KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2021/1773

(2021. gada 28. jūnijs)

par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680

(izziņots ar dokumenta numuru C(2021) 4801)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā 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 ([1]), un jo īpaši tās 36. panta 3. punktu,

tā kā:

1. IEVADS

(1) Ar Direktīvu (ES) 2016/680 ir paredzēti noteikumi, saskaņā ar kuriem Savienības kompetentās iestādes var nosūtīt personas datus trešām valstīm vai starptautiskām organizācijām, ciktāl šāda nosūtīšana ietilpst tās piemērošanas jomā. Noteikumi par datu starptautisku nosūtīšanu, ko veic kompetentās iestādes, ir izklāstīti Direktīvas (ES) 2016/680 V nodaļā, konkrētāk, 35.–40. pantā. Lai gan personas datu plūsma uz valstīm ārpus Eiropas Savienības un no tām ir būtiska efektīvas tiesībaizsardzības sadarbības nodrošināšanai, ir jāgarantē, ka šāda datu nosūtīšana nemazina Eiropas Savienībā nodrošināto personas datu aizsardzības līmeni ([2]).

(2) Atbilstoši Direktīvas (ES) 2016/680 36. panta 3. punktam Komisija, pieņemot īstenošanas aktu, var nolemt, ka trešā valsts, trešās valsts teritorija vai viens vai vairāki konkrēti sektori trešā valstī, vai starptautiska organizācija nodrošina pietiekamu aizsardzības līmeni. Saskaņā ar šo nosacījumu personas datu nosūtīšana uz trešo valsti var notikt bez nepieciešamības saņemt jebkādu turpmāku atļauju (izņemot gadījumus, kad citai dalībvalstij, no kuras dati iegūti, ir jādod atļauja datu nosūtīšanai), kā paredzēts Direktīvas (ES) 2016/680 35. panta 1. punktā un 66. apsvērumā.

(3) Kā norādīts Direktīvas (ES) 2016/680 36. panta 2. punktā, lēmums par aizsardzības līmeņa pietiekamību jāpieņem, pamatojoties uz visaptverošu trešās valsts tiesību sistēmas analīzi. Komisijai novērtējumā jānosaka, vai attiecīgā trešā valsts garantē aizsardzības līmeni, kurš "pēc būtības ir līdzvērtīgs" Eiropas Savienībā nodrošinātajam (Direktīvas (ES) 2016/680 67. apsvērums). Standarts, pēc kura tiek novērtēta "līdzvērtība pēc būtības", ir paredzēts ES tiesību aktos, jo īpaši Direktīvā (ES) 2016/680, kā arī Eiropas Savienības Tiesas judikatūrā ([3]). Šajā ziņā būtiska nozīme ir arī Eiropas Datu aizsardzības kolēģijas pieņemtajām aizsardzības līmeņa pietiekamības atsaucēm ([4]).

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

([1]) OV L 119, 4.5.2016., 89. lpp.
([2]) Sk. Direktīvas (ES) 2016/680 64. apsvērumu.
([3]) Sk. jaunāko lietu C-311/18 *Maximilian Schrems/Data Protection Commissioner* ("*Schrems II*"), ECLI:EU:C:2020:559.
([4]) Sk. 2021. gada februārī pieņemtos Ieteikumus 01/2021 par pietiekamības atsaucēm saskaņā ar Direktīvu par datu aizsardzību tiesībaizsardzības jomā, pieejami vietnē https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_lv.
([5]) Lieta C-362/14 *Maximillian Schrems/Data Protection Commissioner* ("*Schrems*"), ECLI:EU:C:2015:650, 73. punkts.
([6]) *Schrems*, 74. punkts.
([7]) Komisijas paziņojums 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 vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:52017DC0007&from=LV.

(5) Komisija ir rūpīgi izanalizējusi Apvienotās Karalistes attiecīgos tiesību aktus un praksi. Pamatojoties uz turpmāk izklāstītajiem konstatējumiem, Komisija secina, ka Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni personas datiem, kurus no Savienības kompetentajām iestādēm, uz ko attiecas Direktīva (ES) 2016/680, nosūta Apvienotās Karalistes kompetentajām iestādēm, uz kurām attiecas 2018. gada Datu aizsardzības likuma ("2018. gada DAL") ([8]) 3. daļas darbības joma.

(6) Šā lēmuma rezultātā šāda datu nosūtīšana četru gadu periodā, ko ir iespējams pagarināt, var notikt bez nepieciešamības saņemt jebkādu turpmāku atļauju un neskarot Direktīvas (ES) 2016/680 35. pantā paredzētos nosacījumus.

2. NOTEIKUMI, KURUS PIEMĒRO PERSONAS DATU APSTRĀDEI, KO VEIC KOMPETENTĀS IESTĀDES KRIMINĀLTIESĪBU AKTU PIEMĒROŠANAS NOLŪKĀ

2.1. Konstitucionālais regulējums

(7) Apvienotā Karaliste ir parlamentāra demokrātija. Tai ir suverēns parlaments (augstāks par visām valdības iestādēm), parlamenta izveidota un tā priekšā atbildīga izpildvara, kā arī neatkarīga tiesu vara. Izpildvaras pilnvaras izriet no tās spējas gūt ievēlētās Pārstāvju palātas uzticību, un tā par savu darbību atbild abām parlamenta palātām (Pārstāvju palātai un Lordu palātai), kas ir atbildīgas par valdības pārbaudi, kā arī tiesību aktu apspriešanu un to pieņemšanu. Apvienotās Karalistes parlaments ir deleģējis Skotijas parlamentam, Velsas parlamentam (*Senedd Cymru*) un Ziemeļīrijas asamblejai atbildību par tiesību aktu izstrādi attiecībā uz dažiem Skotijas, Velsas un Ziemeļīrijas vietējiem jautājumiem. Lai gan datu aizsardzība ir Apvienotās Karalistes parlamenta kompetencē, t. i., vienus un tos pašus tiesību aktus piemēro visā valstī, citas ar šo lēmumu saistītās politikas jomas ir decentralizētas. Piemēram, Skotijas un Ziemeļīrijas krimināltiesību sistēmas, tostarp policijas darbs (policijas vienību veiktās darbības), ir deleģētas attiecīgi Skotijas parlamentam un Ziemeļīrijas asamblejai ([9]).

(8) Lai gan Apvienotajā Karalistē nepastāv kodificēta konstitūcija kā iesakņojies konstitucionāls dokuments, tās konstitucionālie principi ir attīstījušies laika gaitā, jo īpaši no judikatūras un paražām. Ir atzīts, ka dažiem likumiem, piemēram, Lielajai brīvības hartai, 1689. gada Tiesību likumam un 1998. gada Cilvēktiesību likumam, ir konstitucionāls saturs. Cilvēka pamattiesības kā daļa no konstitūcijas ir attīstītas, izmantojot anglosakšu tiesības, likumus un starptautiskos līgumus, jo īpaši Eiropas Cilvēktiesību konvenciju (ECTK), ko Apvienotā Karaliste ratificēja 1951. gadā. Apvienotā Karaliste 1987. gadā ir arī ratificējusi Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi (Konvencija Nr. 108) ([10]).

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

([8]) 2018. gada Datu aizsardzības likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, F sadaļa "Tiesībaizsardzība"; dokuments pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

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

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

(10) Saskaņā ar 1998. gada Cilvēktiesību likumu visām publisko iestāžu darbībām jābūt saderīgām ar tiesībām, ko garantē saskaņā ar ECTK ([12]). Turklāt primārie un sekundārie tiesību akti ir jāskata un jāpiemēro tā, lai tie būtu saderīgi ar šīm tiesībām ([13]). Ja persona uzskata, ka publiskās iestādes ir pārkāpušas tās tiesības, tostarp tiesības uz privātumu un datu aizsardzību, tā var saņemt kompensāciju, vēršoties Apvienotās Karalistes tiesās saskaņā ar 1998. gada Cilvēktiesību likumu, bet pēc valsts tiesiskās aizsardzības līdzekļu izsmelšanas – saņemt kompensāciju, vēršoties Eiropas Cilvēktiesību tiesā par ECTK garantēto tiesību pārkāpumiem.

2.2. **Apvienotās Karalistes datu aizsardzības regulējums**

(11) Apvienotā Karaliste 2020. gada 31. janvārī izstājās no Eiropas Savienības. Pamatojoties uz Līgumu par Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes izstāšanos no Eiropas Savienības un Eiropas Atomenerģijas kopienas ([14]), Savienības tiesību aktu piemērošana Apvienotajā Karalistē turpinājās pārejas periodā līdz 2020. gada 31. decembrim. Pirms izstāšanās un pārejas periodā tiesisko regulējumu personas datu aizsardzībai Apvienotajā Karalistē attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, veidoja attiecīgās 2018. gada Datu aizsardzības likuma daļas, ar ko bija transponēta Direktīva (ES) 2016/680.

(12) Veicot sagatavošanās pasākumus nolūkā izstāties no ES, Apvienotās Karalistes valdība pieņēma 2018. gada Likumu par izstāšanos no Eiropas Savienības (LIES) ([15]), ar ko Apvienotās Karalistes tiesību aktos iekļāva tieši piemērojamus Savienības tiesību aktus, un noteica, ka tā dēvētie "no ES atvasinātie valsts tiesību akti" turpina būt spēkā arī pēc pārejas perioda beigām. 2018. gada DAL 3. daļa ([16]), ar ko transponē Direktīvu (ES) 2016/680, saskaņā ar LIES ir "no ES atvasināts valsts tiesību akts". LIES paredz, ka Apvienotās Karalistes tiesām negrozītie "no ES atvasinātie valsts tiesību akti" ir jāinterpretē saskaņā ar Eiropas Savienības Tiesas (EST) attiecīgo judikatūru un Savienības tiesību aktu vispārējiem principiem, kas bija spēkā tieši pirms pārejas perioda beigām (attiecīgi "saglabātā ES judikatūra" un "saglabātie ES tiesību aktu vispārējie principi") ([17]).

(13) Saskaņā ar LIES Apvienotās Karalistes ministri ir pilnvaroti, izmantojot normatīvos aktus, pieņemt sekundāros tiesību aktus ar mērķi veikt saglabātajos Eiropas Savienības tiesību aktos nepieciešamos grozījumus, kas izriet no Apvienotās Karalistes izstāšanās no Eiropas Savienības. Šīs pilnvaras tika izmantotas ar 2019. gada Datu aizsardzības, privātuma un elektronisko sakaru (ar grozījumiem) (Izstāšanās no ES) noteikumiem (DAPES noteikumi ([18])). Ar tiem tiek grozīti Apvienotās Karalistes datu aizsardzības tiesību akti, tostarp 2018. gada DAL, lai tie atbilstu vietējam kontekstam ([19]).

