Ar 2022. gada noteikumiem pārskatītais imigrācijas atbrīvojums atkal tika apstrīdēts, pieprasot pārskatīšanu tiesā un pamatojoties uz to, ka minētais atbrīvojums vēl neatbilda visām AK VDAR 23. panta 2. punkta prasībām. Apelācijas tiesa 2023. gada decembrī konstatēja, ka tas nav saderīgs ar AK VDAR 23. panta 2. punkta prasībām. Minētā sprieduma rezultāts bija tāds, ka ar 2024. gada noteikumiem tiek grozīti 2022. gada noteikumi un veikti turpmāki grozījumi imigrācijas atbrīvojumā.

([60]) 2018. gada DAL 2. pielikuma 4.A punkta 2. apakšpunkts.

([61]) 2018. gada DAL 2. pielikuma 4.AB punkta 3. un 4. apakšpunkts. Par 2024. gada noteikumu projektu notika apspriešanās ar Informācijas komisāra biroju, kas publiski paziņoja, ka piekrīt noteikumiem. Vēstule, kas publicēta kā atbilde uz apspriešanās procedūru un kurā apstiprināts Informācijas komisāra biroja viedoklis, ir pieejama šādā vietnē: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) 2018. gada DAL 2. pielikuma 4.B punkta 1. un 2. apakšpunkts.

([63]) 2018. gada DAL 2. pielikuma 4. punkta 1. apakšpunkts.

(38) Turklāt Apvienotās Karalistes *ICO* ir izdevis detalizētus norādījumus par šā īpašā ierobežojuma izmantošanu ([64]). Norādījumos jo īpaši konstatēts, ka "imigrācijas atbrīvojums nebūtu jāpiemēro kā vispārējs atbrīvojums, lai ierobežotu [..] tiesības attiecībā uz visiem jūsu turētiem datiem. Atbrīvojuma tvērums aprobežojas ar tām tiesībām, kas, ja tās tiktu īstenotas attiecībā uz turētajiem datiem, apdraudētu izvirzītos imigrācijas mērķus. [..] Tādēļ datu pārziņa nostājai pēc noklusējuma vajadzētu būt tādai, ka, ciktāl iespējams, ir jāizpilda Regulas (ES) 2016/679 un DAL prasības. [..] Aizspriedumu pārbaudes veikšanai ir noteikts augsts prasību līmenis, un atbrīvojums nebūtu jāizmanto vispārējā veidā. [..] Jāapsver, vai atbrīvojuma piemērošana ir samērīga reakcija uz fiziskās personas datu aizsardzības pieprasījumu. Varat uzskatīt, ka pastāv neatliekama sociāla vajadzība piemērot imigrācijas atbrīvojumu, taču jāņem vērā arī tas, vai tas atsver jūsu pienākumu pret fiziskām personām saskaņā ar Regulu (ES) 2016/679. Fiziskām personām ir tiesības uz saviem personas datiem, kuras jāņem vērā jebkuros apstākļos, it īpaši piekļuves tiesības. Tādēļ ir svarīgi visos gadījumos apsvērt, vai personas tiesības uz datu aizsardzību ir būtiskākas par konstatēto kaitējuma risku. Atbrīvojuma piemērošanai jābūt samērīgai ar apstākļiem, un rūpīgi jāapsver un jāreģistrē katrs gadījums."

(39) Kopumā jānorāda, ka uz imigrācijas ierobežojumu, kas paredzēts 2018. gada DAL 2. pielikuma 4. punktā, kuru Apvienotās Karalistes valdība pārskatīja 2022. un 2024. gadā un kurš interpretēts judikatūrā ([65]) un *ICO* norādījumos, attiecas vairāki stingri nosacījumi, uz kuru pamata minētais ierobežojums tiek piemērots un kuri ir ļoti līdzīgi Savienības tiesību aktos, it īpaši Regulas (ES) 2016/679 23. pantā, izklāstītajiem nosacījumiem par datu aizsardzības tiesību un pienākumu ierobežošanu svarīgu sabiedrisko interešu mērķu nolūkā, piemēram, tādu kā imigrācijas kontrole.

2.2.5. *Tālākas nosūtīšanas ierobežojumi*

(40) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus no Eiropas Savienības nosūta datu pārziņiem vai apstrādātājiem Apvienotajā Karalistē, joprojām nedrīkst pazemināt, šādus datus tālāk nosūtot saņēmējiem trešā valstī. Kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 74.–82. apsvērumā, kārtība attiecībā uz personas datu starptautisko nosūtīšanu no Apvienotās Karalistes vēl aizvien ir ļoti tuva noteikumiem, kas izklāstīti Regulas (ES) 2016/679 V nodaļā.

(41) Kaut arī ar Datu (izmantošanas un piekļuves) aktu tika grozīta AK VDAR 5. nodaļa par personas datu nosūtīšanu uz trešām valstīm vai starptautiskām organizācijām, tomēr tajā ir saglabāta pamatprasība, saskaņā ar kuru personas datus var nosūtīt trešai valstij vai starptautiskai organizācijai tikai tad, ja nosūtīšanas pamatā ir i) noteikumi, ar kuriem apstiprina nosūtīšanu (jauna terminoloģija attiecībā uz to, kas līdz šim tika aprakstīts kā "noteikumi par aizsardzības līmeņa pietiekamību"), ii) pienācīgas garantijas vai iii) atkāpe īpašās situācijās. Šie vispārīgie datu nosūtīšanas principi ir atspoguļoti jaunajā AK VDAR 44.A pantā ([66]), ar kuru aizstāj 44. pantu un kurā arī precizēts, ka personas datu nosūtīšana uz trešo valsti vai starptautisku organizāciju ir atļauta tikai tad, ja nosūtīšana tiek veikta saskaņā ar citiem AK VDAR noteikumiem.

(42) Konkrēti attiecībā uz noteikumiem, ar kuriem apstiprina nosūtīšanu, AK VDAR 45.A panta 2. punktā ir noteikts, ka valsts sekretārs var pieņemt šādus noteikumus tikai tad, ja viņš uzskata, ka datu aizsardzības pārbaude ir sekmīgi izturēta. Tas nozīmē, ka ar AK VDAR 45.A panta 3. punktu ieviestā iespēja, saskaņā ar kuru valsts sekretārs, pieņemot šādus noteikumus, var ņemt vērā vēlamību atvieglot datu plūsmas, vienmēr ir atkarīga no tā, vai ir sekmīgi izturēta datu aizsardzības pārbaude. Juridiskais standarts datu aizsardzības pārbaudes sekmīgai izturēšanai ir izklāstīts AK VDAR jaunajā 45.B panta 1. punktā, kurā noteikts, ka standarts datu subjektu aizsardzībai saņēmējās valstīs vai starptautiskās organizācijās nedrīkst būt būtiski zemāks nekā standarts, kas attiecībā uz datu subjektiem ir paredzēts konkrētajos Apvienotās Karalistes datu aizsardzības tiesību aktos. AK VDAR 45.B panta 2. punktā ir ietverts neizsmeļošs to elementu saraksts, kuri jāņem vērā, novērtējot to, vai iepriekš minētā pārbaude ir sekmīgi izturēta, piemēram, tādi elementi kā tiesiskuma un cilvēktiesību ievērošana, datu aizsardzības iestādes esamība un tās pilnvaras, tiesiskās aizsardzības vai ārpustiesas tiesiskās aizsardzības kārtība, noteikumi par

([64]) Pieejami šādā vietnē: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

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

([66]) Datu (izmantošanas un piekļuves) akta 85. pants un 7. pielikums.

personas datu nosūtīšanu no valsts vai kādas organizācijas uz citām valstīm vai starptautiskām organizācijām, valsts vai organizācijas attiecīgās starptautiskās saistības, kā arī valsts vai organizācijas struktūra, darbības tradīcijas un kultūra. Kaut arī AK VDAR jaunajā 45.B panta 2. punktā ir pārformulēts attiecīgo elementu saraksts, kas ietverts bijušajā 45. pantā, tomēr jaunajā punktā ir saglabāti minētā saraksta pamatelementi, un tādēļ tas joprojām ir tuvu Regulas (ES) 2016/679 V nodaļā izklāstītajam. Turklāt Apvienotās Karalistes iestādes ir apstiprinājušas, ka valsts sekretārs ņems vērā elementus, kas nav uzskaitīti 45.B panta 2. punktā (piemēram, trešās valsts tiesību aktus un praksi attiecībā uz to, kā publiskās iestādes piekļūst personas datiem tādos nolūkos kā valsts drošība vai tiesībaizsardzība), ciktāl tie ietekmē vispārējo aizsardzības standartu. Apvienotās Karalistes iestādes arī uzskata, ka attiecīgā judikatūra trešā valstī būs būtisks elements, apsverot jautājumus, kuri neizsmeļoša saraksta veidā ir uzskaitīti AK VDAR 45.B panta 2. punktā.

(43) Uz noteikumiem, ar kuriem apstiprina nosūtīšanu, arī turpmāk attieksies 2018. gada DAL 182. pantā noteiktās "vispārējās" prasības procedūrai, kā izklāstīts Īstenošanas lēmuma (ES) 2021/1772 77. apsvērumā. Saskaņā ar šo procedūru valsts sekretāram, ierosinot pieņemt Apvienotās Karalistes noteikumus par aizsardzības līmeņa pietiekamību, ir jāapspriežas ar informācijas komisāru ([67]). Pēc tam, kad valsts sekretārs 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 ([68]).

(44) Attiecībā uz pienācīgām garantijām AK VDAR jaunajā 46. panta 1.A punktā ir noteikts, ka šādu nosūtīšanu var veikt tikai tad, ja attiecīgās garantijas ir paredzētas instrumentos, kuri pieejami saskaņā ar AK VDAR 46. panta 2. un 3. punktu ([69]), un ja datu pārzinis, apstrādātājs vai atbildīgās publiskās struktūras, rīkojoties saprātīgi un samērīgi, uzskata, ka datu aizsardzības pārbaude ir sekmīgi izturēta. Jaunievieslajā 6. un 7. punktā ir precizēts, ka datu aizsardzības pārbaude ir sekmīgi izturēta tad, ja, pateicoties nepieciešamajām garantijām, datu subjektiem piemērojamais aizsardzības standarts pēc datu nosūtīšanas nav būtiski zemāks nekā standarts saskaņā ar attiecīgajiem Apvienotās Karalistes datu aizsardzības tiesību aktiem, t. i., tāpat kā saskaņā ar Regulu (ES) 2016/679, kurā noteikts, ka vieni un tie paši juridiskie standarti attiecas gan uz noteikumiem, ar ko apstiprina datu nosūtīšanu, gan uz pienācīgām garantijām. Tajā pašā punktā ir paredzēts, ka tas, kas ir saprātīgs un samērīgs, ir jānosaka, ņemot vērā visus datu nosūtīšanas vai nosūtīšanas veida apstākļus vai iespējamos apstākļus, tostarp nosūtīto personas datu raksturu un apjomu.

(45) Attiecībā uz atkāpēm īpašās situācijās – AK VDAR 49. pantā par nosacījumiem, uz kuru pamata var tikt piemērotas atkāpes īpašās situācijās, ir ieviesti vairāki tehniski grozījumi, ar kuriem saskaņo atbilstošo noteikumu ar izmaiņām citos noteikumos, taču minētie grozījumi neietekmē personas datu aizsardzības līmeni Apvienotajā Karalistē. Turklāt ir iekļauts jauns 4.A punkts, lai atveidotu ietekmi, ko rada 2018. gada DAL 18. panta 1. punkts, ar kuru valsts sekretāram piešķir pilnvaras ar noteikumu palīdzību precizēt apstākļus tādai datu nosūtīšanai, kas tiek uzskatīta par vajadzīgu sabiedrības interešu dēļ. Visbeidzot, ar jauno 49.A pantu tiek atveidota ietekme, kuru rada 2018. gada DAL 18. panta 2. punkts, ar ko ievieš iespēju, saskaņā ar kuru valsts sekretārs, pieņemot noteikumus, var noteikt ierobežojumus datu nosūtīšanai gadījumos, kad tā nav apstiprināta saskaņā ar 45.A pantu (ar noteikumiem apstiprināta pārsūtīšana) un kad to uzskata par vajadzīgu svarīgu sabiedrības interešu dēļ.

(46) Kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas ir bijušas vairākas norises attiecībā uz starptautiskās nosūtīšanas noteikumu īstenošanu Apvienotajā Karalistē.

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

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

([69]) Nosūtīšanas instruments, kas pieejams saskaņā ar AK VDAR 46. panta 2. un 3. punktu, ir juridiski saistoši un izpildāmi instrumenti publisku iestāžu vai struktūru starpā, saistoši uzņēmuma noteikumi saskaņā ar AK VDAR 47. pantu, standarta datu aizsardzības klauzulas, kuras precizētas valsts sekretāra pieņemtajos noteikumos vai Informācijas komisijas izdotajā dokumentā, apstiprināts rīcības kodekss un apstiprināts sertifikācijas mehānisms.

(47) Saistībā ar noteikumiem, ar kuriem apstiprina nosūtīšanu, līdz šim ir pieņemti divi jauni noteikumi, kas atspoguļo lēmumus par aizsardzības līmeņa pietiekamību, kuri ir spēkā arī Savienībā, t. i., noteikumi par nosūtīšanu uz Korejas Republiku un noteikumi par nosūtīšanu komercstruktūrām, kas pievienojušās ES un ASV datu privātuma regulējuma paplašināšanai, aptverot Apvienoto Karalisti. Noteikumi par aizsardzības līmeņa pietiekamību attiecībā uz Korejas Republiku ([70]) stājās spēkā 2022. gada 19. decembrī, un saskaņā ar tiem ir atļauts nosūtīt personas datus no Apvienotās Karalistes uz Korejas Republiku. Ar ES un ASV datu privātuma regulējuma paplašināšanu, kura aptver Apvienoto Karalisti un kuras attiecīgie noteikumi ([71]) stājās spēkā 2023. gada 12. oktobrī, ir atļauta personas datu brīva plūsma uz sertificētām ASV organizācijām.

(48) Attiecībā uz pienācīgām garantijām Apvienotā Karaliste ir publicējusi savas datu aizsardzības līguma standartklauzulas – Starptautisko datu nosūtīšanas nolīgumu (*IDTA*) ([72]) un papildinājumu ES līguma standartklauzulām (*SCC*); abi stājās spēkā 2022. gada martā. Starptautisko datu nosūtīšanas nolīgumā ir paredzēts īpašs mehānisms Apvienotajai Karalistei, lai tā varētu ievērot pienācīgas garantijas personas datu nosūtīšanai, un tam ir daudzas kopīgas iezīmes ar ES līguma standartklauzulām. Saskaņā ar *ICO* izdoto papildinājumu datu pārziņiem un apstrādātājiem Apvienotajā Karalistē ir atļauts izmantot ES līguma standartklauzulas datu starptautiskai nosūtīšanai atbilstīgi AK VDAR. *ICO* ir arī izstrādājis nosūtīšanas riska novērtēšanas rīku, kura mērķis ir palīdzēt Apvienotās Karalistes organizācijām izvērtēt riskus, kas saistīti ar datu starptautisku nosūtīšanu.

(49) Apvienotā Karaliste ir arī racionalizējusi apstiprināšanas procesu attiecībā uz saistošiem uzņēmuma noteikumiem (SUN), pieņemot jaunus norādījumus un izklāstot jaunas iespējas SUN apstiprināšanai. *ICO* 2022. gada jūlijā publicēja norādījumus un atsauces tabulas, lai izskaidrotu pieeju, ko Apvienotā Karaliste pēc *Brexit* īsteno attiecībā uz saistošiem uzņēmuma noteikumiem, un 2023. gada decembrī tika publicēts papildinājums ES saistošiem uzņēmuma noteikumiem, lai nodrošinātu to, ka saistošie uzņēmuma noteikumi, kuri apstiprināti saskaņā ar Savienības regulējumu, ir izpildāmi Apvienotajā Karalistē ([73]).

(50) Visbeidzot, Apvienotā Karaliste 2023. gada jūlijā kļuva par asociēto locekli Globālajā pārrobežu privātuma noteikumu (*CBPR*) forumā ([74]). Svarīgi ir tas, ka dalība minētajā forumā nekādi neatvieglina datu nosūtīšanu no Apvienotās Karalistes uz citiem *CBPR* foruma dalībniekiem. Apvienotā Karaliste ir precizējusi, ka jebkādai personas datu nosūtīšanai no Apvienotās Karalistes uz trešām valstīm vai starptautiskām organizācijām ir jāatbilst Apvienotās Karalistes tiesību aktos izklāstītajiem, iepriekš aprakstītajiem nosacījumiem, jo īpaši datu aizsardzības pārbaudei, kura paredz to, ka piedāvātie aizsardzības standarti "nedrīkst būt būtiski zemāki" nekā standarti, kas izklāstīti AK VDAR ietvaros.

(51) Kā Komisija jau paskaidroja, *CBPR* nenodrošina pietiekamu aizsardzības līmeni personas datiem, kuru izcelsme ir Eiropas Savienībā. Konkrēti – minētā foruma ietvaros nav paredzētas īstenojamas individuālās tiesības ([75]). Tādēļ ir īpaši svarīgi, ka – kaut arī Apvienotā Karaliste ir Globālā *CBPR* foruma asociētā dalībvalsts – *CBPR* nevar būt derīgs nosūtīšanas mehānisms saskaņā ar Apvienotās Karalistes datu aizsardzības tiesību aktiem. Ja situācija šajā sakarā mainītos, tad tiktu apdraudēts aizsardzības līmenis, kāds pašlaik tiek garantēts personas datiem, kurus no Eiropas Savienības nosūta uz Apvienoto Karalisti. Tādēļ Komisija turpinās cieši uzraudzīt turpmākās norises šajā jomā.

([70]) Pieejami šādā vietnē: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Pieejami šādā vietnē: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Pieejams šādā vietnē: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) *ICO* laikā pēc *Brexit* saņēma ievērojamu skaitu Apvienotās Karalistes SUN pieteikumu. Daudzus apstiprinātos saistošos uzņēmuma noteikumus vairs nebija iespējams izmantot, jo pēc *Brexit* varēja turpināt izmantot tikai tos saistošos uzņēmuma noteikumus, kuru gadījumā *ICO* bija piedalījies to apstiprināšanas procesā, taču šiem saistošo uzņēmuma noteikumu turētājiem bija pienākums iesniegt *ICO* tādus dokumentus par saistošiem uzņēmuma noteikumiem, kuri atbilda atjauninātajai AK VDAR.

([74]) *CBPR* foruma dalībvalstis ir Amerikas Savienotās Valstis, Kanāda, Japāna, Korejas Republika, Filipīnas, Singapūra, Taivāna un Austrālija, savukārt Maurīcija, Dubaijas Starptautiskais finanšu centrs un Bermudu salas ir asociētie locekļi – tāpat kā Apvienotā Karaliste.

([75]) Sk., piemēram, G7 datu aizsardzības iestāžu veikto salīdzinošo analīzi par VDAR sertifikācijas shēmas un *CBPR* sistēmas pamatelementiem, kurā tika atklātas "būtiskas atšķirības" starp abām sistēmām, tostarp attiecībā uz izpildāmību un tiesu iestāžu pieejamību, noteikumiem par neatkarīgu pārraudzību un valdības piekļuvi datiem). Pieejama šādā vietnē: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165.
Sk. 79. apsvērumu Komisijas Īstenošanas lēmumā (ES) 2019/419 (2019. gada 23. janvāris), kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu pietiekamu aizsardzību Japānā atbilstoši Likumam par personas informācijas aizsardzību (OV L 76, 19.3.2019., 1. lpp., ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Sk. arī 29. panta darba grupas Atzinumu 02/2014 par atsauces materiālu saistībā ar prasībām, kuras piemēro attiecībā uz ES valstu datu aizsardzības iestādēm iesniegtiem saistošajiem uzņēmuma noteikumiem un *APEC CBPR* pārskatatbildības ekspertiem iesniegtiem pārrobežu privātuma noteikumiem; 2014. gada 6. marts.

2.2.6. *Automatizēta lēmumu pieņemšana*

(52) Kaut arī Datu (izmantošanas un piekļuves) aktā ir saglabāti vairāki automatizētas lēmumu pieņemšanas noteikumu elementi, kas novērtēti Īstenošanas lēmuma (ES) 2021/1772 54. apsvērumā, tomēr ar minēto aktu ir grozīti daži šo noteikumu aspekti.

(53) Pirmkārt, ar jaunieviesto AK VDAR 22.B pantu tiek noteikts vispārējs aizliegums apstrādāt īpašu kategoriju personas datus (kuri definēti AK VDAR 9. panta 1. punktā), lai pieņemtu lēmumus, kas balstīti tikai uz automatizētu apstrādi, kurai ir juridiska vai līdzīgi būtiska ietekme uz datu subjektu. Taču tajā izklāstīti trīs izņēmumi no šā aizlieguma, proti, datu subjekts ir sniedzis nepārprotamu piekrišanu šādai apstrādei vai lēmums ir nepieciešams, lai noslēgtu vai izpildītu līgumu starp datu pārzini un datu subjektu, vai datu apstrāde ir nepieciešama vai atļauta ar tiesību aktiem. Pēdējo divu izņēmumu gadījumā automatizētajai apstrādei ir jābūt nepieciešamai būtisku sabiedrības interešu dēļ ([76]). Vispārējais aizliegums neattiecas uz nozīmīgiem lēmumiem, kuru pamatā ir tādu datu automatizēta apstrāde, kas nav īpašu kategoriju dati.

(54) Turklāt jaunajā AK VDAR 22.A pantā ir precizēta tāda lēmuma definīcija, kas "balstīts vienīgi uz automatizētu apstrādi", nosakot to, ka šāds lēmums ir tāds, kura pieņemšanas procesā nav bijušas jēgpilnas cilvēka iesaistes. Svarīgi ir tas, ka datu pārziņiem ir jānovērtē, cik lielā mērā profilēšana palīdz pieņemt lēmumu, lai noteiktu to, vai cilvēka iesaiste ir bijusi jēgpilna. AK VDAR 22.A pantā arī precizēts, ka "nozīmīgs lēmums" ir tāds lēmums, kas rada datu subjektam tiesiskas sekas vai būtiski ietekmē viņu līdzīgā veidā ([77]).

(55) Otrkārt, ar jaunieviesto AK VDAR 22.C pantu tiek noteikts, ka datu pārziņiem jāīsteno pasākumi, lai nodrošinātu attiecīgās garantijas saistībā ar jebkuru nozīmīgu lēmumu, kas pilnībā vai daļēji balstīts uz personas datiem un kas pieņemts, izmantojot vienīgi automatizētu apstrādi (tostarp tādu datu apstrādi, kuri nav īpašu kategoriju dati). Šajās garantijās jāietver informācijas sniegšana datu subjektam par lēmumu pieņemšanas procesu, ļaujot datu subjektam apstrīdēt lēmumu un izteikt iebildumus un nodrošinot to, ka datu subjekts var panākt cilvēka iejaukšanos lēmumu pieņemšanas procesā ([78]).

(56) Visbeidzot, ar jaunieviesto AK VDAR 22.D pantu valsts sekretāram tiek piešķirtas pilnvaras pieņemt sekundāros tiesību aktus, lai aprakstītu, kas ir cilvēka jēgpilna iesaiste un kāds lēmums ir uzskatāms par tādu, kuram ir līdzīgi būtiska ietekme uz datu subjektiem. Uz minētā panta pamata valsts sekretārs var arī pieņemt sekundāros tiesību aktus, lai i) pievienotu jaunas garantijas, ii) noteiktu prasības, kas papildina esošās garantijas, un iii) definētu pasākumus, kuri neatbilst garantijām ([79]). Svarīgi ir tas, ka valsts sekretāram, pirms pieņemt noteikumus saskaņā ar AK VDAR 22.D pantu, ir jāapspriežas ar *ICO* ([80]), ka ar minētajiem noteikumiem nedrīkst grozīt AK VDAR 22.C pantu ([81]) un ka šādi noteikumi jāapstiprina ar apstiprinošas rezolūcijas procedūru ([82]), kas nozīmē to apstiprināšanu Apvienotās Karalistes parlamenta abās palātās pirms to pieņemšanas.

(57) Kaut arī ar Datu (izmantošanas un piekļuves) aktu tādējādi ir ticis grozīts automatizētas lēmumu pieņemšanas satvars, tomēr ir svarīgi norādīt, ka atbilstīgi Apvienotās Karalistes tiesiskajam regulējumam uz lēmumu automatizētu pieņemšanu vēl aizvien attiecas būtiskas garantijas, saskaņā ar kurām ir jānodrošina tiesības panākt cilvēka iejaukšanos visos tādu nozīmīgu lēmumu gadījumos, kas balstīti vienīgi uz automatizētu apstrādi, t. i., pamatojoties uz sensitīvu un nesensitīvu personas datu apstrādi ([83]). Turklāt, kā Komisija norādījusi iepriekšējos

([76]) AK VDAR 22.B pants, kas ieviests ar Datu (izmantošanas un piekļuves) akta 80. panta 1. punktu.
([77]) AK VDAR 22.A pants, kas ieviests ar Datu (izmantošanas un piekļuves) akta 80. panta 1. punktu.
([78]) AK VDAR 22.C pants, kas ieviests ar Datu (izmantošanas un piekļuves) akta 80. panta 1. punktu.
([79]) AK VDAR 22.D pants, kas ieviests ar Datu (izmantošanas un piekļuves) akta 80. panta 1. punktu. Visi noteikumi, kas pieņemti saskaņā ar šīm pilnvarām, jāapstiprina ar apstiprinošas rezolūcijas procedūru, tādējādi nodrošinot parlamentāro uzraudzību. Ar noteikumiem nevar grozīt 22.C pantā noteiktās prasības.
([80]) 2018. gada DAL 182. panta 2. punkts.
([81]) AK VDAR 22.D panta 4. punkts.
([82]) AK VDAR 22.D panta 5. punkts.
([83]) AK VDAR 22.C panta 2. punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 80. panta 1. punktu.

lēmumos par aizsardzības līmeņa pietiekamību ([84]), AK VDAR ietvertie īpašie noteikumi par lēmumu automatizētu pieņemšanu, visticamāk, neietekmēs to personas datu aizsardzības līmeni, kurus no Savienības nosūta uz Apvienoto Karalisti. Attiecībā uz personas datiem, kas vākti Savienībā – ikvienu lēmumu, kura pamatā ir automatizēta apstrāde, parasti pieņems Savienībā esošs pārzinis (kam ir tieša saistība ar attiecīgo datu subjektu), un tam tādēļ piemēro Regulas (ES) 2016/679 noteikumus.

2.3. **Pārraudzība un izpilde**

2.3.1. *Neatkarīga pārraudzība*

(58) Apvienotajā Karalistē datu aizsardzības regulējuma pārraudzību un izpildes nodrošināšanu joprojām veic neatkarīga datu aizsardzības uzraudzības iestāde, kā analizēts Īstenošanas lēmuma (ES) 2021/1772 85.–91. apsvērumā. Ar Datu (izmantošanas un piekļuves) aktu tiek reformēta šīs iestādes pārvaldības struktūra, izveidojot juridisku personu – Informācijas komisiju, kura aizstās *ICO*, kas bija strukturēts kā "individuāls komersants".