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

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

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

([15]) 2018. gada Likums par izstāšanos no Eiropas Savienības, pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/16/contents.

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

([17]) 2018. gada LIES 6. pants.

([18]) 2019. gada Datu aizsardzības, privātuma un elektronisko sakaru (ar grozījumiem) (Izstāšanās no ES) noteikumi, pieejami vietnē https://www.legislation.gov.uk/uksi/2019/419/contents/made, ar grozījumiem, kas izdarīti ar 2020. gada DAPES, pieejami vietnē https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) Ar Izstāšanās noteikumiem 2018. gada DAL 3. daļā ir izdarīti vairāki grozījumi. Daudzas ir tehniskas izmaiņas, piemēram, svītrojot atsauces uz "dalībvalsti" vai "Tiesībaizsardzības direktīvu" (sk., piemēram, 2018. gada DAL 48. panta 8. punktu vai 73. panta 5. punkta a) apakšpunktu attiecībā uz "valsts tiesību aktiem"), lai pēc pārejas perioda beigām 3. daļa faktiski darbotos kā valsts tiesību akti. Dažās vietās bija nepieciešamas citu veidu izmaiņas, piemēram, attiecībā uz to, kurš pieņem "lēmumus par aizsardzības līmeņa pietiekamību" Apvienotās Karalistes datu aizsardzības tiesiskā regulējuma vajadzībām (sk. 2018. gada DAL 74.A pantu), proti, nevis Eiropas Komisija, bet ministrs.

(14) Līdz ar to juridiskie standarti par to, kā kompetentās iestādes apstrādā personas datus, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai lai izpildītu krimināLsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu Apvienotajā Karalistē pēc pārejas perioda, kas noteikts Izstāšanās līgumā, aizvien būs noteikti attiecīgajā 2018. gada DAL daļā, taču ar grozījumiem, kas izdarīti ar DAPES noteikumiem, jo īpaši minētā likuma 3. daļā. Uz šādu apstrādi neattiecas Apvienotās Karalistes Vispārīgā datu aizsardzības regula (Apvienotās Karalistes VDAR).

(15) 2018. gada DAL 3. daļā ir paredzēti noteikumi par personas datu apstrādi krimināltiesību aktu piemērošanas nolūkā, tostarp datu aizsardzības principi, apstrādes juridiskais pamatojums (likumīgums), datu subjektu tiesības, kompetento iestāžu kā pārziņu pienākumi un tālākas nosūtīšanas ierobežojumi. Savukārt piemērojamie noteikumi par pārraudzību, izpildi un kompensācijām, ko piemēro tiesībaizsardzības jomā, ir paredzēti 2018. gada DAL 5. un 6. daļā.

(16) Turklāt, ņemot vērā policijas vienību attiecīgo lomu tiesībaizsardzības jomā, būtu jāapsver noteikumi, kas regulē policijas darbību. Tā kā policijas jautājumi ir deleģēti, policijas darbam a) Anglijā un Velsā, b) Skotijā un c) Ziemeļīrijā piemēro dažādus tiesību aktus, kuru saturs gan bieži vien ir līdzīgs ([20]). Turklāt dažādos norādījumu dokumentos ir papildus skaidrots, kā būtu jāīsteno policijas pilnvaras. Ir trīs galvenie policijas norādījumu veidi: 1) uz likuma pamata izdotie norādījumi, kas izdoti saskaņā ar tiesību aktiem, piemēram, Ētikas kodekss ([21]) un Policijas informācijas pārvaldības prakses kodekss (PIP prakses kodekss) ([22]), kas izdoti saskaņā ar 1996. gada Policijas likumu ([23]), vai LPPK kodeksi ([24]), kas izdoti saskaņā ar Likumu par policiju un pierādījumiem krimināllietās ([25]), 2) Atļautā profesionālā prakse policijas informācijas pārvaldībai (APP norādījumi par policijas informācijas pārvaldību), ko izdevusi Policijas kolēģija ([26]), un 3) operatīvie norādījumi (ko publicē pati policija). Valsts policijas priekšnieku padome (visu Apvienotās Karalistes policijas vienību koordinējošā iestāde) publicē operatīvos norādījumus, kurus ir apstiprinājušas visas policijas vienības un kuri tādējādi ir piemērojami visā valstī ([27]). Šo norādījumu mērķis ir panākt, ka policijas vienības pārvalda informāciju vienveidīgi ([28]).

(17) PIP prakses kodeksu 2005. gadā izdeva ministrs, izmantojot ar 1996. gada Policijas likuma 39.A pantu piešķirtās pilnvaras ([29]). Saskaņā ar Policijas likumu izdotie kodeksi vai prakse ir jāapstiprina ministram, un pirms to iesniegšanas parlamentā ir jāapspriežas ar Valsts noziedzības apkarošanas aģentūru. Policijas likuma 39.A panta 7. punktā ir noteikts, ka policijai ir pienācīgi jāievēro saskaņā ar likumu izdotie kodeksi, tāpēc ir gaidāms, ka

([20]) Lai iegūtu sīkāku skaidrojumu par policijas vienībām un to pilnvarām Apvienotajā Karalistē, sk. Apvienotās Karalistes paskaidrojuma dokumentu aizsardzības līmeņa pietiekamības apspriešanai, F sadaļu "Tiesībaizsardzība" (sk. 9. zemsvītras piezīmi).

([21]) Anglijas un Velsas policijas darbinieku profesionālās uzvedības principu un standartu prakses kodekss, pieejams vietnē https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Ziemeļīrijas Policijas dienesta Ētikas kodekss, pieejams vietnē https://www.nipolicingboard.org.uk/psni-code-ethics; Skotijas policijas darba ētikas kodekss, pieejams vietnē https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Policijas informācijas pārvaldības prakses kodekss, pieejams vietnē http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) 1996. gada Policijas likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) 1984. gada Likuma par policiju un pierādījumiem krimināllietās (LPPK) prakses kodeksi, pieejami vietnē https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) 1984. gada Likums par policiju un pierādījumiem krimināllietās, pieejams vietnē https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Atļautā profesionālā prakse policijas informācijas pārvaldībai, pieejama vietnē https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Datu aizsardzības rokasgrāmata policijas datu aizsardzības speciālistiem, pieejama vietnē https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Piemēram, PIP prakses kodekss (sk. 22. zemsvītras piezīmi) attiecas uz operatīvās policijas informācijas glabāšanu (sk. šā lēmuma 47. apsvērumu).

([29]) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju laikā, kad notika sarunas par aizsardzības līmeņa pietiekamību, Policijas kolēģija izstrādāja Informācijas un ierakstu pārvaldības prakses kodeksu, lai aizstātu PIP prakses kodeksu. Kodeksa projekts tika publicēts sabiedriskajai apspriešanai 2021. gada 25. janvārī, un tas ir pieejams vietnē https://www.college.police.uk/article/information-records-management-consultation.

policija to ievēros ([30]). Turklāt neobligātajiem norādījumiem (piemēram, APP norādījumiem par policijas informācijas pārvaldību) vienmēr ir jāsaskan ar PIP prakses kodeksu, kas ir par to svarīgāks ([31]). Jebkurā gadījumā, lai gan varētu būt atsevišķas operatīvās situācijas, kad policijas ierēdņiem ir jāatkāpjas no šiem norādījumiem, viņiem joprojām ir jāievēro 2018. gada DAL 3. daļas prasības ([32]).

(18) Papildu norādījumus par Apvienotās Karalistes datu aizsardzības tiesību aktiem attiecībā uz datu apstrādi tiesībaizsardzības jomā sniedz informācijas komisārs (informācijas komisārs vai informācijas komisāra birojs (IKB)) ([33]) (vairāk par IKB sk. 93.–109. apsvērumā). Lai gan norādījumi nav juridiski saistoši, tiesai tiesvedībā būtu pienākums ņemt vērā norādījumu pārkāpumus, jo tiem ir interpretējošs spēks un tie apliecina, kā komisārs interpretē un piemēro praksē datu aizsardzības tiesību aktus ([34]).

(19) Visbeidzot, kā minēts 8.–10. apsvērumā, Apvienotās Karalistes tiesībaizsardzības iestādēm ir jānodrošina atbilstība ECTK un Konvencijai Nr. 108.

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

2.3. **Materiālā un teritoriālā piemērošanas joma**

(21) 2018. gada DAL 3. daļas materiālā piemērošanas joma atbilst Direktīvas (ES) 2016/680 2. panta 2. punktā noteiktajai darbības jomai. 3. daļa attiecas uz personas datu apstrādi, ko kompetentā iestāde pilnībā vai daļēji veic ar automatizētiem līdzekļiem, un uz kompetentās iestādes veiktu personas datu apstrādi bez automatizētiem līdzekļiem, ja tie veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas.

(22) Turklāt pārzinim, lai uz to attiektos minētā 3. daļa, ir jābūt "kompetentajai iestādei" un apstrāde jāveic "tiesībaizsardzības nolūkā". Tādēļ šajā lēmumā vērtētais datu aizsardzības režīms attiecas uz visām šo kompetento iestāžu tiesībaizsardzības darbībām.

(23) Jēdziens "kompetentā iestāde" DAL 30. pantā ir definēts kā persona, kas minēta 2018. gada DAL 7. pielikumā, kā arī jebkura cita persona, ja tai ir likumā noteiktas jebkāda tiesībaizsardzības nolūka funkcijas. 7. pielikumā norādītās kompetentās iestādes ietver ne tikai policijas vienības, bet arī visas Apvienotās Karalistes ministriju nodaļas un citas iestādes, kas veic izmeklēšanas funkcijas (piem., Viņas Majestātes ieņēmumu un muitas komisāru, Velsas Ieņēmumu pārvaldi, Konkurences un tirgu iestādi, Viņas Majestātes Zemes reģistru vai Valsts noziedzības apkarošanas aģentūru), prokuratūras aģentūras, citas krimināltiesību aģentūras un citas personas vai organizācijas, kas veic

([30]) Lietā *R v the Commission of the Police of the Metropolis* (2014), EWCA Civ 585, tika apstiprināts PIP prakses kodeksa juridiskais statuss, un apelācijas tiesnesis *John Laws* paziņoja, ka Metropoles policijas komisāram ir pienākums ņemt vērā PIP prakses kodeksu un ievērot PIP prakses kodeksu un APP norādījumus par policijas informācijas pārvaldību saskaņā ar 1996. gada Policijas likuma 39.A pantu.

([31]) Viņas Majestātes Policijas un ugunsdzēsības un glābšanas dienestu inspekcija (*HMICFRS*) pārbauda, kā policija ievēro PIP prakses kodeksu.