(59) Konkrētāk – pēc Datu (izmantošanas un piekļuves) aktā izklāstīto pārvaldības pasākumu īstenošanas tiks likvidēts informācijas komisāra birojs, un *ICO* funkcijas, darbinieki un īpašums tiks nodoti jaunajai struktūrai – Informācijas komisijai. Informācijas komisijas sastāvā ir locekļi ar izpildpilnvarām un locekļi bez izpildpilnvarām ([85]). Aktā arī paredzēti noteikumi par informācijas komisāra amata pārveidi par Informācijas komisijas priekšsēdētāju, kas ir viens no locekļiem bez izpildpilnvarām ([86]). Datu (izmantošanas un piekļuves) aktā arī noteikts, ka, ciktāl tas iespējams funkciju nodošanas rezultātā, atsauces uz informācijas komisāru visos noteikumos vai citos dokumentos (pēc to pieņemšanas vai izstrādāšanas) tiek uzskatītas par atsaucēm uz Informācijas komisiju. Lai pildītu savas funkcijas, Informācijas komisija var izveidot komitejas un deleģēt funkcijas kādam komisijas loceklim, darbiniekam vai komitejai ([87]), un tā var paredzēt noteikumus par komisijas reglamentu un komiteju reglamentu, tostarp par kvorumu un lēmumu pieņemšanu ar balsu vairākumu. Šie reglamenti ir jāpublisko ([88]).

(60) Svarīgi ir tas, ka uz Informācijas komisijas neatkarību attiecas tādas pašas garantijas kā tās, kas novērtētas Īstenošanas lēmuma (ES) 2021/1772 87.–90. apsvērumā, tostarp attiecībā uz noteikumiem par priekšsēdētāja iecelšanu un atlaišanu ([89]). Līdzīgas garantijas attiecas arī uz pārējiem Informācijas komisijas locekļiem bez izpildpilnvarām. Konkrēti – Informācijas komisijas priekšsēdētāju ieceļ Viņa Majestāte pēc valsts sekretāra ieteikuma. Priekšsēdētāja atlase notiek, pamatojoties uz nopelniem un saskaņā ar godīgu un atklātu konkursu ([90]). Pārējos locekļus bez izpildpilnvarām ieceļ valsts sekretārs pēc apspriešanās ar priekšsēdētāju. Kandidātus var ieteikt iecelšanai vai iecelt tikai tad, ja viņi ir atlasīti, pamatojoties uz nopelniem un saskaņā ar godīgu un atklātu konkursu, un ja valsts sekretārs ir pārliecinājies par to, ka viņiem nav interešu konflikta ([91]). Locekļi ar izpildpilnvarām ir Informācijas komisijas darbinieki, kas tiek nodarbināti saskaņā ar noteikumiem, kurus noteikuši locekļi bez izpildpilnvarām ([92]). Izpilddirektoru ieceļ priekšsēdētājs un citi locekļi bez izpildpilnvarām pēc apspriešanās ar valsts sekretāru. Arī locekļu ar izpildpilnvarām iecelšana tiek veikta pēc atlases, pamatojoties uz nopelniem un saskaņā ar godīgu un atklātu konkursu ([93]).

(61) Priekšsēdētāju no amata var atbrīvot tikai Viņa Majestāte pēc tam, kad abas parlamenta palātas ir izdarījušas uzrunu, un tikai tad, ja valsts sekretārs abām palātām ir iesniedzis ziņojumu, kurā norādīts, ka valsts sekretārs ir pārliecināts, ka priekšsēdētājs ir vainojams nopietnā pārkāpumā, viņam ir interešu konflikts, viņš nav ievērojis īpašas

([84]) Sk., piemēram, 94. apsvērumu Īstenošanas lēmumā (ES) 2019/419 un 81. apsvērumu Komisijas Īstenošanas lēmumā (ES) 2022/254 (2021. gada 17. decembris), kas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 pieņemts par personas datu pietiekamu aizsardzību Korejas Republikā atbilstīgi Likumam par personas informācijas aizsardzību (OV L 44, 24.2.2022., 1. lpp., ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) 2018. gada DAL 12.A pielikuma 3. punkta 1. apakšpunkts.
([86]) Datu (izmantošanas un piekļuves) akta 117., 118., 119. un 120. pants kopā ar 14. pielikumu.
([87]) 2018. gada DAL 12.A pielikuma 13. un 14. punkts.
([88]) 2018. gada DAL 12.A pielikuma 16. punkts.
([89]) AK VDAR 52. pants, kā arī 2018. gada DAL 12.A pielikums, kas ieviesti ar Datu (izmantošanas un piekļuves) akta 114.A pantu.
([90]) 2018. gada DAL 12.A pielikuma 5. punkta 1. apakšpunkts un 3. punkta 2. apakšpunkts.
([91]) 2018. gada DAL 12.A pielikuma 3. punkta 2. apakšpunkts un 5. un 6. punkts.
([92]) 2018. gada DAL 12.A pielikuma 11. punkts.
([93]) 2018. gada DAL 12.A pielikuma 5. punkta 2. apakšpunkts.

informēšanas prasības attiecībā uz iespējamiem interešu konfliktiem un ka viņš nespēj vai nevēlas pildīt priekšsēdētāja funkcijas vai nav piemērots šādu funkciju veikšanai ([94]). Locekļus bez izpildpilnvarām no amata var atbrīvot valsts sekretārs tikai tad, ja viņš ir pārliecināts, ka ir izpildīti īpašie nosacījumi, kas paredzēti tiesību aktos. Minētie nosacījumi cita starpā ir interešu konflikts, smagi pārkāpumi vai nespēja, nevēlēšanās vai nepiemērotība attiecībā uz to pienākumu pildīšanu. Attiecībā uz papildu garantijām valsts sekretāram ir pienākums publiskot lēmumu par atbrīvošanu no amata un sniegt attiecīgajam loceklim atbrīvošanas pamatojumu ([95]).

(62) Informācijas komisijas galvenais uzdevums arī turpmāk būs datu aizsardzības regulējuma uzraudzība un izpilde Apvienotajā Karalistē, lai "aizsargātu personu pamattiesības un pamatbrīvības" ([96]). Attiecībā uz Informācijas komisijas funkciju nodrošināt personas datu aizsardzības pienācīgu līmeni Datu (izmantošanas un piekļuves) aktā ir īpaši noteikts, ka Informācijas komisija ņems vērā datu subjektu, pārziņu un citu personu intereses un vispārējo sabiedrības interešu jautājumus, kā arī to, lai tiktu veicināta sabiedrības uzticēšanās un paļāvība personas datu apstrādes jomā ([97]). Šie mērķi arī minēti Regulas (ES) 2016/679 7. apsvērumā.

(63) Turklāt Datu (izmantošanas un piekļuves) aktā ir precizēts, ka Informācijas komisija, pildot savas funkcijas saskaņā ar tiesību aktiem datu aizsardzības jomā, apsver inovācijas un konkurences veicināšanu, to, cik svarīgi ir novērst, izmeklēt, atklāt noziedzīgus nodarījumus un saukt pie atbildības par tiem, nepieciešamību garantēt sabiedrisko drošību un valsts drošību, kā arī īpašās vajadzības saistībā ar bērnu aizsardzību ([98]). ES datu aizsardzības tiesību aktos arī atzīta nepieciešamība nodrošināt līdzsvaru starp personas datu aizsardzību un vairākām citām pamattiesībām un mērķiem, piemēram, ekonomisko un sociālo progresu, drošību un tiesiskumu, kā arī darījumdarbības brīvību ([99]).

2.3.2. *Izpildes panākšana, ieskaitot sankcijas*

(64) Informācijas komisijas pilnvaras un uzdevumi joprojām atbilst dalībvalstu datu aizsardzības iestāžu pilnvarām un uzdevumiem saskaņā ar attiecīgajiem Regulas (ES) 2016/679. pantiem ([100]), kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 91.–95. apsvērumā.

(65) Ar Datu (izmantošanas un piekļuves) aktu ir ieviesti konkrēti precizējumi attiecībā uz dažu šo pilnvaru īstenošanu.

(66) No vienas puses, Datu (izmantošanas un piekļuves) aktā ir precizēts, ka Informācijas komisija var pieprasīt specifiskus "dokumentus" un "informāciju" tad, kad tā izmanto informācijas pieprasīšanas pilnvaras ([101]). No otras puses, ar Datu (izmantošanas un piekļuves) aktu tiek ieviestas divas jaunas izmeklēšanas pilnvaras Informācijas komisijai, proti, jaunas pilnvaras pieprasīt ziņojumu ([102]) un jaunas pilnvaras izdot "uzaicinājumus uz interviju" datu pārziņiem gadījumos, kad pastāv aizdomas par AK VDAR vai 2018. gada DAL pārkāpumu ([103]).

([94]) 2018. gada DAL 12.A pielikuma 7. punkta 6. un 7. apakšpunkts.
([95]) 2018. gada DAL 12.A pielikuma 9. punkta 6., 7., 8. un 9 apakšpunkts.
([96]) AK VDAR 51. pants.
([97]) Datu (izmantošanas un piekļuves) akta 91. pants, ar ko ieviests 2018. gada DAL 120.A pants.
([98]) Datu (izmantošanas un piekļuves) akta 91. pants, ar ko ieviests 2018. gada DAL 120.B pants. Ar Datu (izmantošanas un piekļuves) aktu tiek arī ieviests jauns 2018. gada DAL 120.C pants, kurā noteikts, ka Informācijas komisijai jāsagatavo un jāpublicē stratēģija, kas cita starpā atspoguļo veidu, kādā Informācijas komisija apsvērs iepriekš minētos jautājumus un ekonomikas izaugsmes veicināšanu savu regulatīvo funkciju veikšanas gaitā.
([99]) Sk. jo īpaši Regulas (ES) 2016/679 2. un 4. apsvērumu, kā arī 23. pantu.
([100]) AK VDAR 57. un 58. pants.
([101]) Datu (izmantošanas un piekļuves) akta 97. pants, ar ko groza 2018. gada DAL 142. pantu. Apsvērumi par tehnoloģiju ietekmi un to, kāda nozīme ir datu aizsardzībai, lai veidotu uzticēšanos digitālajai ekonomikai, ir daļa no datu aizsardzības regulatoru darbībām gan Apvienotajā Karalistē, gan Eiropas Savienībā. Sk., piemēram, Eiropas Datu aizsardzības kolēģijas 2024. gada ziņojumu, 12. lpp.: "EDAK ir dinamiska un sadarbīga struktūra, kurai ir izšķiroša nozīme datu aizsardzības tiesību aktu konsekventas piemērošanas nodrošināšanā visā Eiropā. Raugoties no manas – priekšsēdētaja vietnieka – perspektīvas, es uzskatu, ka tā aizstāv fizisku personu tiesības uz privātumu, prasmīgi līdzsvarojot inovācijas un ekonomikas izaugsmes vajadzības."
([102]) Datu (izmantošanas un piekļuves) akta 98. pants, ar ko groza 2018. gada DAL 146. pantu.
([103]) Datu (izmantošanas un piekļuves) akta 100. pants, ar ko ieviests 2018. gada DAL 148.A pants.

(67) Attiecībā uz to, kā Informācijas komisija īsteno šīs pilnvaras – informācijas komisārs kopš Īstenošanas lēmuma (ES) 2021/1772 stāšanās spēkā ik gadus ir izskatījis aptuveni 40 000 sūdzību no datu subjektiem; šis skaits līdzinās to sūdzību skaitam, kuras tika izskatītas laikā, kad Apvienotā Karaliste vēl bija Savienības dalībvalsts un piemēroja Regulu (ES) 2016/679 ([104]). *ICO* arī veica *ex officio* izmeklēšanas, kas aptvēra daudzus un dažādus nozaru un atbilstības jautājumus, tostarp datu subjektu tiesības ([105]).

(68) Attiecībā uz izpildes pasākumiem – kopš Īstenošanas lēmuma (ES) 2021/1772 stāšanās spēkā informācijas komisārs ir izteicis 120 rājienus, pieņēmis 32 informatīvos paziņojumus, 3 novērtējuma paziņojumus un 12 izpildes paziņojumus, izdevis 2 brīdinājumus un uzlicis 12 naudas sodus ([106]). Tas ietver vairākus būtiskus naudas sodus, kas uzlikti saskaņā ar AK VDAR un 2018. gada DAL. Piemēram, informācijas komisārs 2023. gada aprīlī piemēroja 12,7 miljonu sterliņu mārciņu lielu naudas sodu sociālo mediju platformai par bērnu datu ļaunprātīgu izmantošanu ([107]). Kādam programmatūras uzņēmumam 2025. gada martā tika uzlikts 3,07 miljonu sterliņu mārciņu liels naudas sods par nepilnībām drošības jomā, kuru dēļ bija apdraudēti vairāk nekā 70 000 cilvēku personas dati ([108]). Pavisam nesen – 2025. gada jūnijā – informācijas komisārs piemēroja 2,31 miljona sterliņu mārciņu lielu naudas sodu kādam ģenētiskās testēšanas uzņēmumam par to, ka tas pēc plaša mēroga kiberuzbrukuma 2023. gada nebija īstenojis pienācīgus drošības pasākumus, lai aizsargātu lietotāju personu datus Apvienotajā Karalistē ([109]).