([32]) Šajā sakarā skatīt Policijas kolēģijas nostāju attiecībā uz atbilstību APP norādījumiem par visiem policijas darbības aspektiem, kurā paskaidrots, ka "Atļauto profesionālo praksi (APP) ir apstiprinājusi profesionāla struktūra policijas jomā (Policijas kolēģija) kā oficiālu policijas profesionālās prakses avotu. No policijas ierēdņiem un personāla tiek gaidīts, ka tie, pildot savus pienākumus, ievēros APP. Tomēr var būt apstākļi, kad ir likumīgs, ar operatīvo darbību saistīts iemesls, lai policijas vienība atkāptos no APP, ja vien tam ir skaidrs pamatojums. Šādā gadījumā policijas vienībai jāuzņemas atbildība par jebkuru risku vietējā un valsts mērogā, kas saistīts ar darbošanos ārpus valstī pieņemtajām pamatnostādnēm, un, ja tādēļ notiek incidents vai tiek uzsākta izmeklēšana (piemēram, ar Neatkarīgā policijas rīcības biroja starpniecību), policijas vienība atbild par jebkādu risku"; pieejams vietnē https://www.app.college.police.uk/faq-page/.

([33]) Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Skatīt lietu *Bridges v the Chief Constable of South Wales Police* (2019), EWHC 2341 (Admin), kurā Augstā tiesa, gan norādot, ka komisāra norādījumiem nav likumisks raksturs, tomēr konstatēja, ka, "vērtējot, vai pārzinis ir vai nav izpildījis 64. panta pienākumu [veikt novērtējumu par ietekmi uz datu aizsardzību saistībā ar augsta riska apstrādi], Tiesa ņems vērā norādījumus, ko attiecībā uz novērtējumiem par ietekmi uz datu aizsardzību ir izdevis informācijas komisārs".

tiesībaizsardzības darbības ([35]). 2018. gada DAL 3. daļa, izņemot sadaļu par datu subjekta tiesībām un IKB pārraudzību, attiecas arī uz tiesām un tribunāliem, kad tie pilda savas tiesas funkcijas ([36]). 7. pielikumā norādītais kompetento iestāžu saraksts nav galīgs, un ministrs to var atjaunināt saskaņā ar noteikumiem, ņemot vērā izmaiņas valsts iestāžu organizācijā ([37]).

(24) Minētajai apstrādei jābūt arī "tiesībaizsardzības nolūkā", kas definēts kā noziedzīgu nodarījumu novēršana, izmeklēšana, atklāšana vai saukšana pie atbildības par tiem vai krimināl sodu izpilde, tostarp aizsardzība pret draudiem sabiedriskajai drošībai un to novēršana ([38]). Ja apstrāde ko veic kompetentā iestāde, nenotiek tiesībaizsardzības nolūkā, 2018. gada DAL 3. daļa uz to neattiecas. Tas tā ir, piemēram, tad, kad Konkurences un tirgu iestāde izmeklē lietas, kurās nav paredzēta krimināl atbildība (piemēram, uzņēmumu apvienošanās). Šādā gadījumā piemēros Apvienotās Karalistes VDAR kopā ar 2018. gada DAL 2. daļu, jo kompetentās iestādes apstrādā personas datus ar tiesībaizsardzību nesaistītā nolūkā. Lai noteiktu, kāds datu aizsardzības režīms piemērojams (2018. gada DAL 3. vai 2. daļa) attiecīgo personas datu apstrādei, kompetentajai iestādei, proti, pārzinim, ir jāizvērtē, vai šādas apstrādes primārais nolūks ir viens no tiesībaizsardzības nolūkiem saskaņā ar 2018. gada DAL.

(25) Attiecībā uz 2018. gada DAL 3. daļas teritoriālo piemērošanas jomu 207. panta 2. punktā noteikts, ka DAL attiecas uz personas datu apstrādi saistībā ar tādas personas darbībām, kura darbojas visā Apvienotās Karalistes teritorijā. Tas ietver Anglijas, Velsas, Skotijas un Ziemeļīrijas teritoriju publiskās iestādes, kuras ietilpst 2018. gada DAL 3. daļas materiālajā piemērošanas jomā ([39]).

2.3.1. *Personas datu un apstrādes definīcija*

(26) Personas datu un apstrādes pamatjēdzieni ir definēti 2018. gada DAL 3. pantā, un tos piemēro visam DAL. Šīs definīcijas ir ļoti tuvas attiecīgajām definīcijām Direktīvas (ES) 2016/680 3. pantā. Saskaņā ar 2018. gada DAL personas dati ir jebkāda informācija, kas attiecas uz identificētu vai identificējamu dzīvu fizisku personu ([40]). Saskaņā ar 2018. gada DAL 3. panta 3. punktu fiziska persona ir identificējama, ja to var tieši vai netieši identificēt pēc informācijas, tostarp atsaucoties uz vārdu, uzvārdu vai identifikatoru vai atsaucoties uz vienu vai vairākiem personas fiziskajai, fizioloģiskajai, ģenētiskajai, garīgajai, ekonomiskajai, kultūras vai sociālajai identitātei raksturīgiem faktoriem. Jēdziens "apstrāde" ir definēts kā darbība vai darbību kopums, ko veic ar informāciju vai informācijas kopām, piemēram, tās: a) vākšana, reģistrēšana, organizēšana, strukturēšana vai glabāšana; b) pielāgošana vai pārveidošana; c) atgūšana, aplūkošana vai izmantošana; d) izpaušana, nosūtot, izplatot vai citādi darot pieejamu; e) saskaņošana vai kombinēšana; vai f) ierobežošana, dzēšana vai iznīcināšana. Turklāt likumā "sensitīva apstrāde" ir definēta kā "a) tādu personas datu apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās; b) ģenētisko datu vai biometrisko datu apstrāde, lai viennozīmīgi identificētu personu; c) veselības datu apstrāde; d) datu apstrāde attiecībā uz personas dzimumdzīvi vai seksuālo orientāciju" ([41]). Šajā sakarā 2018. gada DAL 205. pantā ir sniegta "biometrisko datu" ([42]), "veselības datu" ([43]) un "ģenētisko datu" ([44]) definīcija.

([35]) No to vidus 2018. gada DAL 7. pielikumā ir minēti valsts prokuratūru direktori, Ziemeļīrijas valsts prokuratūru direktors un Informācijas komisija.

([36]) 2018. gada DAL 43. panta 3. punkts.

([37]) 2018. gada DAL 30. panta 3. punkts. Izlūkdienesti (Slepenās izlūkošanas dienests, Drošības dienests un Valdības sakaru štābs) nav kompetentas iestādes (sk. 2018. gada DAL 30. panta 2. punktu), un 2018. gada DAL 3. daļa uz to darbībām neattiecas. Uz to darbībām attiecas 2018. gada DAL 4. daļa.

([38]) 2018. gada DAL 31. pants.

([39]) Tas nozīmē, ka 2018. gada DAL – un līdz ar to šis lēmums – neattiecas uz Apvienotās Karalistes kroņa teritorijām un pārējām Apvienotās Karalistes aizjūras teritorijām, piemēram, Folklenda Salām un Gibraltāra teritoriju.

([40]) Ar mirušu personu saistīti personas dati neietilpst 2018. gada DAL darbības jomā.

([41]) 2018. gada DAL 35. panta 8. punkts.

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

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

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

(27) 2018. gada DAL 32. pantā ir precizētas "pārziņa" un "apstrādātāja" definīcijas saistībā ar personas datu apstrādi tiesībaizsardzības nolūkā, ievērojot līdzvērtību ar Direktīvas (ES) 2016/680 definīcijām. Pārzinis ir kompetentā iestāde, kas nosaka personas datu apstrādes nolūkus un līdzekļus. Ja apstrāde ir paredzēta tiesību aktos, pārzinis ir kompetentā iestāde, kurai minētais likums uzliek šādu pienākumu. Apstrādātājs ir jebkura persona, kas pārziņa vārdā apstrādā personas datus (kas nav persona, kura ir pārziņa darbinieks).

2.4. **Garantijas, tiesības un pienākumi**

2.4.1. *Apstrādes likumīgums un godprātība*

(28) Saskaņā ar 2018. gada DAL 35. pantu (līdzīgi tam, kā paredzēts Direktīvas (ES) 2016/680 4. panta 1. punkta a) apakšpunktā) personas datu apstrādei jābūt likumīgai un godprātīgai. Saskaņā ar 2018. gada DAL 35. panta 2. punktu personas datu apstrāde jebkādā tiesībaizsardzības nolūkā ir likumīga tikai tad, ja tās pamatā ir tiesību akti un vai nu datu subjekts ir devis piekrišanu apstrādei šajā nolūkā, vai arī apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko šajā nolūkā veic kompetenta iestāde.

2.4.1.1. Apstrāde uz tiesību aktu pamata

(29) Līdzīgi tam, kā paredzēts Direktīvas (ES) 2016/680 8. pantā, lai nodrošinātu apstrādes likumīgumu saskaņā ar 2018. gada DAL 3. daļu, šādai apstrādei jābūt "uz tiesību aktu pamata". "Likumīga" apstrāde ir tāda, ko atļauj likums, anglosakšu tiesības vai monarha prerogatīvas ([45]).

(30) Kompetento iestāžu pilnvaras parasti reglamentē likumi, kas nozīmē, ka to funkcijas un pilnvaras ir skaidri izklāstītas parlamenta pieņemtajos normatīvajos aktos ([46]). Atsevišķos gadījumos, lai apstrādātu datus, policija, kā arī citas kompetentās iestādes, kas uzskaitītas 2018. gada DAL 7. pielikumā, var paļauties uz anglosakšu tiesībām ([47]). Anglosakšu tiesības ir veidojušās no tiesu lēmumu precedentiem. Anglosakšu tiesību nozīme izpaužas policijai pieejamajās pilnvarās, kas izriet no šā tiesību avota, un tās pamatpienākumā – aizsargāt sabiedrību, atklājot un novēršot noziedzību ([48]). Tomēr

([45]) 2018. gada DAL paskaidrojuma raksts, 181. punkts, pieejams vietnē https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Piemēram, Valsts noziedzības apkarošanas aģentūras pilnvaras izriet no 2013. gada Noziedzības un tiesu likuma, kas pieejams vietnē https://www.legislation.gov.uk/ukpga/2013/22/contents. Līdzīgi arī Pārtikas standartu aģentūras pilnvaras paredzētas 1999. gada Pārtikas standartu likumā, kas pieejams vietnē https://www.legislation.gov.uk/ukpga/1999/28/contents. Citi piemēri ir 1985. gada Pārkāpēju kriminālvajāšanas likums, ar kuru izveidoja valsts prokuratūru (sk. https://www.legislation.gov.uk/ukpga/1985/23/contents); 2005. gada Ieņēmumu un muitas komisāru likums, ar kuru izveidoja Viņas Majestātes Ieņēmumu un muitas dienestu (sk. https://www.legislation.gov.uk/ukpga/2005/11/contents); 1995. gada Skotijas Kriminālprocesa likums, ar ko tika izveidota Skotijas Kriminällietu pārskatīšanas komisija (sk. https://www.legislation.gov.uk/ukpga/1995/46/contents); 2002. gada Ziemeļīrijas Likums par tieslietām, ar ko izveidoja Ziemeļīrijas prokuratūru (sk. https://www.legislation.gov.uk/ukpga/2002/26/contents), un Smagu krāpšanas gadījumu apkarošanas birojs, kuru izveidoja un kuram pilnvaras tika piešķirtas ar 1987. gada Krimināltiesību likumu (sk. https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Piemēram, saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju valsts biroja un prokuratūras finanšu dienesta (kas ir atbildīgs par kriminālvajāšanu Skotijā) ģenerālprokurors kā Skotijas kriminālvajāšanas sistēmas vadītājs iegūst pilnvaras izmeklēt nāves gadījumus un īstenot kriminālvajāšanu par nodarījumiem uz anglosakšu tiesību pamata, turpretī dažas no viņa funkcijām ir noteiktas likumā. Turklāt valsts un attiecīgi dažādas valdības, ministrijas un ministri savas pilnvaras iegūst no tiesību aktu, anglosakšu tiesību un monarha prerogatīvu apvienojuma (tās ir anglosakšu tiesībās paredzētas pilnvaras, kas piešķirtas valstij, bet kuras īsteno ministri).

([48]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, F sadaļa "Tiesībaizsardzība", 8. lpp. (sk. 9. zemsvītras piezīmi).

policijas vienībām šā pienākuma izpildei ir gan no anglosakšu tiesībām, gan normatīvajiem aktiem izrietošas pilnvaras ([49]). Ja policijai ir likumā noteikta vara, tā aizstāj jebkuru no anglosakšu tiesībām izrietošu varu ([50]).

(31) Tiesa ir atzinusi, ka anglosakšu tiesībās paredzētās policijas ierēdņa pilnvaras un pienākumi ietver "visus pasākumus, kas viņam šķiet nepieciešami, lai uzturētu mieru, novērstu noziedzību vai aizsargātu īpašumu pret noziedzīgu kaitējumu" ([51]). Anglosakšu tiesībās paredzētās pilnvaras nav neierobežotas pilnvaras. Uz tām attiecas virkne ierobežojumu, tostarp ierobežojumi, ko noteikušas tiesas ([52]) un ko paredz normatīvie akti, jo īpaši 1998. gada Cilvēktiesību likums un 2010. gada Vienlīdzības likums ([53]). Turklāt attiecībā uz kompetentajām iestādēm, kas apstrādā datus saskaņā ar 2018. gada DAL 3. daļu, tas ietver anglosakšu tiesībās paredzēto pilnvaru īstenošanu saskaņā ar 2018. gada DAL noteiktajām prasībām ([54]). Turklāt, pieņemot lēmumu veikt jebkāda veida datu apstrādi, jāņem vērā piemērojamo norādījumu prasības, piemēram, PIP prakses kodekss, kā arī norādījumi, kas attiecas uz vienu no Apvienotās Karalistes pavalstīm ([55]). Valdība un operatīvā policija izdod norādījumus, lai nodrošinātu, ka policijas ierēdņi īsteno savas apstrādes pilnvaras saskaņā ar anglosakšu tiesībās vai attiecīgajos likumos noteiktajiem ierobežojumiem ([56]).

(32) Monarha prerogatīvas ir vēl viena tiesību sastāvdaļa, kas attiecas uz atsevišķām pilnvarām, kuras piešķirtas monarham un kuras var īstenot izpildvara, un tās nav pamatotas ar likumu, bet izriet no monarha suverenitātes ([57]). Ir ļoti maz piemēru tam, kā prerogatīvu pilnvaras varētu būt svarīgas tiesībaizsardzības jomā. Tie ietver, piemēram,

([49]) Galvenie tiesību akti, kas nosaka galveno policijas pilnvaru (aizturēšanas, kratīšanas, ilgstošas aizturēšanas atļaujas, pirkstu nospiedumu un intīmu paraugu ņemšanas, uz ordera pamata veiktas noklausīšanās, sakaru datu iegūšanas) īstenošanas kārtību, ir šādi: i) attiecībā uz Angliju un Velsu – 1984. gada Likums par policiju un pierādījumiem krimināllietās (LPPK), pieejams vietnē https://www.legislation.gov.uk/ukpga/1984/60/contents (ar grozījumiem, kas izdarīti ar 2012. gada Likumu par brīvību aizsardzību (LBA), kas pieejams vietnē https://www.legislation.gov.uk/ukpga/2012/9/contents), un 2016. gada Izmeklēšanas pilnvaru likums (IPL), pieejams vietnē https://www.legislation.gov.uk/ukpga/2016/25/contents, ii) attiecībā uz Skotiju – 2016. gada Skotijas Krimināltiesību likums, pieejams vietnē https://www.legislation.gov.uk/asp/2016/1/contents, un 1995. gada Skotijas Kriminālprocesa likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/1995/46/contents, iii) attiecībā uz Ziemeļīriju – 1989. gada Ziemeļīrijas Rīkojums par policiju un pierādījumiem krimināllietās, pieejams vietnē https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Apvienotās Karalistes iestādes ir paskaidrojušas, ka Apvienotajā Karalistē jau sen ir atzīts tiesību aktu pārākums, jo jau spriedumā lietā *Entick v Carrington* (1765), EWHC KB J98 tika atzīts, ka izpildvaras pilnvaru īstenošana ir ierobežota, un tika noteikts princips, ka monarha un valdības anglosakšu tiesībās paredzētās pilnvaras un prerogatīvu pilnvaras ir pakļautas valsts likumam.

([51]) Sk. lietu *Rice v Connolly* (1966), 2 QB 414.

([52]) Sk. lietu *R(Catt) v Association of Chief police Officers* (2015), AC 1065, kur saistībā ar policijas pilnvarām iegūt un glabāt informāciju par personu (kas izdarījusi noziegumu), lords *Sumption* uzskatīja, ka saskaņā ar anglosakšu tiesībām policijai ir tiesības iegūt un glabāt informāciju policijas darba vajadzībām, proti, lai uzturētu sabiedrisko kārtību un novērstu un atklātu noziedzību kopumā. Šīs pilnvaras neļauj izmantot uzbāzīgus informācijas iegūšanas paņēmienus, piemēram, iekļūšanu privātīpašumā vai darbības (izņemot anglosakšu tiesībās paredzēto aizturēšanu), kas būtu uzbrukums. Tiesnesis uzskatīja, ka šajā gadījumā ar anglosakšu tiesībās paredzētajām pilnvarām pilnīgi pietiek, lai varētu iegūt un glabāt ar šīm pārsūdzībām saistīto publisko informāciju.

([53]) 2010. gada Vienlīdzības likums, pieejams vietnē https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Kā piemēru lietai, kurā anglosakšu tiesībās paredzētās policijas pilnvaras tiek skatītas saskaņā ar 1998. gada DAL, skatīt Augstās tiesas lēmumu lietā *Bridges v the Chief Constable of South Wales Police* (sk. 33. zemsvītras piezīmi). Sk. arī lietas *Vidal-Hall v Google Inc* (2015), EWCA Civ 311, un *Richard v BBC* (2018), EWHC 1837 (Ch).

([55]) Skatīt, piemēram, Ziemeļīrijas Policijas dienesta norādījumus par lietvedības dienesta instrukciju, kas pieejami vietnē https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Pārstāvju palāta ir publicējusi informatīvu dokumentu, kurā izklāstītas galvenās Anglijas un Velsas policijas anglosakšu tiesībās un likumā noteiktās pilnvaras (sk. https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Saskaņā ar šo dokumentu, lai gan, piemēram, pilnvaras uzturēt "valsts mieru" un "lietot spēku" ir no anglosakšu tiesībām atvasinātas pilnvaras, "apturēšanas un pārmeklēšanas pilnvaras" vienmēr izriet no likuma. Turklāt Skotijas valdība savā tīmekļa vietnē sniedz informāciju par policijas aizturēšanas, kā arī apturēšanas un pārmeklēšanas pilnvarām (sk. https://www.gov.scot/policies/police/police-powers/).

([57]) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju valdības īstenotās prerogatīvu pilnvaras ir, piemēram, līgumu noslēgšana un ratifikācija, diplomātija, bruņoto spēku izmantošana Apvienotajā Karalistē, lai atbalstītu policiju miera uzturēšanā.

savstarpējās tiesiskās palīdzības sistēmu, kas ļauj ministram apmainīties ar datiem ar trešām valstīm tiesībaizsardzības nolūkā, un tiesības šādā veidā apmainīties ar datiem ne vienmēr ir noteiktas likumā ([58]). Monarha prerogatīvām ir saistoši anglosakšu tiesību principi ([59]), un tās ir pakļautas likumam, tāpēc tām piemēro 1998. gada Cilvēktiesību likumā un 2018. gada DAL noteiktos ierobežojumus ([60]).

(33) Līdzīgi kā Direktīvas (ES) 2016/680 8. pantā, Apvienotās Karalistes režīms paredz, ka, lai ievērotu likumīguma principu, kompetentajām iestādēm ir jānodrošina, ka, veicot apstrādi saskaņā ar tiesību aktu, tai ir jābūt "nepieciešamai", lai izpildītu tiesībaizsardzības nolūkā veikto uzdevumu. Šajā sakarā IKB sniedz norādījumus, precizējot, ka "ir jābūt mērķtiecīgam un samērīgam veidam, kā sasniegt nolūku. Likumīgais pamats netiks piemērots, ja nolūku saprātīgi var sasniegt ar kādu citu mazāk traucējošu līdzekli. Nepietiek tikai ar to, ka pārstrāde ir nepieciešama, jo esat izvēlējies darījumdarbību veikt noteiktā veidā. Jautājums ir par to, vai apstrāde ir nepieciešama norādītajam nolūkam" ([61]).

2.4.1.2. Apstrāde, pamatojoties uz datu subjekta piekrišanu

(34) Kā minēts 28. apsvērumā, 2018. gada DAL 35. panta 2. punktā ir paredzēta iespēja apstrādāt personas datus, pamatojoties uz personas piekrišanu.

(35) Tomēr šķiet, ka piekrišana nebūtu juridisks pamats, kas attiektos uz šā lēmuma darbības jomā ietilpstošajām apstrādes darbībām. Faktiski apstrādes darbības, uz kurām attiecas šis lēmums, vienmēr būs saistītas ar datiem, ko dalībvalsts kompetentā iestāde saskaņā ar Direktīvu (ES) 2016/680 ir nosūtījusi Apvienotās Karalistes kompetentajai iestādei. Tāpēc tās parasti neietver tiešu mijiedarbību (vākšanu) starp publisko iestādi un datu subjektiem, ko varētu pamatot ar piekrišanu 2018. gada DAL 35. panta 2. punkta a) apakšpunkta izpratnē.