(69) Kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas informācijas komisāra birojs arī izstrādājis un publicējis ievērojamu skaitu pamatnostādņu, atzinumu un citu norādījumu dokumentu, kuros precizēta datu aizsardzības noteikumu piemērošana tādās svarīgās jomās kā, piemēram, sejas atpazīšana, taisnīgums mākslīgā intelekta jomā, bērnu dati, tiešā tirgvedība, videonovērošana, piekļuves tiesības, pārredzamība veselības, sociālās aprūpes un citās jomās attiecībā pret dažādiem datu lietotājiem, tostarp maziem un vidējiem uzņēmumiem, specifiskām struktūrām, piemēram, skolām, bērnudārziem vai mazām publiskām iestādēm, kā arī attiecībā pret uzņēmumiem kopumā, plašu sabiedrību vai datu subjektiem ([110]).

3. ATTIECĪGĀS NORISES SAISTĪBĀ AR APVIENOTĀS KARALISTES PUBLISKO IESTĀŽU PIEKĻUVI PERSONAS DATIEM, KURUS NOSŪTA NO EIROPAS SAVIENĪBAS, UN ŠĀDU DATU IZMANTOŠANU

3.1. Vispārējais tiesiskais regulējums

(70) Apvienotā Karaliste joprojām ir Eiropas Padomes dalībvalsts, tā ievēro Eiropas Cilvēktiesību konvenciju un uz to attiecas Eiropas Cilvēktiesību tiesas jurisdikcija. Tādēļ uz Apvienoto Karalisti vēl aizvien attiecas pienākumi, kuri, kā aprakstīts Īstenošanas lēmuma (ES) 2021/1772 116.–119. apsvērumā, ir nostiprināti starptautiskajās tiesībās un nosaka Apvienotās Karalistes sistēmu valdības piekļuvei personas datiem, pamatojoties uz principiem, garantijām un individuālām tiesībām, kas ir identiskas tām, kuras tiek piemērotas 27 dalībvalstīm, kas ir ECTK puses, un kuras lielā mērā ir atspoguļotas attiecīgajā Eiropas Savienības Tiesas judikatūrā.

(71) Ar 2018. gada DAL vēl aizvien tiek nodrošinātas īpašas datu aizsardzības garantijas un tiesības gadījumos, kad datus apstrādā Apvienotās Karalistes publiskās iestādes, tostarp tiesībaizsardzības un valsts drošības struktūras, kā analizēts Īstenošanas lēmuma (ES) 2021/1772 121.–132. apsvērumā. Ar Datu (izmantošanas un piekļuves) aktu ir veikti tikai nelieli un mērķorientēti grozījumi tajās 2018. gada DAL daļās, kurās izklāstīti noteikumi par personas datu apstrādi kriminālmtiesību aktu piemērošanas (2018. gada DAL 3. daļa) un valsts drošības (2018. gada DAL 4. daļa) kontekstā.

([104]) Informācijas komisāra gada pārskati par 2021. un 2022. gadu, 2022. un 2023. gadu 2023. un 2024. gadu. Sk. arī Īstenošanas lēmuma (ES) 2021/1772 96. apsvērumu.
([105]) Informācijas komisāra gada pārskats par 2023. un 2024. gadu, 41. lpp.
([106]) Informācijas komisāra gada pārskati par 2021. un 2022. gadu, 2022. un 2023. gadu 2023. un 2024. gadu.
([107]) Plašākai informācijai par šīm un citām izpildes panākšanas darbībām sk. *ICO* tīmekļa vietni, kas pieejama šādā saitē: https://ico.org.uk/action-weve-taken/enforcement/.
([108]) Plašāka informācija pieejama šādā saitē: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.
([109]) Plašāka informācija pieejama šādā saitē: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.
([110]) Pieejami šādā vietnē: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) Attiecībā uz personas datu apstrādi, 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, 2018. gada DAL 3. daļā joprojām ir paredzēti principi, tiesības un pienākumi, kas ir līdzīgi Direktīvā (ES) 2016/680 izklāstītajiem principiem, tiesībām un pienākumiem ([111]).

(73) Konkrēti – šā lēmuma pieņemšanas dienā Komisija ir pieņēmusi lēmumu uz Direktīvas (ES) 2016/680 36. panta 3. punkta pamata, kurā tā konstatē, ka datu aizsardzības režīms, kas piemērojams datu apstrādei, kuru Apvienotās Karalistes krimināLizmeklēšanas iestādes veic krimināltiesību aktu piemērošanas nolūkos, joprojām nodrošina aizsardzības līmeni, kas pēc būtības ir līdzvērtīgs Direktīvā (ES) 2016/680 garantētajam.

(74) Ar Datu (izmantošanas un piekļuves) aktu ir grozīti un konsolidēti spēkā esošie atbrīvojumi, kas izklāstīti 2018. gada DAL 3. daļā un pieejami kompetentajām iestādēm valsts drošības nolūkos. Pamatojoties uz atbrīvojumu sakarā ar valsts drošību, kompetentajām iestādēm ir atļauts nepiemērot konkrētus 2018. gada DAL 3. daļas noteikumus tad, ja atbrīvojums no minētajiem noteikumiem ir vajadzīgs valsts drošības grantēšanas nolūkos ([112]). Minētais atbrīvojums atspoguļo tos atbrīvojumus sakarā ar valsts drošību, kuri paredzēti attiecībā uz personas datu apstrādi saskaņā ar AK VDAR (tie izklāstīti 2018. gada DAL 26. pantā) un saskaņā ar 2018. gada DAL 4. daļu (tie izklāstīti 2018. gada DAL 110. pantā).

(75) Uz atbrīvojumu sakarā ar valsts drošību attiecas tie paši ierobežojumi un garantijas kā uz atbrīvojumiem, kuri paredzēti saskaņā ar AK VDAR un 2018. gada DAL 4. daļu, kā analizēts Īstenošanas lēmuma (ES) 2021/1772 64.–67. apsvērumā un 126. apsvērumā. Konkrēti – atbrīvojumu var piemērot tikai tad, ja un ciktāl tas ir nepieciešams nolūkā garantēt valsts drošību. Tas nav vispārējs atbrīvojums, un datu pārzinim šis atbrīvojums jāizvērtē un jāpiemēro katrā gadījumā atsevišķi ([113]). Turklāt visos atbrīvojuma piemērošanas gadījumos ir jāievēro cilvēktiesību standarti (kuru pamatā ir 1998. gada Cilvēktiesību likums un Eiropas Cilvēktiesību konvencija), kas paredz, ka demokrātiskā sabiedrībā tiesību uz privātumu ierobežojumiem vienmēr jāatbilst nepieciešamības un samērīguma principiem ([114]). Tas arī apstiprināts *ICO* norādījumos par atbrīvojumu sakarā ar valsts drošību piemērošanu ([115]).

(76) Turklāt, pamatojoties uz grozījumiem, kuri ieviesti ar Datu (izmantošanas un piekļuves) aktu ([116]), konkrētu apstrādes darbību, ko veic iestādes, kuru kompetencē ir krimināltiesību aktu piemērošana, var arī reglamentēt ar 2018. gada DAL 4. daļas noteikumiem, kas parasti attiecas tikai uz datu apstrādi, kuru veic valsts drošības iestādes.

([111]) Ar Datu (izmantošanas un piekļuves) akta 69. pantu ievieš (kā 2018. gada DAL jaunu 33. panta 1.A un 40.A punktu) piekrišanas definīciju un nosacījumus, ar kādiem var paļauties uz piekrišanu, kā paredzēts AK VDAR 4. panta 11. punktā un 7. pantā (kas atspoguļo atbilstošos Regulas (ES) 2016/679 noteikumus), tādējādi precizējot piekrišanas jēdzienu un nosacījumus, ar kādiem var paļauties uz piekrišanu gadījumos, ja tā tiek izmantota kā juridiskais pamats personas datu apstrādei, ko kompetentās iestādes veic krimināltiesību aktu piemērošanas nolūkos. Turklāt Datu (izmantošanas un piekļuves) akta 71. panta 7. un 8. punktā ir nedaudz precizēts formulējums, kas izklāstīts 2018. gada DAL 36. panta 1. punktā. Visbeidzot, AK VDAR grozījumi, kas izdarīti ar Datu (izmantošanas un piekļuves) aktu un aprakstīti 2. iedaļā, attiecīgā gadījumā ir atspoguļoti arī 2018. gada DAL 3. daļā; sk. piemēram, 74. panta 2.–5. punktu par sensitīvu datu apstrādi, 76. panta 4.–6. punktu par termiņiem, kādos jāatbild uz datu subjekta pieprasījumiem, 78. panta 2. un 3. punktu par vaicājumiem, kurus veic, atbildot uz datu subjektu pieprasījumiem, un 80. panta 3.–5. punktu par lēmumu automatizētu pieņemšanu.

([112]) 2018. gada DAL 78.A panta 1. punkts, kas ieviests ar Datu (izmantošanas un piekļuves) akta 88. pantu. Kā noteikts 2018. gada DAL 78.A panta 2.–4. punktā, uz atbrīvojuma pamata ir atļauts nepiemērot datu aizsardzības principus (izņemot likumīguma principu, kā arī nosacījumus un garantijas sensitīvu datu apstrādei), individuālās tiesības, datu pārziņu un apstrādātāju pienākumus attiecībā uz datu aizsardzības pārkāpumiem, noteikumu par datu starptautisku nosūtīšanu konkrētas daļas un dažas informācijas komisāra iekļūšanas pilnvaras, lai veiktu pārbaudes un izpildes darbības.

([113]) Sk. lietu *Baker v Secretary of State for the Home Department* (2001), UKIT NSA2 (“*Baker v Secretary of State*”).

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

([115]) Sk. *ICO* norādījumus par atbrīvojumu sakarā ar valsts drošību un aizsardzību; pieejami šādā vietnē: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Datu (izmantošanas un piekļuves) akta 89. un 90. pants.

(77) Kaut arī datu aizsardzības režīms, ko datu apstrādei piemēro valsts drošības nolūkos, tādējādi dažās situācijās tiek attiecināts arī uz datu apstrādi, kuru veic krimināllizmeklēšanas iestādes, tomēr tas tā ir tikai specifiskos apstākļos un atkarībā no stingriem nosacījumiem un garantijām, t. i., tad, ja i) valsts sekretāra pieņemtajos noteikumos, kas jāapstiprina parlamentā, kompetentā iestāde ir norādīta kā "kvalificētā kompetentā iestāde" ([117]), un ii) valsts sekretārs, pieņemot atbilstošu paziņojumu, nosaka konkrētu apstrādes darbību, kuru veic kvalificētā kompetentā iestāde. Svarīgi ir tas, ka iepriekš minētā apstrādes darbības noteikšana var notikt tikai tad, ja valsts sekretārs uzskata, ka apstrādes darbības noteikšana ir vajadzīga valsts drošības grantēšanas nolūkos, t. i., ja krimināllizmeklēšanas iestāde rīkojas valsts drošības nolūkos un ja apstrādes darbību veic kvalificētā kompetentā iestāde kā kopīgs pārzinis kopā ar vismaz vienu izlūkdienestu ([118]). Papildu garantijas ir šādas: valsts sekretāram, pirms pieņemt paziņojumu par apstrādes darbības noteikšanu, ir jāapspriežas ar informācijas komisāru ([119]), paziņojuma teksts principā ir jāpublicē ([120]) un persona, kuru tieši skar paziņojums par apstrādes darbības noteikšanu, var pieprasīt pārskatīšanu tiesā ([121]). Tādēļ šā grozījuma mērķis būtībā ir precizēt to, ka gadījumos, kad Apvienotās Karalistes iestādēm ir pilnvaras gan tiesībaizsardzības, gan valsts drošības jomā, un tās apstrādā datus pēdējo minēto pienākumu kontekstā, tad var piemērot datu aizsardzības režīmu, kurš attiecas uz valsts drošības dienestiem.

(78) 2018. gada DAL 4. daļa reglamentē datu apstrādi, ko veic Apvienotās Karalistes izlūkdienesti. Tajā joprojām ir noteikti svarīgākie datu aizsardzības principi, izklāstīti nosacījumi īpašu kategoriju datu apstrādei, paredzētas datu subjektu tiesības, noteikta prasība par datu integrētu aizsardzību un reglamentēta personas datu nosūtīšana, kā aprakstīts Īstenošanas lēmuma (ES) 2021/1772 125.–132. apsvērumā.

(79) Grozījumiem šajā režīmā, kuri ieviesti ar Datu (izmantošanas un piekļuves) aktu, ir ierobežots apmērs. Attiecībā uz 2018. gada DAL 94. pantā paredzētajām datu subjektu piekļuves tiesībām ar Datu (izmantošanas un piekļuves) aktu ir ieviests jauns 2.A apakšpunkts, kurā precizēts, ka datu subjektam ir tiesības uz attiecīgo informāciju tikai tiktāl, ciktāl datu pārzinis to var sniegt, pamatojoties uz saprātīgu un samērīgu meklēšanu ([122]). Kā paskaidrots 35. apsvērumā, šis grozījums nosaka piekļuves tiesības, pamatojoties uz iedibinātiem juridiskiem standartiem, ar kuriem ņem vērā arī datu subjekta intereses. Automatizētas lēmumu pieņemšanas jomā pārziņiem joprojām ir aizliegts pieņemt lēmumu, kas ievērojami ietekmē datu subjektu un kas pilnībā balstīts uz datu subjekta personas datu automatizētu apstrādi, ja vien šāds lēmums nav prasīts vai atļauts ar tiesību aktiem, datu subjekts ir devis piekrišanu lēmuma pieņemšanai, balstoties uz minēto pamatu, vai lēmums ir pieņemts saistībā ar līgumu ([123]), savukārt ar Datu (izmantošanas un piekļuves) aktu tiek ieviesta (2018. gada DAL 4. daļā) ([124]) jēdziena "lēmumi, kas pilnībā balstīts uz automatizētu apstrādi" tāda pati definīcija, kas ietverta AK VDAR 22.A pantā un analizēta šā lēmuma 53. apsvērumā.