(36) Lai gan tādējādi paļaušanās uz piekrišanu netiek uzskatīta par būtisku novērtējumā, ko veic saskaņā ar šo lēmumu, pilnīguma labad ir vērts atzīmēt, ka tiesībaizsardzības kontekstā apstrādes pamatā nekad nav tikai piekrišana, jo kompetentajai iestādei vienmēr ir jābūt pamatā esošām pilnvarām, kas tai ļauj apstrādāt datus ([62]). Konkrētāk, līdzīgi kā atļauts saskaņā ar Direktīvu (ES) 2016/680 ([63]), tas nozīmē, ka piekrišana kalpo kā papildu nosacījums, lai varētu veikt konkrētas ierobežotas un īpašas apstrādes darbības, ko citādi nevarētu veikt, piemēram, tādas personas DNS parauga savākšanu un apstrādi, kura nav aizdomās turamā persona. Šādā gadījumā apstrāde netiktu veikta, ja piekrišana netiktu dota vai tā tiktu atsaukta ([64]).

([58]) Šajā sakarā sk. Apvienotās Karalistes tālākas nosūtīšanas režīma novērtējumu 74.–87. apsvērumā.

([59]) Sk. lietu *Bancoult v Secretary of State for Foreign and Commonwealth Affairs* (2008), UKHL 61, kurā tiesa atzina, ka prerogatīvu pilnvaras izdot rīkojumus Padomē ir pakļautas arī parastajam pamatojumam attiecībā uz pārskatīšanu tiesā.

([60]) Sk. lietu *Attorney-General v De Keyser's Royal Hotel Ltd* (1920) (1920), AC 508, kurā tiesa atzina, ka prerogatīvu pilnvaras nevar izmantot, ja tās aizstātas ar likumā noteiktajām pilnvarām; lietu *Laker Airways Ltd v Department of Trade* (1977), QB 643, kurā tiesa konstatēja, ka prerogatīvu pilnvaras nevar izmantot, lai kaitētu tiesību aktiem; lietu *R v Secretary of State for the Home Department, ex p. Fire Brigades Union* (1995), UKHL 3, kurā tiesa atzina, ka prerogatīvu pilnvaras nevar izmantot, ja tās ir pretrunā ar pieņemtajiem tiesību aktiem, pat ja šie tiesību akti vēl nav spēkā; lietu *R (Miller) v Secretary of State for Exiting the European Union* (2017), UKSC 5, kurā tiesa apstiprināja, ka ar likumu ir iespējams pielāgot un atcelt prerogatīvu pilnvaras. Vispārīgs pārskats par monarha prerogatīvu un likumu, kā arī anglosakšu tiesību savstarpējām attiecībām atrodams Pārstāvju palātas informatīvajā dokumentā, kas pieejams vietnē https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *What is the first principle about?*, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Tas izriet no 2018. gada DAL attiecīgās normas redakcijas, kas paredz, ka personas datu apstrāde jebkādā tiesībaizsardzības nolūkā ir likumīga tikai tad un tiktāl, cik "tās pamatā ir tiesību akti" un vai nu a) datu subjekts ir devis piekrišanu apstrādei šim nolūkam, vai arī b) apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko šim nolūkam veic kompetenta iestāde.

([63]) Sk. Direktīvas (ES) 2016/680 35. un 37. apsvērumu.

([64]) Apvienotās Karalistes iestādes ir paskaidrojušas, ka piemērs, kad piekrišana varētu būt piemērots pamats apstrādei, būtu tas, ka policija iegūst DNS paraugu saistībā ar pazudušu personu, lai to varētu salīdzināt ar mirstīgajām atliekām, ja tādas atrastu. Šādos apstākļos nebūtu pareizi, ja policija piespiestu datu subjektu sniegt paraugu; tā vietā policija lūgtu personas piekrišanu, kas tiek dota labprātīgi un var tikt atsaukta jebkurā brīdī. Ja piekrišana tiek atsaukta, datus vairs nevar apstrādāt, ja vien nav noteikts jauns juridiskais pamats, lai turpinātu apstrādāt paraugu (piemēram, datu subjekts kļuvis par aizdomās turēto). Cits piemērs varētu būt gadījums, kad policijas vienības izmeklē noziegumu, kurā cietušais (tas varētu būt laupīšanas, noziedzīga nodarījuma pret tikumību un dzimumneaizskaramību, vardarbības ģimenē upuris, slepkavības vai cita nozieguma upura radinieks) varētu gūt labumu no nosūtījuma uz *Victim Support* (neatkarīga labdarības organizācija, kas atbalsta noziedzīgos nodarījumos un traumatiskos incidentos cietušas personas). Šādos apstākļos policija sniegs *Victim Support* personisko informāciju, piemēram, vārdu, uzvārdu un kontaktinformāciju, tikai tad, ja cietušais būs tam piekritis.

(37) Gadījumos, kad nepieciešama fiziskas personas piekrišana, šādai atļaujai jābūt nepārprotamai un jāietver nepārprotami apstiprinoša rīcība ([65]). Policijas vienībām ir jābūt paziņojumam par privātumu, kurā cita starpā iekļauta ar piekrišanas likumīgu izmantošanu saistītā nepieciešamā informācija. Turklāt dažas no tiem publicē papildu materiālus par to, kā tās ievēro datu aizsardzības tiesību aktus, tostarp par to, kā un kad tās piekrišanu izmantotu kā juridisko pamatu ([66]).

2.4.1.3. Sensitīva apstrāde

(38) Būtu vajadzīgas īpašas garantijas gadījumos, kad tiek apstrādāti "īpašu kategoriju" dati. Šajā sakarā, līdzīgi tam, kas paredzēts Direktīvas (ES) 2016/680 10. pantā, 2018. gada DAL 3. daļā ir paredzētas stingrākas garantijas tā dēvētajai "sensitīvajai apstrādei" ([67]).

(39) Saskaņā ar 1998. gada DAL 35. panta 3. punktu kompetentās iestādes var apstrādāt sensitīvus datus tiesībaizsardzības nolūkā tikai divos gadījumos: 1) datu subjekts ir devis piekrišanu apstrādei tiesībaizsardzības nolūkā, un apstrādes veikšanas laikā pārzinim ir atbilstošs politikas dokuments ([68]); vai 2) apstrāde ir absolūti nepieciešama tiesībaizsardzības nolūkā, tā atbilst vismaz vienam no 2018. gada DAL 8. pielikumā paredzētajiem nosacījumiem, un apstrādes veikšanas laikā pārzinim ir atbilstošs politikas dokuments ([69]).

(40) Attiecībā uz pirmo gadījumu un kā paskaidrots 38. apsvērumā, paļaušanos uz piekrišanu neuzskata par būtisku tādās nosūtīšanas situācijās, uz kurām attiecas šis lēmums ([70]).

(41) Ja sensitīvu datu apstrāde nav balstīta uz piekrišanu, to var veikt, izmantojot vienu no 2018. gada DAL 8. pielikumā minētajiem nosacījumiem. Šie nosacījumi attiecas uz datu apstrādi, kas nepieciešama likumā paredzētiem nolūkiem; tiesas spriešanai; datu subjekta vai citas personas vitālu interešu aizsardzībai; bērnu un apdraudētu personu aizsardzībai; likumīgām prasībām; procesuālai darbībai; krāpšanas novēršanai; arhivēšanai; ja datu subjekts ir acīmredzami publiskojis personas datus. Izņemot gadījumu, kad dati ir acīmredzami publiskoti, uz visiem 8. pielikumā paredzētajiem nosacījumiem attiecas "obligātas nepieciešamības" pārbaude. Kā skaidro IKB, "obligāta nepieciešamība šajā kontekstā nozīmē, ka apstrādei ir jābūt saistītai ar neatliekamu sociālo vajadzību, ko nevar

([65]) "Piekrišana" personas datu apstrādei saskaņā ar 2018. gada DAL 3. daļu nav atsevišķi definēta. IKB sniedza norādījumus par "piekrišanas" jēdzienu saskaņā ar 2018. gada DAL 3. daļu, precizējot, ka tam ir tāda pati nozīme kā VDAR lietotajai definīcijai un tam jābūt saskaņotam ar to, konkrēti, "piekrišana ir jāsniedz brīvi, konkrēti un pēc attiecīgas informācijas iegūšanas, un ir jābūt patiesai izvēlei piekrist datu apstrādei" (Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *What is the first principle about?* (sk. 64. zemsvītras piezīmi) un Datu aizsardzības rokasgrāmatas noteikumi par piekrišanu, kas pieejami vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Sk., piemēram, Linkolnšīras policijas tīmekļa vietnē (sk. https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) vai Rietumjorkšīras policijas tīmekļa vietnē (sk. https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf) esošo informāciju.

([67]) 2018. gada DAL 35. panta 8. punkts.

([68]) 2018. gada DAL 35. panta 4. punkts.

([69]) 2018. gada DAL 35. panta 5. punkts.