3.2. **Attiecīgās norises saistībā ar Apvienotās Karalistes publisko iestāžu piekļuvi datiem un datu izmantošanu krimināltiesību aktu piemērošanas nolūkā**

(80) Apvienotās Karalistes tiesību aktos joprojām ir noteikti būtiski ierobežojumi piekļuvei personas datiem un to izmantošanai krimināltiesību aktu piemērošanas nolūkā, un tajos ir paredzēti pārraudzības un tiesiskās aizsardzības mehānismi šajā jomā, kā analizēts Īstenošanas lēmuma (ES) 2021/1772 134.–174. apsvērumā.

([117]) 2018. gada DAL 82. panta A1., 2.A un 4. punkts, kas ieviesti ar Datu (izmantošanas un piekļuves) akta 89. panta 2. punktu.

([118]) 82.A panta 1. un 2. punkts, kas ieviesti ar Datu (izmantošanas un piekļuves) akta 89. panta 3. punktu. Papildu garantijas ir šādas: valsts sekretāram, pirms pieņemt paziņojumu par apstrādes darbības noteikšanu, ir jāapspriežas ar komisāru, sk. 2018. gada DAL 82.A panta jauno 8. punktu; paziņojuma teksts principā ir jāpublicē, sk. 82.D panta jauno 1. punktu; uz to attiecas izņēmumi, kas izklāstīti 2018. gada DAL 82.D panta jaunajā 3. punktā; un persona, kuru tieši skar paziņojums par apstrādes darbības noteikšanu, var pieprasīt pārskatīšanu tiesā, sk. 2018. gada DAL jauno 82.E pantu.

([119]) 2018. gada DAL 82.A panta 8. punkts.

([120]) 2018. gada DAL 82.D panta 1. punkts, ievērojot izņēmumus, kas izklāstīti 82.D panta jaunajā 3. punktā.

([121]) 2018. gada DAL 82.E pants.

([122]) Datu (izmantošanas un piekļuves) akta 78. panta 4. punkts.

([123]) 2018. gada DAL 96. pants.

([124]) Kā noteikts 2018. gada DAL 96. panta jaunajā 4. punktā, lēmums ir pilnībā balstīts uz automatizētu apstrādi tad, ja lēmuma pieņemšanas procesā nav paredzēta iespēja cilvēkam akceptēt, noraidīt vai ietekmēt lēmumu. Datu (izmantošanas un piekļuves) akta 80. panta 4. punkta c) apakšpunkts.

3.2.1. *Juridiskais pamats un piemērojamie ierobežojumi/garantijas*

(81) Saskaņā ar Apvienotās Karalistes tiesisko kārtību personas datu vākšana no uzņēmējiem Apvienotajā Karalistē krimināltiesību aktu piemērošanas nolūkos vēl aizvien ir atļauta, pamatojoties uz kratīšanas orderiem un pierādījumu sniegšanas orderiem un ievērojot Īstenošanas lēmuma (ES) 2021/1772 135.–138. apsvērumā aprakstītos nosacījumus un garantijas.

(82) Turklāt ar 2023. gada Nacionālās drošības likumu ([125]), kura mērķis ir novērst tādus draudus valsts drošībai, kurus izraisa spiegošana, sabotāža un personas, kas darbojas ārvalstu uzdevumā, Apvienotās Karalistes policijai ir piešķirtas jaunas pilnvaras iekļūšanai telpās, kratīšanai un izņemšanai, tostarp iespēja iegūt personas datus gadījumos, kad ir pamatots iemesls aizdomām, ka tiks iegūts materiāls, kas, visticamāk, ir pierādījums tam, ka ir izdarīts vai var tikt izdarīts kāds no smagākajiem, 2023. gada Nacionālās drošības likumā ietvertajiem noziedzīgajiem nodarījumiem vai darbībām saistībā ar apdraudējumu no ārvalstīm ([126]). Uz šīm pilnvarām attiecas līdzīgi nosacījumi un garantijas kā tie nosacījumi un garantijas, kas analizēti Īstenošanas lēmumā (ES) 2021/1772 attiecībā uz tobrīd spēkā esošajām pilnvarām. Konkrēti – minēto pilnvaru izmantošanai jābūt atļautai ar orderi, pierādījumu sniegšanas orderi vai paskaidrojumu sniegšanas orderi, ko izdevusi neatkarīga tiesu iestāde pēc konstebla/izmeklēšanas darbinieka pieprasījuma ([127]). Īpaša aizsardzība tiek attiecināta uz konfidenciāliem materiāliem, piemēram, žurnālistikas materiāliem un advokāta un klienta saziņas konfidencialitātei pakļautiem priekšmetiem ([128]). Tāpat ir vajadzīga tiesneša atļauja (pēc atbilstošās amatpersonas pieprasījuma), lai izdotu rīkojumus par informācijas atklāšanu ([129]), rīkojumus informēšanai par klientu ([130]) un konta pārraudzības rīkojumus ([131]), kuri arī izveidoti ar 2023. gada Nacionālās drošības likumu un uz kuriem attiecas īpaši nosacījumi un garantijas, tostarp tas, ka rīkojums tiek prasīts par kādu konkrētu personu, ar mērķi izmeklēt darbību saistībā ar apdraudējumu no ārvalstīm, ka rīkojums uzlabos izmeklēšanas efektivitāti un ka tas netiks izmantots, lai iegūtu informāciju, uz kuru attiecas advokāta un klienta saziņas konfidencialitāte, vai kura ir izslēgta citu iemeslu dēļ, piemēram, žurnālistikas materiāli un konkrēti veselības dati ([132]).

(83) Kā aprakstīts Īstenošanas lēmuma (ES) 2021/1772 139.–141. apsvērumā, Apvienotās Karalistes tiesiskajā regulējumā ir paredzēts, ka konkrētas tiesībaizsardzības iestādes, piemēram, Valsts noziedzības apkarošanas aģentūra (*National Crime Agency*) vai Metropoles policijas dienests (*Metropolitan Police Service*), var arī izmantot mērķorientētas izmeklēšanas pilnvaras saskaņā ar 2016. gada Likumu par izmeklēšanas pilnvarām (2016. gada IPL) ([133]), lai novērstu vai atklātu smagus noziegumus. Konkrētās izmeklēšanas pilnvaras, ko minētās tiesībaizsardzības iestādes var izmantot, ir šādas: mērķorientēta pārtveršana (2016. gada IPL 2. daļa), saziņas datu iegūšana (2016. gada IPL 3. daļa) un mērķorientēta iekārtu noklausīšanās (2016. gada IPL 5. daļa). Gadījumos, kad valsts sekretārs izdod paziņojumus par datu saglabāšanu saskaņā ar 2016. gada IPL 4. daļu, tiesībaizsardzības iestādes arī var piekļūt saglabātajiem saziņas datiem, izmantojot 2016. gada IPL 3. daļā paredzētās saziņas datu iegūšanas pilnvaras.

([125]) Pieejams šādā vietnē: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) 2023. gada Nacionālās drošības likuma 2. pielikums. Attiecīgie noziedzīgie nodarījumi saskaņā ar 2023. gada Nacionālās drošības likumu ir, piemēram, aizsargātas informācijas iegūšana vai izpaušana (1. iedaļa), komercnoslēpuma iegūšana vai izpaušana (3. iedaļa), palīdzība ārvalstu izlūkošanas dienestam (4. iedaļa), sabotāžas veikšana (12. iedaļa) vai konkrētas aizliegtas darbības veikšana ārvalsts labā ar nolūku radīt traucējošu ietekmi (13. iedaļa).

([127]) Sk. 2023. gada Nacionālās drošības likuma 2. pielikuma 2. panta 1. punktu, 3. panta 1. punktu, 4. panta 1. punktu un 10. panta 1. punktu.

([128]) Sk. 2023. gada Nacionālās drošības likuma 2. pielikuma 2. panta 4. punkta b) apakšpunktu, 3. panta 4. punkta b) un c) apakšpunktu, 4. panta 4. punkta b) un c) apakšpunktu un 10. panta 1. punktu.

([129]) Izmantojot 2023. gada Nacionālās drošības likuma 3. pielikumā paredzētos rīkojumus par informācijas atklāšanu, amatpersona var izdot personai paziņojumu, liekot tai sniegt informāciju, uzrādīt dokumentus un/vai atbildēt uz izmeklēšanai būtiskiem jautājumiem, lai apzinātu īpašumu, kas saistīts ar apdraudējumu no ārvalstīm, tostarp konstatētu īpašuma pārvietošanu vai izmantošanu.

([130]) Izmantojot 2023. gada Nacionālās drošības likuma 4. pielikumā paredzētos rīkojumus informēšanai par klientu, amatpersona var izdot finanšu iestādei paziņojumu, lai panāktu, ka tā sniedz visu tādu informāciju par klientu, kura attiecas uz konkrēto personu.

([131]) Izmantojot 5. pielikumā paredzētos konta pārraudzības rīkojumus, finanšu iestādei var pieprasīt, lai finanšu iestāde rīkojumā norādītajā veidā sniegtu amatpersonai tur minēto informāciju par šajā rīkojumā norādīto laikposmu, kas nedrīkst pārsniegt 90 dienas.

([132]) 2023. gada Nacionālās drošības likuma 3. pielikuma 2. panta 1. punkts, 4. pielikuma 1. pants, 5. pielikuma 1. pants.

([133]) Ar 2016. gada Likumu par izmeklēšanas pilnvarām (sk. https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) aizstāja atšķirīgus likumus attiecībā uz saziņas pārtveršanu, iekārtu noklausīšanos un saziņas datu iegūšanu, jo īpaši 2000. gada Likuma par izmeklēšanas pilnvaru regulējumu (*Regulation of Investigatory Powers Act*) I daļu, kas iepriekš sniedza vispārējo tiesisko regulējumu izmeklēšanas pilnvaru izmantošanai tiesībaizsardzības un valsts drošības iestādēs.

(84) Kopš ticis pieņemts Īstenošanas lēmums (ES) 2021/1772, 2016. gada IPL kopā ar 2000. gada Likumu par izmeklēšanas pilnvaru regulējumu (*RIPA*) Anglijai, Velsai un Ziemeļīrijai un 2000. gada Likumu par izmeklēšanas pilnvaru regulējumu (Skotija) attiecībā uz Skotiju (*RIPSA*) joprojām ir juridiskais pamats un nosaka piemērojamos ierobežojumus un garantijas šādu pilnvaru izmantošanai, kā aprakstīts Īstenošanas lēmumā (ES) 2021/1772. Svarīgi ir tas, ka tiesiskajā regulējumā vēl aizvien ir noteikts, ka, lai izmantotu šīs pilnvaras, iestādēm jāsaņem orderis ([134]), kuru izdevusi kompetenta iestāde ([135]) un apstiprinājis neatkarīgs tieslietu komisārs ([136]) (tā dēvētā "divkāršās drošības" procedūra). Šāda ordera iegūšanai joprojām jāveic nepieciešamības un samērīguma pārbaude ([137]).

(85) Vienlaikus, kopš ticis pieņemts Īstenošanas lēmums (ES) 2021/1772, ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām, kuram 2024. gada aprīlī tika saņemta karaliskā piekrišana, ir grozīti konkrēti, specifiski 2016. gada IPL elementi ([138]). Ciktāl šie grozījumi un citas attiecīgās norises skar nosacījumus, ierobežojumus un garantijas saistībā ar to, kā Apvienotās Karalistes publiskās iestādes izmanto iepriekš minētās, Īstenošanas lēmuma (ES) 2021/1772 177.–215. apsvērumā novērtētās konkrētās izmeklēšanas pilnvaras krimināltiesību aktu piemērošanas nolūkā, minētie grozījumi un citas attiecīgās norises ir analizēti turpmākajos punktos. Attiecībā uz Apvienotās Karalistes regulējuma elementiem, kuri nav grozīti ar iepriekš minēto likumu vai kurus nav ietekmējušas citas attiecīgās norises, joprojām ir spēkā Īstenošanas lēmumā (ES) 2021/1772 veiktā analīze.

(86) Attiecībā uz saziņas datu mērķorientētu iegūšanu un saglabāšanu ([139]) vēl aizvien ir spēkā nosacījumi un garantijas, kas reglamentē šīs pilnvaras, kā novērtēts Īstenošanas lēmumā (ES) 2021/1772. Ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām tika precizētas esošās garantijas, ieviešot 2016. gada IPL 11. pantā (kurā nosaka, ka saziņas datu nelikumīga iegūšana no telesakaru operatora ir noziedzīgs nodarījums) sarakstu ar piemēriem par to, kas uzskatāms par minētajā noteikumā ietverto "likumīgo pilnvarojumu" ([140]). Turklāt ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām vēl sīkāk precizēja saziņas datu definīciju, kas ietverta 2016. gada IPL 261. pantā, skaidri norādot to, ka abonenta dati ir uzskatāmi par saziņas datiem ([141]).

([134]) 2016. gada IPL 2. daļas 2. nodaļā ir paredzēts ierobežots skaits gadījumu, kad pārtveršanu var veikt bez ordera. Tostarp šādos gadījumos: pārtveršana ar sūtītāja vai saņēmēja piekrišanu, pārtveršana administratīvos vai izpildes nolūkos, pārtveršana, kas notiek noteiktās iestādēs (cietumos, psihiatriskajās slimnīcās un imigrācijas aizturēšanas iestādēs), kā arī pārtveršana, kura tiek veikta saskaņā ar attiecīgo starptautisko līgumu.