([70]) Pilnīguma labad ir vērts atzīmēt, ka, ja apstrādes pamatā ir piekrišana, tā ir jādod brīvi, konkrēti un pēc attiecīgas informācijas iegūšanas, un ir jāparedz īpaša izvēle piekrist datu apstrādei. Turklāt pārzinim, kas veic apstrādi, pamatojoties uz datu subjekta piekrišanu, ir jābūt "atbilstošam politikas dokumentam" (APD). 2018. gada DAL 42. pantā ir izklāstīts, kādām prasībām jāatbilst APD. Tajā ir skaidri noteikts, ka dokumentā ir vismaz jāizskaidro, ar kādām procedūrām pārzinis nodrošina atbilstību datu aizsardzības principiem, un jāizskaidro pārziņa politika attiecībā uz personas datu glabāšanu un dzēšanu. Saskaņā ar 2018. gada DAL 42. pantu tas nozīmē, ka pārzinim jāiesniedz dokuments, kurā a) izskaidrotas pārziņa procedūras, lai nodrošinātu atbilstību datu aizsardzības principiem; un b) izskaidrota pārziņa politika attiecībā uz tādu personas datu glabāšanu un dzēšanu, kurus apstrādā, pamatojoties uz datu subjekta piekrišanu, vai norādīts, cik ilgi šādi personas dati varētu tikt saglabāti. Jo īpaši politikas dokumentā paredzēts, ka pārzinim, ievērojot savu pienākumu reģistrēt apstrādes darbības, vienmēr būtu jāiekļauj a) un b) apakšpunktā minētie elementi. IKB ir publicējis dokumenta paraugu (Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *Conditions for sensitive processing*), pieejams vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing), un var veikt izpildes darbības, ja pārziņi neievēro šīs prasības. Atbilstošo politikas dokumentu izskata arī tiesas, vērtējot iespējamos 2018. gada DAL pārkāpumus. Piemēram, nesen izskatītajā lietā *R (Bridges) v Chief Constable of South Wales Police* tiesa pārskatīja pārziņa APD un konstatēja, ka tas ir pienācīgs, bet būtu bijis lietderīgi to izvērst. Tā rezultātā Dienvidvelsas policija pārskatīja APD un atjaunināja to saskaņā ar jaunajiem IKB norādījumiem (sk. 33. zemsvītras piezīmi). Turklāt saskaņā ar 2018. gada DAL 42. panta 3. punktu pārzinim regulāri jāpārskata APD. Visbeidzot, saskaņā ar 2018. gada DAL 42. panta 4. punktu kā papildu garantija ir paredzēts pārziņa pienākums veikt apstrādes darbību padziļinātu uzskaiti, iekļaujot tajā papildu elementus, salīdzinot ar vispārējo pārzinim noteikto pienākumu uzskaitīt apstrādes darbības, ko paredz 2018. gada DAL 61. pants.

saprātīgi sasniegt ar mazāk traucējošiem līdzekļiem" ([71]). Turklāt uz dažiem nosacījumiem attiecas papildu ierobežojumi. Piemēram, lai atsauktos uz "likumā noteikto nolūku" nosacījumu un "aizsardzības nosacījumu" (8. pielikuma 1. un 4. punkts), ir jāveic papildu pārbaude attiecībā uz būtiskām sabiedrības interesēm. Turklāt attiecībā uz nosacījumiem par bērna aizsardzību (8. pielikuma 4. punkts) datu subjektam arī jābūt konkrētā vecumā un ir jāuzskata, ka tas ir pakļauts riskam. Turklāt 8. pielikuma 4. punktā paredzēto nosacījumu pārzinis var piemērot tikai īpašu apstākļu gadījumā ([72]). Līdzīgi ierobežojumi ir arī attiecībā uz "procesuālu darbību" un "krāpšanas novēršanas" nosacījumiem (attiecīgi 8. pielikuma 7. un 8. punkts). Abi nosacījumi ir piemērojami tikai konkrētiem pārziņiem. Procesuālas darbības nosacījumu var izmantot tikai tiesa vai cita tiesu iestāde, bet uz krāpšanas novēršanas nosacījumu var atsaukties tikai pārziņi, kas ir krāpšanas apkarošanas organizācijas.

(42) Visbeidzot, ja apstrāde ir pamatota ar kādu no 8. pielikumā minētajiem nosacījumiem un attiecīgi saskaņā ar 2018. gada DAL 42. pantu, ir jābūt "atbilstošam politikas dokumentam", kurā ir izskaidrotas pārziņa procedūras, kā tas nodrošina datu aizsardzības principu ievērošanu, un pārziņa politika attiecībā uz personas datu glabāšanu un dzēšanu; papildus ir piemērojami padziļinātas uzskaites veikšanas pienākumi.

2.4.2. *Mērķa ierobežojums*

(43) Personas dati būtu jāapstrādā konkrētā nolūkā, un pēc tam tos var izmantot, ciktāl tas nav pretrunā apstrādes nolūkam. Šo datu aizsardzības principu garantē 2018. gada DAL 36. pants. Šajā noteikumā, līdzīgi kā Direktīvas (ES) 2016/680 4. panta 1. punkta b) apakšpunktā, ir paredzēts, ka a) tiesībaizsardzības nolūkam, kādam jebkurā gadījumā tiek vākti personas dati, jābūt konkrētam, skaidram un leģitīmam un b) šādi savāktos personas datus nedrīkst apstrādāt veidā, kas nav saderīgs ar nolūku, kādam tie tika vākti.

(44) Ja kompetentās iestādes apstrādā datus tiesībaizsardzības nolūkā, šāda apstrāde var ietvert arhivēšanas, zinātniskās vai vēstures pētniecības un statistikas nolūkus ([73]). Šajos gadījumos 2018. gada DAL arī precizēts, ka arhivēšana (vai apstrāde zinātniskās vai vēstures pētniecības un statistikas nolūkos) nav atļauta, ja tā tiek veikta saistībā ar lēmumiem, kas pieņemti attiecībā uz konkrētu datu subjektu, vai ja tā varētu radīt tam būtisku kaitējumu vai radīt būtisku spriedzi ([74]).

2.4.3. *Precizitāte un datu minimizēšana*

(45) Datiem jābūt precīziem, un vajadzības gadījumā tie jāatjaunina. Tiem arī jābūt atbilstīgiem un būtiskiem un nav jābūt pārmērīgiem, ņemot vērā nolūkus, kādos tie tiek apstrādāti. Līdzīgi kā Direktīvas (ES) 2016/680 4. panta 1. punkta c), d) un e) apakšpunktā, šie principi ir nostiprināti 2018. gada DAL 37. un 38. pantā. Ir jāveic visi pamatotie pasākumi, lai nodrošinātu, ka neprecīzus personas datus ([75])

([71]) Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *Conditions for sensitive processing* (sk. 70. zemsvītras piezīmi).

([72]) Apstrādi veic bez datu subjekta piekrišanas, ja: a) datu subjekts nevar dot piekrišanu datu apstrādei; b) no pārziņa nevar pamatoti gaidīt, ka tas iegūs datu subjekta piekrišanu apstrādei; c) apstrāde jāveic bez datu subjekta piekrišanas, jo datu subjekta piekrišanas saņemšana kaitētu 1. punkta a) apakšpunktā minētās aizsardzības nodrošināšanai.

([73]) Sk. 2018. gada DAL 41. panta 1. punktu.

([74]) Sk. 2018. gada DAL 41. panta 2. punktu.

([75]) 2018. gada DAL 205. pantā "neprecīzi" personas dati ir definēti kā "nepareizi vai maldinoši" personas dati. Apvienotās Karalistes iestādes ir paskaidrojušas, ka ar kriminālizmeklēšanu saistīti dati ļoti bieži būs nepilnīgi, taču tie tomēr var būt precīzi.

nekavējoties dzēš vai labo ([76]), ņemot vērā tiesībaizsardzības nolūku, kādā tie tiek apstrādāti ([77]), un lai nodrošinātu, ka neprecīzi, nepilnīgi vai vairs neaktuāli personas dati netiek nosūtīti vai darīti pieejami jebkādā tiesībaizsardzības nolūkā ([78]).

(46) Turklāt, līdzīgi kā Direktīvas (ES) 2016/680 7. pantā, Apvienotās Karalistes datu aizsardzības regulējumā ir noteikts, ka personas dati, kas balstās uz faktiem, cik vien iespējams, ir jānošķir no personas datiem, kas balstās uz personisku vērtējumu ([79]). Attiecīgos gadījumos, ciktāl tas iespējams, ir skaidri jānošķir personas dati, kas attiecas uz dažādām datu subjektu kategorijām, piemēram, aizdomās turētām, par noziedzīgiem nodarījumiem notiesātām, noziedzīgos nodarījumos cietušām personām un lieciniekiem ([80]).

2.4.4. *Glabāšanas ierobežojums*

(47) Saskaņā ar Direktīvas (ES) 2016/680 5. pantu dati būtībā nebūtu jāuzglabā ilgāk, nekā tas nepieciešams personas datu apstrādes nolūkam. Saskaņā ar 2018. gada DAL 39. pantu, kas ir līdzīgs minētās direktīvas 5. pantam, jebkādā tiesībaizsardzības nolūkā apstrādātus personas datus ir aizliegts glabāt ilgāk, nekā tas nepieciešams saistībā ar to apstrādes nolūku. Apvienotās Karalistes tiesiskais regulējums paredz, ka ir jānosaka atbilstīgi termiņi, pēc kuriem periodiski pārskata nepieciešamību turpināt glabāt personas datus jebkādā tiesībaizsardzības nolūkā. Attiecīgajos normatīvajos aktos un norādījumos, kas reglamentē policijas pilnvaras un darbību, ir paredzēti papildu noteikumi un prakse saistībā ar personas datu glabāšanu un tai piemērojamajiem termiņiem. Piemēram, Anglijā un Velsā Policijas kolēģijas PIP prakses kodekss un APP norādījumi par policijas informācijas pārvaldību, kas nodrošina konsekventu uz risku balstītu glabāšanas, pārskatīšanas un iznīcināšanas procesu operatīvās policijas informācijas pārvaldībai ([81]). Šajā regulējumā ir skaidri izklāstītas vienotas prasības visā dienestā attiecībā uz informācijas veidošanu, koplietošanu, izmantošanu un pārvaldību atsevišķās policijas vienībās un citās iestādēs, kā arī to starpā ([82]). No policijas tiek gaidīts, ka tā ievēros Prakses kodeksu, un atbilstību pārbauda Viņas Majestātes Policijas un ugunsdzēsības un glābšanas dienestu inspekcija ([83]).

(48) Ziemeļīrijas Policijas dienestam (*PSNI*) nav tiesību aktos noteikta pienākuma ievērot PIP prakses kodeksu. Tomēr 2011. gadā pieņemto PIP regulējumu papildina *PSNI* rokasgrāmata ([84]), kurā izklāstīta politika un procedūras PIP prakses kodeksa piemērošanai Ziemeļīrijā.

([76]) 2018. gada DAL 38. panta 1. punkta b) apakšpunkts.

([77]) Saskaņā ar Apvienotās Karalistes paskaidrojuma dokumentu aizsardzības līmeņa pietiekamības apspriešanai "tas nodrošina, ka tiek atzītas gan datu subjektu tiesības, gan tiesībaizsardzības iestāžu operatīvās vajadzības. Minētais jautājums tika rūpīgi apsvērts Datu aizsardzības likumprojekta izstrādes gaitā, jo tam, kādēļ datus nav iespējams labot, var būt konkrēti un šauri ar operatīvo darbību saistīti iemesli. Visticamāk, tas būs tad, ja attiecīgie neprecīzie personas dati ir jāsaglabā sākotnējā formā pierādīšanas nolūkā" (sk. Apvienotās Karalistes paskaidrojuma dokumentu aizsardzības līmeņa pietiekamības apspriešanai, F sadaļu "Tiesībaizsardzība", 21. lpp., sk. 9. zemsvītras piezīmi).

([78]) 2018. gada DAL 38. panta 4. punkts. Turklāt saskaņā ar 2018. gada DAL 38. panta 5. punktu, pirms personas dati tiek nosūtīti vai darīti pieejami, to kvalitāte ir jāpārbauda; visos personas datu sūtījumos ir jāiekļauj nepieciešamā informācija, kas ļauj saņēmējam novērtēt datu precizitāti, pilnīgumu un ticamību, kā arī to aktualitāti, un, ja pēc personas datu nosūtīšanas atklājas, ka dati ir bijuši nepareizi vai ka nosūtīšana ir bijusi nelikumīga, par to nekavējoties jāinformē saņēmējs.

([79]) 2018. gada DAL 38. panta 2. punkts.

([80]) 2018. gada DAL 38. panta 3. punkts.

([81]) Šis regulējums nodrošina, ka to konsekventi piemēro iegūto personas datu glabāšanai. Pārskatīšanas periods ir atkarīgs no nodarījuma, un nodarījumus iedala četrās grupās: 1) atsevišķi sabiedrības drošības jautājumi; 2) citi ar seksuālu vardarbību saistīti un smagi nodarījumi; 3) pārējie nodarījumi; 4) dažādi. Sīkāka informācija ir pieejama APP norādījumos par policijas informācijas pārvaldību (sk. 26. zemsvītras piezīmi).

([82]) Saskaņā ar Apvienotās Karalistes iestāžu sniegto informāciju citas organizācijas var brīvi ievērot PIP prakses kodeksa principus, ja tās to vēlas, piemēram, Viņas Majestātes Ieņēmumu un muitas dienests un Valsts noziedzības apkarošanas aģentūra brīvprātīgi pieņem daudzus PIP prakses kodeksa principus, lai nodrošinātu konsekvenci visā tiesībaizsardzības jomā. Lielākā daļa organizāciju parasti informē savus darbiniekus par konkrētu rīcībpolitiku un visiem darbiniekiem adresē konkrētajai organizācijai pielāgotus norādījumus, kā, pildot amata pienākumus, rīkoties ar personas datiem. Parasti tiek rīkotas arī obligātas mācības.

([83]) PIP prakses kodekss tika izdots, izmantojot ar 1996. gada Policijas likumu piešķirtās pilnvaras, kas ļauj Policijas kolēģijai izdot prakses kodeksus, kas attiecas uz policijas efektīvu darbību. Saskaņā ar likumu izstrādātie kodeksi vai prakse ir jāapstiprina ministram, un pirms to iesniegšanas parlamentam ir jāapspriežas ar Valsts noziedzības apkarošanas aģentūru. Saskaņā ar 1996. gada Policijas likuma 39.A panta 7. punktu policijai pienācīgi jāņem vērā uz 1996. gada Policijas likuma pamata izdotie kodeksi.

([84]) *PSNI* PIP rokasgrāmatas 1.–6. nodaļa.

(49) Skotijas policijas vienības izmanto Ierakstu glabāšanas standarta operāciju procedūru (SOP) ([85]), kas papildina Skotijas Policijas dienesta ierakstu pārvaldības politiku ([86]). SOP nosaka konkrētus Skotijas Policijas dienesta rīcībā esošo ierakstu glabāšanas noteikumus.

(50) Papildus vispārējai prasībai pārskatīt ierakstus, ko piemēro visā Apvienotajā Karalistē, vietējos noteikumos ir paredzētas sīkākas prasības. Daži piemēri attiecībā uz Angliju un Velsu ir atrodami Likumā par policiju un pierādījumiem krimināllietās, kurš grozīts ar 2012. gada Likumu par brīvību aizsardzību (LBA) un kurā ir paredzēti pirkstu nospiedumu un DNS profilu glabāšanas noteikumi, kā arī īpaša kārtība, ko piemēro personām, kuras nav notiesātas ([87]). Ar LBA tika izveidots arī par biometrisko materiālu glabāšanu un izmantošanu atbildīgā komisāra amats ("biometrijas komisārs") ([88]). Īpaši noteikumi par aizturēto personu attēliem ir izklāstīti 2017. gada aizturēto personu attēlu pārskatā ([89]). Attiecībā uz Skotiju 1995. gada Skotijas Kriminālprocesa likums paredz pirkstu nospiedumu un bioloģisko paraugu iegūšanas un glabāšanas noteikumus ([90]). Tāpat kā Anglijas un Velsas gadījumā, tiesību akti regulē biometrisko datu glabāšanu atšķirīgās situācijās ([91]).

2.4.5. *Datu drošība*

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

(52) Šie principi ir atspoguļoti 2018. gada DAL 40. pantā, saskaņā ar kuru, līdzīgi Direktīvas (ES) 2016/680 4. panta 1. punkta f) apakšpunktam, personas dati, ko apstrādā jebkādā tiesībaizsardzības nolūkā, ir jāapstrādā tā, lai nodrošinātu personas datu atbilstīgu drošību, izmantojot atbilstīgus tehniskos vai organizatoriskos pasākumus. Minētais ietver datu aizsardzību pret neatļautu vai nelikumīgu apstrādi un nejaušu nozaudēšanu, iznīcināšanu vai

([85]) Ierakstu glabāšanas standarta operāciju procedūra (SOP), pieejama vietnē https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Lai uzzinātu vairāk par ierakstu pārvaldību, sk. ar Skotijas Valsts arhīviem saistīto informāciju, kas pieejama vietnē https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Glabāšanas periodi atšķiras atkarībā no tā, vai persona ir vai nav bijusi notiesāta (1984. gada LPPK 63.I–63.KI pants). Piemēram, ja pieaugušais ir notiesāts par reģistrējamu nodarījumu, tā pirkstu nospiedumus un DNS profilu var glabāt nenoteiktu laiku (1984. gada LPPK 63.I panta 2. punkts), bet glabāšana ir ierobežota laikā, ja notiesātajam vēl nav 18 gadu, nodarījums ir "maznozīmīgs" reģistrējams nodarījums un persona nav iepriekš tiesāta (1984. gada LPPK 63.K pants). Glabāšanas termiņš attiecībā uz aizturētu vai apsūdzētu, bet ne notiesātu personu ir ierobežots līdz trim gadiem (1984. gada LPPK 63.F pants). Glabāšanas perioda pagarināšana ir jāapstiprina tiesu iestādei (1984. gada LPPK 63.F panta 7. punkts). Ja personas ir aizturētas vai apsūdzētas, bet nav notiesātas par maznozīmīgu nodarījumu, glabāšana nav iespējama (1984. gada LPPK 63.D pants un 63.H pants).

([88]) Biometrijas komisāra amats izveidots ar 2012. gada LBA 20. pantu. Biometrijas komisārs līdztekus citiem pienākumiem lemj par to, vai policija var glabāt DNS profila ierakstus un pirkstu nospiedumus, kas iegūti no personām, kuras ir aizturētas, bet nav apsūdzētas par attiecīga nodarījuma izdarīšanu (1984. gada LPPK 63.G pants). Turklāt Biometrijas komisārs ir vispārēji atbildīgs par DNS un pirkstu nospiedumu glabāšanu un izmantošanu, kā arī glabāšanu valsts drošības apsvērumu dēļ (2012. gada LBA 20. panta 2. punkts). Biometrijas komisāru ieceļ saskaņā ar Kodeksu par valsts amatpersonu iecelšanu amatā (kodekss pieejams šādā vietnē: Pārvaldības kodekss par valsts amatpersonu iecelšanu amatā – GOV.UK (www.gov.uk)), un viņa iecelšanas nosacījumi skaidri nosaka, ka viņu var atbrīvot no amata vienīgi iekšlietu ministrs konkrētos, precīzi definētos apstākļos; šādi apstākļi ir pienākumu nepildīšana trīs mēnešu garumā, notiesāšana par noziedzīgu nodarījumu vai iecelšanas nosacījumu neievērošana.

([89]) Pārskats par aizturēto personu attēlu izmantošanu un glabāšanu, pieejams vietnē https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) 1995. gada Skotijas Kriminālprocesa likuma 18. pants un turpmākie panti.

([91]) Glabāšanas periodi atšķiras atkarībā no tā, vai persona ir notiesāta (1995. gada Skotijas Kriminālprocesa likuma 18. panta 3. punkts) un vai tā ir nepilngadīga. Pēdējā gadījumā glabāšanas periods ir trīs gadi no notiesāšanas bērnu lietu tiesas sēdē (1995. gada Skotijas Kriminālprocesa likuma 18.E panta 8. punkts). Datus par aizturētajām personām, kas nav notiesātas, nedrīkst glabāt (1995. gada Skotijas Kriminālprocesa likuma 18. panta 3. punkts), izņemot īpašos gadījumos atkarībā no nozieguma smaguma (1995. gada Skotijas Kriminālprocesa likuma 18.A pants). Ar 2020. gada Likumu par Skotijas biometrijas komisāru (sk. https://www.legislation.gov.uk/asp/2020/8/contents) ir izveidots Skotijas biometrijas komisāra amats, kurā jāizstrādā un jāpārskata prakses kodeksi (ko apstiprinājis Skotijas parlaments) attiecībā uz biometrisko datu iegūšanu, glabāšanu, izmantošanu un iznīcināšanu krimināltiesību un policijas nolūkiem (2020. gada Likuma par Skotijas biometrijas komisāru 7. pants).

sabojāšanu ([92]). 2018. gada DAL 66. pantā turklāt noteikts, ka katram pārzinim un katram apstrādātājam jāīsteno atbilstīgi tehniskie un organizatoriskie pasākumi, lai nodrošinātu tādu drošības līmeni, kas atbilst personas datu apstrādes riskiem. Saskaņā ar paskaidrojuma rakstu pārzinim jāizvērtē riski un jāievieš atbilstoši drošības pasākumi, pamatojoties uz veikto izvērtējumu, piemēram, šifrēšana vai noteikti drošības pielaides līmeņi personālam, kas apstrādā datus ([93]). Izvērtējumā jāņem vērā arī, piemēram, apstrādāto datu veids un citi būtiski faktori vai apstākļi, kas varētu ietekmēt apstrādes drošību.

(53) Regulējums, ko piemēro datu drošības principu ievērošanai, ir ļoti līdzīgs režīmam, kas paredzēts Direktīvas (ES) 2016/680 29.–31. pantā. Jo īpaši gadījumā, kad personas datu aizsardzības pārkāpums ir saistīts ar personas datiem, par kuriem ir atbildīgs pārzinis, pārzinim saskaņā ar 2018. gada DAL 67. panta 1. punktu bez nepamatotas kavēšanās un, ja iespējams, 72 stundu laikā pēc tam, kad tas uzzinājis par pārkāpumu, par personas datu aizsardzības pārkāpumu ir jāpaziņo informācijas komisāram ([94]). Paziņošanas pienākums neattiecas uz gadījumiem, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu apdraudēt personu tiesības un brīvības ([95]). Pārzinim ir jādokumentē fakti, kas attiecas uz personas datu aizsardzības pārkāpumiem, to sekām un koriģējošām darbībām, kas ļauj informācijas komisāram pārbaudīt atbilstību DAL ([96]). Ja apstrādātājs uzzina par drošības pārkāpumu, tam bez nepamatotas kavēšanās jāpaziņo par to pārzinim ([97]).