([135]) Lielākajā daļā gadījumu valsts sekretārs ir tā iestāde, kura izdod orderus saskaņā ar 2016. gada IPL, savukārt Skotijas ministri ir pilnvaroti izdot mērķorientētas pārtveršanas orderus, savstarpējās palīdzības orderi un mērķorientētas iekārtu noklausīšanās orderus, kad personas vai telpas, kurās jāveic pārtveršana, un iekārta, kura jānoklausās, atrodas Skotijā (sk. 2016. gada IPL 22. un 103. pantu). Ja notiek mērķorientēta iekārtu noklausīšanās, tiesībaizsardzības iestādes vadītājs (aprakstīts 2016. gada IPL 6. pielikuma 1. un 2. daļā) var izdot orderi saskaņā ar 2016. gada IPL 106. panta nosacījumiem.

([136]) Tieslietu komisāri palīdz izmeklēšanas pilnvaru komisāram (IPK) – neatkarīgai struktūrai, kas pārrauga izlūkošanas aģentūru izmeklēšanas pilnvaru izmantošanu.

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

([138]) Pieejams šādā vietnē: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) Termins "saziņas dati" aptver saziņas "kurš", "kad", "kur" un "kā", bet ne saturu, t. i., teikto vai rakstīto. Saziņas dati varētu ietvert saziņas laiku un ilgumu, nosūtītāja un saņēmēja tālruņa numuru vai e-pasta adresi un dažkārt to ierīču atrašanās vietu, no kurām tika īstenoti telesakari; sk. 2016. gada IPL 261. panta 5. punktu. Ar 2016. gada IPL valsts sekretāram tiek atļauts pieprasīt no telesakaru operatoriem saglabāt saziņas datus, lai virkne publisko iestāžu, tostarp tiesībaizsardzības iestādes un izlūkdienesti, varētu tiem mērķorientēti piekļūt. 2016. gada IPL 4. daļā ir paredzēta saziņas datu saglabāšana, savukārt 3. daļā ir paredzēta saziņas datu mērķorientēta iegūšana. 2016. gada IPL 3. un 4. daļā arī ir noteikti konkrēti ierobežojumi šo pilnvaru izmantošanai un paredzētas īpašas garantijas.

([140]) Piemēram, gadījumos, kad attiecīgā persona iegūst saziņas datus, īstenojot attiecīgās publiskās iestādes likumā noteiktās pilnvaras, vai gadījumos, kad saziņas dati ir iegūti saskaņā ar tiesas rīkojumu vai jebkādu citu tiesas atļauju. 2016. gada IPL 11. panta 3.A punkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 12. panta 3. punktu.

([141]) 261. panta 5.A un 5.B punkts, kas ieviesti ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 13. panta 3. punktu.

(87) Uz tādu paziņojumu izdošanu, ar kuriem tiek prasīta saziņas datu saglabāšana ([142]), joprojām attiecas ierobežojumi un garantijas, kas aprakstītas Īstenošanas lēmuma (ES) 2021/1772 208. un 209. apsvērumā, jo īpaši nepieciešamības un samērīguma prasības, kā arī neatkarīga tieslietu komisāra apstiprinājums. Kaut arī ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām tika ieviesta iespēja šādus paziņojumus atjaunot, tomēr uz jebkuru atjaunošanu attiecas tie paši nepieciešamības un samērīguma nosacījumi, un tai ir vajadzīgs tieslietu komisāra apstiprinājums ([143]).

(88) Attiecībā uz saziņas datiem ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām tika arī grozīta telesakaru operatora definīcija, t. i., datu saglabāšanas paziņojuma iespējamo adresātu definīcija. Šajā definīcijā tagad ir iekļauta jebkura persona, kas "kontrolē vai nodrošina telesakaru sistēmu, kura i) neatrodas (pilnībā vai daļēji) Apvienotajā Karalistē vai netiek kontrolēta no Apvienotās Karalistes un ii) kuru cita persona izmanto, lai piedāvātu vai sniegtu telesakaru pakalpojumus personām Apvienotajā Karalistē" ([144]). Svarīgi ir tas, ka saskaņā ar grozīto definīciju joprojām ir vajadzīga cieša saikne ar Apvienotās Karalistes tirgu. Tādējādi ar grozījumu tiek precizēts, ka 2016. gada IPL tvērumā pilnībā ir aptverti lieli uzņēmumi ar sarežģītām korporatīvajām struktūrām; vienlaikus definīcijas tvērums nav ticis paplašināts tā, lai aptvertu tādu telesakaru pakalpojumu sniedzējus, kas nav vērsti uz personām Apvienotajā Karalistē.. To arī apstiprina skaidrojumi, kuri pievienoti 2024. gada Likumam (grozījumam) par izmeklēšanas pilnvarām un kuros izklāstīts, ka grozījuma mērķis nav ietvert papildu uzņēmumus attiecīgajā 2016. gada IPL tvērumā ([145]), bet tam būtībā ir precizēšanas funkcija.

(89) Visbeidzot, ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām tika arī ieviesti daži mērķtiecīgi grozījumi orderu izdošanas procedūrā, tostarp attiecībā uz mērķorientētu pārtveršanu un mērķorientētu iekārtu noklausīšanos, t. i., attiecībā uz pilnvarām, ko arī var izmantot konkrētas tiesībaizsardzības iestādes Apvienotajā Karalistē, lai novērstu vai atklātu smagus noziegumus. Grozījumi attiecas tikai uz specifisko situāciju, kad šīs pilnvaras tiek izmantotas, lai iegūtu personas, kura ir attiecīgās likumdošanas iestādes deputāts, saziņas datus vai privātu informāciju par šādu personu ([146]). Lai gan orderus saistībā ar mērķorientētu pārtveršanu un iekārtu noklausīšanos parasti var izdot valsts sekretārs un tos apstiprina tieslietu komisārs (sk. Īstenošanas lēmuma (ES) 2021/1772 186.–196. un 210.–215. apsvērumu), tomēr saskaņā ar IPL 26. un 111. pantu papildus ir vajadzīgs premjerministra apstiprinājums tajos gadījumos, kad orderis attiecas uz parlamenta vai citas attiecīgās likumdošanas iestādes deputātu (tā dēvētā "trīskāršās drošības" procedūra). Ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām tagad premjerministram ir atļauts izvirzīt piecus valsts sekretārus, kuri būs pilnvaroti īstenot premjerministra pilnvaras apstiprināt šos orderus – ar nosacījumu, ka atļauja ir steidzami vajadzīga un premjerministrs nevar to piešķirt veselības stāvokļa dēļ vai tādēļ, ka nav piekļuves drošiem saziņas kanāliem. Svarīgi ir tas, ka joprojām ir spēkā ierobežojumi un garantijas attiecībā uz šo orderu izdošanu, kā aprakstīts iepriekš minētajos Īstenošanas lēmuma (ES) 2021/1772 apsvērumos.

3.2.2. *Savāktās informācijas turpmāka izmantošana*

(90) Īstenošanas lēmuma (ES) 2021/1772 142.–156. apsvērumā analizētie nosacījumi joprojām tiek attiecināti uz datu apmaiņu, ko tiesībaizsardzības iestādes veic ar citām iestādēm tādiem nolūkiem, kuriem tie sākotnēji netika vākti (tā dēvētā "tālākā apmaiņa").

([142]) Šādu saskaņā ar 2016. gada IPL 87.–89. panta izdotu paziņojumu par datu saglabāšanu mērķis ir nodrošināt to, ka telesakaru operatori ne ilgāk kā 12 mēnešus saglabā attiecīgos saziņas datus, kuri citādi tiktu izdzēsti, ja tie vairs nebūtu nepieciešami uzņēmējdarbības vajadzībām. Saglabātajiem datiem ir jābūt pieejamiem prasītajā laika posmā, ja publiskajai iestādei vēlāk būtu nepieciešamība tos iegūt, pamatojoties uz 2016. gada IPL 3. daļā paredzēto atļauju saziņas datu mērķorientētai iegūšanai.

([143]) 2016. gada IPL 94.A pants, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 20. panta 4. punktu.

([144]) 2016. gada IPL 261. panta 10. punkta c) apakšpunkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 19. pantu.

([145]) Skaidrojumi, kas pievienoti 2024. gada Likumam (grozījumam) par izmeklēšanas pilnvarām, 359. punkts; pieejami šādā tīmekļa vietnē: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Sk. 2016. gada IPL 26. un 111. pantu.

(91) Attiecībā uz specifisko situāciju saistībā ar datu tālāku nosūtīšanu no Apvienotās Karalistes uz Amerikas Savienotajām Valstīm ir stājies spēkā un kopš 2022. gada oktobra tiek īstenots 2019. gada oktobrī noslēgtais Nolīgums starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā (AK un ASV nolīgums) ([147]). Saskaņā ar AK un ASV nolīgumu uz datiem, kas no Eiropas Savienības nosūtīti pakalpojumu sniedzējiem Apvienotajā Karalistē, varētu attiekties pierādījumu sniegšanas rīkojumi, kurus izdevušas kompetentās ASV tiesībaizsardzības iestādes un kuri ir piemērojami Apvienotajā Karalistē.

(92) Svarīgi ir tas, ka joprojām tiek piemēroti nosacījumi un garantijas, saskaņā ar kuriem šādus rīkojumus var izdot un izpildīt, kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 154. apsvērumā. Konkrēti – datiem, kas iegūti saskaņā ar nolīgumu, tiek nodrošināta aizsardzība, kura ir līdzvērtīga īpašajām garantijām, kas paredzētas tā dēvētajā "ES un ASV jumta nolīgumā" ([148]) un kas visas ir iestrādātas AK un ASV nolīgumā, piemērojot *mutatis mutandis* ([149]).

(93) Kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas Apvienotā Karaliste ir paskaidrojusi, ka tā ir precizējusi (tostarp sadarbojoties ar attiecīgajām personām AK un ASV nolīguma īstenošanas ietvaros) to, kā jumta nolīgumā ietvertās īpašās garantijas, kas bija paredzētas tiesībaizsardzības iestāžu savstarpējās sadarbības nodrošināšanai, tiek pielāgotas un piemērotas specifiskajai datu nosūtīšanai, uz kuru attiecas AK un ASV nolīgums. Konkrēti – Apvienotā Karaliste ir paskaidrojusi, ka jumta nolīgumā ietvertie noteikumi, saskaņā ar kuriem ir paredzēti uzdevumi attiecīgajai kompetentajai iestādei (kura nepastāv tiešas sadarbības kontekstā starp Apvienotās Karalistes pakalpojumu sniedzēju un tiesībaizsardzības iestādi Amerikas Savienotajā Valstīs), tiek interpretēti *mutatis mutandis* kā atsauce uz attiecīgās Puses izraudzīto iestādi (kas definēta AK un ASV nolīgumā) ([150]).

(94) Piemēram, attiecībā uz informācijas drošības incidentu paziņošanu saskaņā ar ES un ASV jumta nolīguma 10. pantu, kurā noteikts, ka ir jāsūta paziņojums pārsūtošajai kompetentajai iestādei, Apvienotā Karaliste ir paskaidrojusi, ka šis noteikums tiek piemērots *mutatis mutandis*, kas nozīmē to, ka paziņojums būtu jānosūta tās Puses izraudzītajai iestādei, no kuras dati tika nosūtīti.

(95) Attiecībā uz atļauju, ko pārsūtošā kompetentā iestāde piešķir pirms personas datu tālākas nosūtīšanas saskaņā ar jumta nolīguma 7. pantu, Apvienotā Karaliste ir precizējusi, ka tā šo noteikumu piemēros *mutatis mutandis*, kas nozīmē, ka tās Puses izraudzītajai iestādei, no kuras dati tika nosūtīti, būs pienākums atļaut jebkādu tālāku nosūtīšanu.

(96) Attiecībā uz jumta nolīguma 8. pantā paredzētajiem pienākumiem par informācijas kvalitātes un integritātes saglabāšanu minētā noteikuma *mutatis mutandis* interpretācija nozīmētu to, ka gadījumos, kad rodas problēmas saistībā ar datu kvalitāti un integritāti, tās Puses izraudzītā iestāde, kura saņem datus, būtu atbildīga par sadarbību ar datu nosūtītāju.

([147]) Nolīgums starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā, pieejams šādā tīmekļa 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.

([148]) Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par personas 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., ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Nolīguma 9. panta 1. punkts.

([150]) Saskaņā ar AK un ASV nolīguma 1. panta 8. punktu "izraudzītā iestāde" ir valdības struktūra, ko attiecībā uz Apvienoto Karalisti ir izraudzījies Iekšlietu ministrijas valsts sekretārs, savukārt attiecībā uz Amerikas Savienotajām Valstīm – ģenerālprokurors.

(97) Attiecībā uz tiesiskās aizsardzības līdzekļiem Apvienotā Karaliste ir uzsvērusi, ka datu nosūtīšanā, ko veic saskaņā ar AK un ASV nolīgumu, vienmēr būs iesaistīta katras Puses izraudzītā iestāde. Gadījumos, kad ASV ir tā Puse, kas saņem datus no pakalpojumu sniedzējiem Apvienotajā Karalistē, ASV Tieslietu departaments darbosies kā izraudzītā iestāde. Tādēļ saskaņā ar Apvienotās Karalistes interpretāciju katrā pieprasījumā, kas izdots uz AK un ASV nolīguma pamata, tiks iesaistīts Tieslietu departaments – federāla iestāde, kura izraudzīta atbilstīgi ASV Tiesiskās aizsardzības aktam, un tādējādi tiesiskās aizsardzības līdzekļus var izmantot attiecībā pret Tieslietu departamentu, kā paredzēts jumta nolīguma 19. pantā. Turklāt Apvienotā Karaliste ir apstiprinājusi Komisijas dienestiem to, ka Tiesiskās aizsardzības akts nav vienīgais mehānisms tiesiskās aizsardzības iegūšanai. Atkarībā no konkrētās lietas apstākļiem un konteksta arī citos piemērojamos ASV tiesību aktos ir paredzēti alternatīvi veidi, kā varētu izmantot tiesiskās aizsardzības līdzekļus.

3.2.3. *Pārraudzība un tiesiskā aizsardzība*

(98) Atkarībā no pilnvarām, ko kompetentās iestādes izmanto, apstrādājot personas datus tiesībaizsardzības nolūkā (vai nu saskaņā ar 2018. gada DAL, vai arī 2016. gada IPL), dažādas struktūras turpina nodrošināt pārraudzību pār šo pilnvaru izmantošanu, kā novērtēts Īstenošanas lēmuma (ES) 2021/1772 158.–174. apsvērumā, un tiesiskās aizsardzības mehānismi vēl aizvien ir pieejami saskaņā ar 2018. gada DAL 3. daļu, 2016. gada IPL un 1998. gada Cilvēktiesību likumu, kā analizēts Īstenošanas lēmuma (ES) 2021/1772 250.–269. apsvērumā.

(99) Attiecībā uz pārraudzību, kas paredzēta 2018. gada DAL 3. daļā, Informācijas komisijas funkcijas un pilnvaras ir analizētas Īstenošanas lēmuma (ES) 2021/1772 158.–160. un 162. apsvērumā, ņemot vērā grozījumus, kas ieviesti ar Datu (izmantošanas un piekļuves) aktu un aprakstīti šā lēmuma 2.3.1. un 2.3.2. iedaļā.

(100) Attiecībā uz šo pilnvaru īstenošanu informācijas komisārs kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas ir izskatījis daudzas sūdzības ([151]), veicis vairākas izmeklēšanas un īstenojis izpildes pasākumus saistībā ar datu apstrādi, ko veic tiesībaizsardzības iestādes. 2021.–2025. gada laikposmā informācijas komisārs veica izmeklēšanu un izteica rājienu dažādām policijas struktūrām par daudzveidīgiem datu aizsardzības pienākumu pārkāpumiem, piemēram, tādiem, kas tikuši izdarīti, atbildot uz pieprasījumiem par piekļuvi datiem, ieviešot drošības pasākumus attiecībā uz videonovērošanas datiem, apstrādājot sensitīvus sodāmības reģistrus, apvienojot dažādu personu datus vai izpaužot personas datus trešām personām ([152]). Informācijas komisārs arī izdeva pamatnostādnes, atzinumus un norādījumus, piemēram, par piekļuves tiesībām vai par to, kā izskatīt acīmredzami nepamatotus vai pārmērīgus pieprasījumus saskaņā ar 2018. gada DAL 3. daļu ([153]).

(101) Attiecībā uz izmeklēšanas pilnvaru izmantošanu saskaņā ar 2016. gada IPL – neatkarīgu un tiesisku pārraudzību joprojām nodrošina izmeklēšanas pilnvaru komisārs (*IPC*), kam palīdz citi tieslietu komisāri, kurus kopā sauc par tieslietu komisāriem ([154]). Šajā jomā ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām ir tikuši izdarīti tikai ierobežoti un mērķorientēti grozījumi, kas neietekmē tieslietu komisāru neatkarību, uzdevumus un pilnvaras, bet kuru mērķis ir stiprināt esošā pārraudzības režīma darbību praksē, jo īpaši ieviešot *IPC* vietniekus, kuriem *IPC* var deleģēt konkrētas pilnvaras tajos gadījumos, kad izmeklēšanas pilnvaru komisāri nespēj pildīt savas funkcijas vai nav pieejami šo funkciju veikšanai. Šādiem *IPC* vietniekiem ir jābūt tieslietu komisāriem, un tos ieceļ izmeklēšanas pilnvaru komisārs ([155]).

([151]) Piemēram, 2023. un 2024. gadā Informācijas komisija saņēma 1 890 sūdzības uz VDAR un/vai 2018. gada DAL pamata par dažādām organizācijām šādās apakškategorijās: "policijas iestāde", "policijas spēki" un "policijas komisāri". Sk. arī informācijas komisāra gada pārskatu un finanšu pārskatus par 2023. un 2024. gadu, pieejami šādā tīmekļa vietnē: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Papildinformācija ir pieejama šādā tīmekļa vietnē: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

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

([154]) Sk. Īstenošanas lēmuma (ES) 2021/1772 250. apsvērumu.

([155]) 2016. gada IPL 227. pants, kas ieviests ar Likuma (grozījuma) par izmeklēšanas pilnvarām 7. pantu.

3.3. Attiecīgās norises saistībā ar Apvienotās Karalistes publisko iestāžu piekļuvi datiem un datu izmantošanu valsts drošības nolūkos

(102) Attiecībā uz izmeklēšanas pilnvarām, kas tiek īstenotas valsts drošības kontekstā, 2016. gada IPL joprojām ir paredzēts tiesiskais regulējums šo pilnvaru izmantošanai. Papildus grozījumiem, kuri skar mērķorientētas izmeklēšanas pilnvaras, ko, ievērojot īpašus nosacījumus, var izmantot arī konkrētas tiesībaizsardzības iestādes, kā aprakstīts šā lēmuma 77.–85. apsvērumā, ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām ir arī veiktas izmaiņas vienā no pilnvarām, kuras paredzētas saskaņā ar 2016. gada IPL un var tikt izmantotas masveidā.

(103) Konkrētāk – ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām 2016. gada IPL jaunajā 7.A daļā ir ieviests īpašs režīms masveida personas datu kopu kādas specifiskas apakškopas ([156]) saglabāšanai un pārbaudīšanai, t. i., saistībā ar tādām datu kopām, kuru gadījumā personām, uz kurām attiecas personas dati, nevarētu būt pamatotas gaidas uz privātuma ievērošanu saistībā ar datiem vai šādas gaidas varētu būt tikai nelielas ([157]). To, vai masveida personas datu kopa ir daļa no šīs specifiskās datu kopu apakškopas, nosaka izlūkdienesta vadītājs, pamatojoties uz visiem apstākļiem, jo īpaši uz šādiem: i) datu raksturs, ii) apmērs, kādā personas publiskojušas datus, vai tas, ka personas ir piekritušas datu publiskošanai, iii) gadījumos, kad dati tikuši publiskoti – apmērs, kādā tie publiskoti, ievērojot redakcionālo atbildību, vai tos publicējusi persona saskaņā ar profesionāliem standartiem, iv) gadījumos, kad dati tikuši publiskoti vai ir citādi publiski pieejami – apmērs, kādā dati ir plaši zināmi, un v) apmērs, kādā dati jau tikuši izmantoti publiskajā telpā ([158]).

(104) Svarīgi ir tas, ka Īstenošanas lēmuma (ES) 2021/1772 239. un 240. apsvērumā novērtētais režīms joprojām ir spēkā attiecībā uz tādu masveida personas datu kopu saglabāšanu un pārbaudīšanu, kuri neietilpst šajā kategorijā (t. i., personas dati, kas ir sensitīvāki un kuru gadījumā tādēļ jābūt pamatotām gaidām uz privātuma ievērošanu), jo īpaši nepieciešamība pēc ordera, kuru vispirms apstiprina valsts sekretārs un pēc tam tieslietu komisārs, ievērojot pasākuma nepieciešamības un samērīguma prasības, kas paredzētas 2016. gada IPL 7. daļā ([159]).

(105) 2016. gada IPL 7.A daļā ir paredzēti šādi divi atļauju veidi: individuāla atļauja un kategorijas atļauja. Visu masveida personas datu kopu, kas tiek glabātas saskaņā ar 7.A daļu, saglabāšanai vai saglabāšanai un pārbaudīšanai ir nepieciešama viena no šīm atļaujām. Abu atļauju piešķiršanai principā ir vajadzīga ([160]) izlūkdienesta vadītāja (vai personas, kas rīkojas viņa vārdā) atļauja un neatkarīga tieslietu komisāra apstiprinājums ([161]). Individuālu atļauju piešķir izlūkdienesta vadītājs, ievērojot 2016. gada IPL 226.B panta 4. punktā izklāstītos nosacījumus un saņemot tieslietu komisāru iepriekšēju apstiprinājumu. Tieslietu komisāram jāizvērtē tās personas izdarītie secinājumi, kura piešķīrusi atļauju, un tas, vai uz atļaujā aprakstīto masveida personas datu kopu attiecas 226.A pants, t. i., vai pamatotas gaidas uz privātuma ievērošanu ir nelielas vai šādu gaidu nav ([162]).

([156]) Masveida personas datu kopu orderi, kas izdoti saskaņā ar 2016. gada IPL 200. pantu, ļauj izlūkošanas aģentūrām glabāt un pārbaudīt datu kopas, kuras satur personas datus, kas attiecas uz vairākām personām, un šīs datu kopas būtība ir tāda, ka, izlūkdienestam pildot savas funkcijas, lielākā daļa šo personu nav un visdrīzāk nebūs tā intereses lokā, un izlūkdienests saglabā minēto datu kopu elektroniski analīzes veikšanai, lai pildītu savas likumā noteiktās funkcijas; sk. arī 2016. gada IPL 199. pantu.

([157]) 2016. gada IPL 226.A panta 1. punkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([158]) 2016. gada IPL 226.A panta 3. punkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([159]) Ar 2024. gada Likumu (grozījumu) par izmeklēšanas pilnvarām ir grozīts 2016. gada IPL 213. pants, nosakot to, ka masveida personas datu kopu orderi zaudē spēku 12 mēnešus pēc to izdošanas. Iepriekš bija noteikts, ka šādi orderi ir jāatjauno ik pēc 6 mēnešiem. Sk. 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 3. pantu.

([160]) Individuālu atļauju var piešķirt bez iepriekšēja tieslietu komisāra apstiprinājuma tikai tad, ja i) persona, kas piešķir individuālo atļauju, uzskata, ka attiecīgā masveida personas datu kopa ietilpst esošajā kategorijas atļaujā, vai ii) steidzamības gadījumā; sk. 2016. gada IPL 226.B panta 6. punktu. Pēdējā minētajā gadījumā lēmums par steidzamas individuālas atļaujas piešķiršanu ir jāizvērtē tieslietu komisāram, darot to trīs darbdienu laikā pēc atļaujas piešķiršanas dienas; sk. 2016. gada IPL 226.BC pantu.

([161]) 2016. gada IPL 226.B panta 1. punkts, kas ieviests ar Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([162]) 2016. gada IPL 226.BB panta 1. punkta a) apakšpunkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

(106) Ar kategorijas atļauju tiek atļauts saglabāt vai saglabāt un pārbaudīt masveida personas datu kopu kategoriju, kas aprakstīta atļaujā.

(107) Lēmumu par kategorijas atļaujas piešķiršanu pieņem izlūkdienesta vadītājs, ja viņš uzskata, ka 226.A pants attiecas uz visām datu kopām attiecīgās kategorijas ietvaros, un ja lēmumu par atļaujas piešķiršanu ir apstiprinājis neatkarīgs tieslietu komisārs ([163]). Tieslietu komisāram jāizvērtē, vai uz visām datu kopām, kas ietilpst atļaujā aprakstītajā datu kopu kategorijā, attiecas 226.A pants, t. i., vai pamatotas gaidas uz privātuma ievērošanu ir nelielas vai šādu gaidu nav ([164]).

(108) Svarīgi ir tas, ka tieslietu komisāram, apstiprinot lēmumu par individuālās vai kategorijas atļaujas piešķiršanu, "ir jāpiemēro tie paši principi, kurus piemērotu tiesa, izskatot pieteikumu par pārskatīšanu tiesā" ([165]), un viņam šie jautājumi jāizskata pietiekami rūpīgi, lai nodrošinātu to, ka tieslietu komisārs pilda pienākumus, kas noteikti ar 2016. gada IPL 2. pantu (vispārējie pienākumi saistībā ar privātumu) ([166]). Turklāt atļauju izdošana ir pakļauta stingrai *ex post* pārraudzībai, proti, ir jāsniedz ikgadēji ziņojumi valsts sekretāram un parlamenta Izlūkošanas un drošības komitejai ([167]) un jāveic regulāras pārbaudes *IPC* birojā ([168]).

(109) Attiecībā uz būtiskajām norisēm pārraudzības jomā *IPC* birojs ir publicējis ikgadējos pārskatus par 2021., 2022. un 2023. gadu, kuros sniegta detalizēta statistika un informācija par to, kā izlūkošanas aģentūras un tiesībaizsardzības iestādes Apvienotajā Karalistē izmanto izmeklēšanas pilnvaras ([169]). Minētajos pārskatos arī aprakstītas biroja veiktās revīzijas un izmeklēšanas, kā arī tajās izdarītie konstatējumi, apstiprinot to, ka *IPC* turpina nodrošināt savu ļoti svarīgo pārraudzības funkciju atbilstīgi Apvienotās Karalistes izmeklēšanas pilnvaru režīmam. Piemēram, 2023. gadā birojs pārbaudīja nepieciešamības un samērīguma pamatojumus saistībā ar to, kā Valdības sakaru štābs (*GCHQ*) izmanto masveida pārtveršanas pilnvaras (kas novērtētas Īstenošanas lēmuma (ES) 2021/1772 218.–225. apsvērumā), secinot, ka lielākā daļa paziņojumu bija formulēti ar pārliecinošu pamatojumu, savukārt dažos gadījumos samērīgums nebija īsti nodrošināts. Šie konstatējumi tika apspriesti ar *GCHQ* atbilstības komandu, kas apņēmās rīkot papildu apmācību iekšējās izpratnes jomā, lai pievērstos šim jautājumam ([170]).

(110) Turklāt Izmeklēšanas pilnvaru tribunāls izdeva publisku ziņojumu par savu darbību un judikatūru 2021.–2023. gada laikposmā ([171]). Ziņojums liecina, ka tribunāla saņemto lietu skaits kopš 2017. gada ir vairāk nekā divkāršojies, un 2023. gadā tika saņemtas vairāk nekā 400 lietas ([172]). Lielākā daļa sūdzību bija vērstas pret tiesībaiz-

([163]) 2016. gada IPL 226.BA pants, kas ieviests ar Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([164]) 2016. gada IPL 226.BB panta 1. punkta b) apakšpunkts, kas ieviests ar Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([165]) 2016. gada IPL 226.BB panta 2. punkta a) apakšpunkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([166]) 2016. gada IPL 226.BB panta 2. punkta b) apakšpunkts, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu. Saskaņā ar vispārējiem pienākumiem saistībā ar privātumu, kuri izklāstīti 2016. gada IPL 2. pantā, publiskajai iestādei jāņem vērā, a) vai mērķi, ko vēlas sasniegt ar orderi, pilnvarojumu vai paziņojumu, varētu pamatoti panākt ar citiem mazāk traucējošiem līdzekļiem, b) vai aizsardzības līmenis, kurš jāpiemēro attiecībā uz informācijas iegūšanu, pamatojoties uz orderi, pilnvarojumu vai paziņojumu, ir augstāks šīs informācijas īpašās sensitivitātes dēļ, c) sabiedrības intereses telesakaru sistēmu un pasta pakalpojumu integritātes un drošības jomā un d) visi citi sabiedrības interešu aspekti privātuma aizsardzības jomā.

([167]) 2016. gada IPL 226.DA un 226.DB pants, kas ieviests ar 2024. gada Likuma (grozījuma) par izmeklēšanas pilnvarām 2. pantu.

([168]) Sk. izmeklēšanas pilnvaru komisāra biroja 2023. gada pārskatu, kas pieejams šādā vietnē: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, 3. lpp.

([169]) Ikgadējie pārskati ir pieejami šādā vietnē: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Sk. 2023. gada pārskata 6.39.–6.43. punktu; pieejams šādā vietnē: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) Izmeklēšanas pilnvaru tribunāla 2021.–2023. gada ziņojums; pieejams šādā vietnē: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) Izmeklēšanas pilnvaru tribunāla 2021.–2023. gada ziņojums, 5. lpp.

sardzības iestādēm, tām cieši sekoja sūdzības pret drošības un izlūkošanas iestādēm ([173]). Svarīgi ir tas, ka tribunāls 2022. un 2023. gadā pasludināja spriedumus lietās, kuras tas bija saņēmis pirms 2021. gada un kurās tas konstatēja, ka Apvienotās Karalistes publiskās iestādes (attiecīgi – Skotijas Policija ([174]), Lielās Mančestras grāfistes Policija ([175]) un Sarijas Policija ([176]), kā arī *MI5* un valsts sekretārs ([177])) bija rīkojušās nelikumīgi. Attiecībā uz tiesiskās aizsardzības līdzekļiem Izmeklēšanas pilnvaru tribunāls cita starpā izdeva rīkojumu iznīcināt visus nelikumīgi iegūtos materiālus, kā arī vienā lietā izdeva rīkojumu samaksāt 12 000 GBP kā taisnīgu kompensāciju par konstatētajiem pārkāpumiem. Tādējādi gada ziņojumā ir apstiprināts, ka Izmeklēšanas pilnvaru tribunāls efektīvi pilda savu svarīgo lomu, proti, garantēt pārraudzību un tiesisko aizsardzību krimināltiesiskās izpildes jomā un attiecībā uz piekļuvi personas datiem valsts drošības nolūkos.

(111) Turklāt ziņojumā arī uzsvērtas svarīgas norises, piemēram, Eiropas Cilvēktiesību tiesas spriedums, kurā tā noteica, ka personas jebkurā pasaules vietā var iesniegt prasību pret Izmeklēšanas pilnvaru tribunālu saistībā ar datu masveida pārtveršanas režīma darbību Apvienotās Karalistē tad, ja attiecīgo rīcību ir izdarījusi Apvienotās Karalistes publiskā iestāde un tā ir veikta Apvienotajā Karalistē ([178]).

4. **SECINĀJUMS**

(112) Komisija uzskata, ka AK VDAR un 2018. gada DAL, kas grozīti ar Datu (izmantošanas un piekļuves) aktu, joprojām nodrošina no Eiropas Savienības nosūtīto personas datu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Regulā (ES) 2016/679 garantētajam līmenim.

(113) Komisija arī uzskata, ka kopumā pārraudzības mehānismi un tiesiskās aizsardzības līdzekļi, kas paredzēti Apvienotās Karalistes tiesību aktos, joprojām 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.

(114) 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, joprojām ir tikai tāds, kas ir absolūti nepieciešams attiecīgā leģitīmā mērķa sasniegšanai, un ka pastāv efektīva tiesiskā aizsardzība pret šādu iejaukšanos.

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

(116) Šis secinājums ir balstīts gan uz attiecīgo Apvienotās Karalistes iekšējo režīmu, kas ir attīstījies kopš Īstenošanas lēmuma (ES) 2021/1772 pieņemšanas, gan uz tās starptautiskajām saistībām, jo īpaši to, ka Apvienotā Karaliste turpina ievērot Eiropas Cilvēktiesību konvenciju un turpina pakļauties Eiropas Cilvēktiesību tiesas jurisdikcijai. Tādēļ šā lēmuma pamatā esošajā novērtējumā šādu starptautisku saistību pastāvīga ievērošana ir īpaši svarīgs elements.

([173]) Izmeklēšanas pilnvaru tribunāla 2021.–2023. gada ziņojums, 12. lpp.
([174]) Lieta *Wilson v Police Scotland* (2022) *UKIPTrib 5*.
([175]) Lieta *Pendlebury v Greater Manchester Police* (2023) *UKIPTrib 2*.
([176]) Lieta *Hill v Metropolitan Police Service & Independent Office For Police Conduct* (2022) *UKIPTrib 6*.
([177]) Lieta *Liberty & Privacy International v Security Service and Secretary of State for the Home Department* (2023) *UKIPTrib 1*.
([178]) Lieta *Wieder* un *Guarnieri* pret AK, (2023) *ECHR* 668; sk. arī Izmeklēšanas pilnvaru tribunāla 2021.–2023. gada ziņojumu, 6. lpp.

5. ŠĀ LĒMUMA SEKAS UN DATU AIZSARDZĪBAS IESTĀŽU RĪCĪBA

(117) 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.

(118) 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 – Īstenošanas lēmuma (ES) 2021/1772, kas grozīts ar šo lēmumu, piemērošanas laikā nosūtīšana no pārziņa vai apstrādātāja Eiropas Savienībā pārziņiem vai apstrādātājiem Apvienotajā Karalistē var notikt bez nepieciešamības saņemt jebkādu turpmāku atļauju.

(119) Vienlaikus būtu jāatgādina, ka saskaņā ar Regulas (ES) 2016/679 58. panta 5. punktu un kā Tiesa paskaidrojusi spriedumā *Schrems I* lietā ([179]), 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 ([180]).

6. UZRAUDZĪBA

(120) Saskaņā ar Regulas (ES) 2016/679 45. panta 4. punktu Komisijai pastāvīgi jāuzrauga attiecīgās norises Apvienotajā Karalistē, lai izvērtētu, vai tā joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Šāda uzraudzība ir īpaši svarīga, jo Apvienotajā Karalistē tiks piemērots un īstenots grozīts datu aizsardzības režīms. Turklāt Apvienotās Karalistes grozītajā datu aizsardzības regulējumā ir paredzētas valsts sekretāra pilnvaras sīkāk precizēt šo regulējumu, pieņemot sekundāros tiesību aktus. Šajā sakarā īpaša uzmanība būtu jāpievērš šādiem papildu precizējumiem un tam, kā Apvienotās Karalistes grozītie noteikumi par personas datu nosūtīšanu uz trešām valstīm tiek piemēroti praksē, kā arī individuālo tiesību izmantošanas efektivitātei, tostarp visām attiecīgajām norisēm tiesību aktu jomā un praksē saistībā ar jaunieviestajiem izņēmumiem no šādām tiesībām vai to ierobežojumiem, pārstrukturētā *ICO* darbībai, tostarp attiecībā uz sūdzību izskatīšanu un korektīvo pilnvaru piemērošanu, kā arī ierobežojumu un garantiju ievērošanai attiecībā uz valdības piekļuvi datiem, jo īpaši saistībā ar 2016. gada IPL jaunieviesto 7.A daļu. Komisijai, īstenojot uzraudzību, cita starpā būtu jāņem vērā jaunākā judikatūra un *ICO* un citu neatkarīgu struktūru veiktā pārraudzība.

(121) 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 Īstenošanas lēmums (ES) 2021/1772, kas grozīts ar šo lēmumu, kā arī par Īstenošanas lēmumā (ES) 2021/1772, kurš grozīts ar šo lēmumu, novērtētās personas datu apstrādes prakses maiņu gan attiecībā uz datu pārziņu un apstrādātāju veiktu personas datu apstrādi saskaņā ar AK VDAR, gan attiecībā uz ierobežojumiem un garantijām, kas piemēro publiskām iestādēm nodrošinātai piekļuvei personas datiem. Tam būtu jāietver norises, kuras attiecas uz 120. apsvērumā minētajiem elementiem.

(122) 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 datu pārziņiem vai 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.

([179]) Lieta *Schrems I*, 65. punkts.

([180]) Lieta *Schrems I*, 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."

(123) Ja pieejamā informācija, jo īpaši informācija, kura iegūta, uzraugot Īstenošanas lēmumu (ES) 2021/1772, kas grozīts ar šo lēmumu, vai informācija, kuru 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 valsts sekretāra 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.

(124) 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.

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

(126) 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 PĀRSKATĪŠANA, DARBĪBAS TERMIŅŠ UN ATJAUNOŠANA

(127) Piemērojot Regulas (ES) 2016/679 45. panta 3. punktu un ņemot vērā to, ka Apvienotās Karalistes tiesiskajā regulējumā paredzētais aizsardzības līmenis var mainīties, Komisijai pēc šā lēmuma pieņemšanas būtu periodiski jāpārskata tas, vai konstatējumi par Apvienotās Karalistes nodrošinātā aizsardzības līmeņa pietiekamību joprojām ir faktiski un juridiski pamatoti, ņemot vērā Regulas (ES) 2016/679 45. panta 2. punktā uzskaitītos elementus. Šādai izvērtēšanai būtu jānotiek vismaz reizi četros gados, un tai būtu jāaptver visi šā lēmuma darbības aspekti, tostarp attiecīgo pārraudzības un izpildes mehānismu darbība.

(128) Lai veiktu pārskatīšanu, Komisijai būtu jātiekas ar attiecīgajiem pārstāvjiem no Apvienotās Karalistes iestādēm, tostarp Informācijas komisijas. Būtu jānodrošina iespēja arī Eiropas Datu aizsardzības kolēģijas pārstāvjiem apmeklēt šādas sanāksmes. Pārskatīšanas ietvaros Komisijai būtu jāprasa, lai Apvienotā Karaliste sniedz vispusīgu informāciju par visiem aspektiem, kas ir būtiski konstatējumam par aizsardzības līmeņa pietiekamību. Komisijai arī būtu jāprasa paskaidrojumi par jebkuru informāciju, kas ir būtiska šim lēmumam un ko tā saņēmusi no Eiropas Datu aizsardzības kolēģijas, individuālām datu aizsardzības iestādēm, pilsoniskās sabiedrības grupām, publiskiem vai plašsaziņas līdzekļu ziņojumiem vai jebkuriem citiem pieejamiem informācijas avotiem.

(129) Pamatojoties uz pārskatīšanu, Komisijai būtu jāsagatavo publisks ziņojums, kas jāiesniedz Eiropas Parlamentam un Padomei.

(130) Komisijai arī jāņem vērā, ka šajā lēmumā un Īstenošanas lēmumā (ES) 2021/1772 novērtētais datu aizsardzības regulējums var mainīties.

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

(132) 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.

8. **NOSLĒGUMA APSVĒRUMI**

(133) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([181]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(134) Šajā lēmumā paredzētais pasākums ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Regulas (ES) 2016/679 93. pantu.

(135) Tāpēc Īstenošanas lēmums (ES) 2021/1772 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Īstenošanas lēmuma (ES) 2021/1772 1. panta 2. punktu atceļ.

2. pants

Īstenošanas lēmuma (ES) 2021/1772 4. pantu aizstāj ar šādu:

"*4. pants*

Šis lēmums zaudē spēku 2031. gada 27. decembrī, ja vien tā termiņš netiek pagarināts saskaņā ar Regulas (ES) 2016/679 93. panta 2. punktā minēto procedūru."

3. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2025. gada 19. decembrī

Komisijas vārdā –
Komisijas loceklis
Michael MCGRATH

([181]) Atzinums 26/2025 par Eiropas Komisijas īstenošanas lēmuma projektu saskaņā ar Regulu (ES) 2016/679 par personas datu pietiekamu aizsardzību Apvienotajā Karalistē; pieejams šādā tīmekļa vietnē: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.