(54) Saskaņā ar 2018. gada DAL 68. panta 1. punktu, ja personas datu aizsardzības pārkāpums var radīt augstu risku personu tiesībām un brīvībām, pārzinim bez nepamatotas kavēšanās jāinformē datu subjekts par pārkāpumu ([98]). Paziņojumā jāiekļauj tāda pati informācija kā 53. apsvērumā aprakstītajā paziņojumā informācijas komisāram. Šo pienākumu nepiemēro, ja pārzinis ir īstenojis atbilstīgus tehniskos un organizatoriskos aizsardzības pasākumus, kas tika piemēroti personas datiem, kurus skāris pārkāpums. To nepiemēro arī tad, ja pārzinis ir veicis turpmākus pasākumus, kas nodrošina to, ka augstais risks datu subjektu tiesībām un brīvībām, visticamāk, vairs neīstenosies. Visbeidzot, pārzinim nav jāinformē datu subjekts, ja šāda darbība prasītu nesamērīgi lielas pūles ([99]). Šādā gadījumā informācija jādara pieejama datu subjektam citā tikpat efektīvā veidā, piemēram, ar publisku saziņu ([100]). Ja pārzinis nav informējis datu subjektu par pārkāpumu, informācijas komisārs, kurš ir ticis informēts saskaņā ar DAL 67. pantu un ir apsvēris iespējamību, ka pārkāpums varētu radīt augstu risku, var pieprasīt, lai pārzinis par pārkāpumu paziņo datu subjektam ([101]).

([92]) Saskaņā ar 2018. gada DAL paskaidrojuma rakstu (sk. 45. zemsvītras piezīmi) pārzinim jo īpaši ir pienākums: izstrādāt un organizēt drošību, lai tā būtu atbilstīga tā rīcībā esošo personas datu veidam un kaitējumam, ko varētu radīt drošības pārkāpums; skaidri zināt, kas organizācijā atbild par informācijas drošības nodrošināšanu; nodrošināt attiecīgu fizisko un tehnisko drošību, ko papildina stingra politika un procedūras, kā arī uzticami, labi apmācīti darbinieki; būt gatavam ātri un efektīvi reaģēt uz jebkuru drošības pārkāpumu.

([93]) 2018. gada DAL paskaidrojuma raksta 221. punkts (sk. 45. zemsvītras piezīmi).

([94]) 2018. gada DAL 67. panta 4. punktā paredzēts, ka paziņojumā jāiekļauj personas datu aizsardzības pārkāpuma būtības apraksts (tostarp, ja iespējams, attiecīgo datu subjektu kategorijas un aptuvenais skaits un attiecīgo personas datu ierakstu kategorijas un aptuvenais skaits), kontaktpunkta nosaukums un kontaktinformācija, personas datu aizsardzības pārkāpuma iespējamo seku apraksts un to pasākumu apraksts, kurus pārzinis veicis vai ieteicis veikt, lai novērstu personas datu aizsardzības pārkāpumu (tostarp, ja nepieciešams, lai mazinātu tā iespējamo nelabvēlīgo ietekmi).

([95]) 2018. gada DAL 67. panta 2. punkts.

([96]) 2018. gada DAL 67. panta 6. punkts.

([97]) 2018. gada DAL 67. panta 9. punkts.

([98]) Saskaņā ar 2018. gada DAL 68. panta 7. punktu pārzinis var pilnībā vai daļēji ierobežot informācijas sniegšanu datu subjektam tiktāl un tik ilgi, kamēr ierobežojums, ņemot vērā datu subjekta pamattiesības un leģitīmās intereses, pastāv kā nepieciešams un samērīgs pasākums, lai a) novērstu, ka tiek traucēta oficiāla vai juridiska pārbaude, izmeklēšana vai procedūra; b) novērstu, ka tiek kaitēts noziedzīgu nodarījumu novēršanai, atklāšanai un izmeklēšanai vai saukšanai pie atbildības par tiem vai krimināsodu izpildei; c) aizsargātu sabiedrisko drošību; d) aizsargātu valsts drošību; e) aizsargātu citu personu tiesības un brīvības.

([99]) 2018. gada DAL 68. panta 3. punkts.

([100]) 2018. gada DAL 68. panta 5. punkts.

([101]) 2018. gada DAL 68. panta 6. punkts, ievērojot 2018. gada DAL 68. panta 8. punktā noteikto ierobežojumu.

2.4.6. *Pārredzamība*

(55) Datu subjekti ir jāinformē par viņu personas datu apstrādes galvenajām iezīmēm. Šis datu aizsardzības princips ir atspoguļots 2018. gada DAL 44. pantā, kurā tāpat kā Direktīvas (ES) 2016/680 13. pantā ir noteikts, ka pārzinim ir vispārējs pienākums datu subjektiem darīt pieejamu informāciju par to personas datu apstrādi (neatkarīgi no tā, vai informāciju dara publiski vispārpieejamu vai jebkādā citā veidā) ([102]). Informācija, kas jāsniedz, ietver: a) pārziņa identitāti un kontaktinformāciju; b) attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformāciju; c) nolūku, kādā pārzinis apstrādā personas datus; d) informāciju par datu subjektu tiesībām pieprasīt pārzinim piekļuvi personas datiem, personas datu labošanu un personas datu dzēšanu vai to apstrādes ierobežošanu; un e) informāciju par tiesībām iesniegt sūdzību informācijas komisāram un komisāra kontaktinformāciju ([103]).

(56) Pārzinim konkrētos gadījumos, lai varētu īstenot datu subjekta tiesības saskaņā ar 2018. gada DAL (piemēram, ja apstrādājamie personas dati ir savākti, datu subjektam par to nezinot), ir arī jāsniedz datu subjektam: a) informācija par apstrādes juridisko pamatu; b) informācija par laikposmu, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritērijiem, kas izmantoti minētā laikposma noteikšanai; c) attiecīgā gadījumā – informācija par personas datu saņēmēju kategorijām (ieskaitot saņēmējus trešās valstīs vai starptautiskās organizācijās); d) tāda papildu informācija, kas vajadzīga, lai ļautu īstenot datu subjekta tiesības saskaņā ar 2018. gada DAL 3. daļu ([104]).

2.4.7. *Individuālās tiesības*

(57) Ir jāatzīst vairākas īstenojamas datu subjektu tiesības. Ar 2018. gada DAL 3. daļas 3. nodaļu personām ir piešķirtas piekļuves, labošanas, dzēšanas un ierobežošanas tiesības ([105]), kas ir līdzīgas Direktīvas (ES) 2016/680 3. nodaļā paredzētajām.

(58) Piekļuves tiesības ir noteiktas 2018. gada DAL 45. pantā. Pirmkārt, personai ir tiesības saņemt apstiprinājumu no pārziņa par to, vai tās personas dati tiek apstrādāti ([106]). Otrkārt, ja personas datus apstrādā, datu subjektam ir tiesības piekļūt šiem datiem un saņemt šādu informāciju par apstrādi: a) apstrādes nolūks un juridiskais pamats; b) attiecīgo datu kategorijas; c) saņēmējs, kuram dati ir izpausti; d) laikposms, cik ilgi personas dati tiks glabāti; e) vai pastāv datu subjekta tiesības labot un dzēst personas datus; f) tiesības iesniegt sūdzību; g) jebkāda informācija par attiecīgo personas datu izcelsmi ([107]).

(59) Saskaņā ar 2018. gada DAL 46. pantu datu subjektam ir tiesības pieprasīt, lai pārzinis labo ar viņu saistītos neprecīzos personas datus. Pārzinim dati jālabo (vai, ja dati ir neprecīzi to nepilnības dēļ, jāpapildina) bez nepamatotas kavēšanās. Ja personas dati ir jāglabā pierādījumu nolūkā, pārzinim ir jāierobežo to apstrāde (tā vietā, lai labotu personas datus) ([108]).

([102]) Rokasgrāmatā par apstrādi tiesībaizsardzības nolūkā ir sniegts šāds piemērs: "Jūsu tīmekļa vietnē ir vispārīgs paziņojums par privātumu, kas ietver pamatinformāciju par organizāciju, personas datu apstrādes nolūku, datu subjekta tiesībām un tiesībām iesniegt sūdzību informācijas komisāram. Jūs esat saņēmis informāciju, ka kāda persona ir bijusi klāt nozieguma izdarīšanas brīdī. Pirmo reizi iztaujājot šo personu, jums ir jāsniedz vispārīga informācija, kā arī papildu informācija, lai tā varētu izmantot savas tiesības. Jūs varat ierobežot savu sniegto informāciju par godprātīgu apstrādi tikai tad, ja tā negatīvi ietekmēs jūsu veikto izmeklēšanu." (Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *What information should we supply to an individual?*, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Rokasgrāmatā par apstrādi tiesībaizsardzības nolūkā ir noteikts, ka informācijai, ko sniedz par personas datu apstrādi, jābūt kodolīgai, saprotamai un viegli pieejamai, rakstītai skaidrā un vienkāršā valodā, pielāgojot to neaizsargātu personu, piemēram, bērnu, vajadzībām, un pieejamai bez maksas (Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *How should we provide this information?*, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) 2018. gada DAL 44. panta 2. punkts.

([105]) Sīkāku datu subjektu tiesību analīzi sk. Rokasgrāmatā par apstrādi tiesībaizsardzības nolūkā attiecībā uz individuālām tiesībām, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) 2018. gada DAL 45. panta 1. punkts.

([107]) 2018. gada DAL 45. panta 2. punkts.

([108]) 2018. gada DAL 46. panta 4. punkts.

(60) 2018. gada DAL 47. pants nodrošina fiziskām personām tiesības uz datu dzēšanu un tiesības ierobežot apstrādi. Pārzinim bez nepamatotas kavēšanās jādzēš ([109]) personas dati, ja ar personas datu apstrādi pārkāpj kādu no datu aizsardzības principiem, apstrādes juridisko pamatojumu vai ar arhivēšanu un sensitīvu datu apstrādi saistītās garantijas. Pārzinim ir arī jādzēš dati, ja tam ir juridisks pienākums to darīt. Ja personas dati ir jāsaglabā pierādījumu nolūkā, pārzinim ir jāierobežo to apstrāde (tā vietā, lai dzēstu personas datus) ([110]). Pārzinim jāierobežo personas datu apstrāde, ja datu subjekts apstrīd personas datu precizitāti, bet nav iespējams noskaidrot, vai tie ir vai nav precīzi ([111]).

(61) Ja datu subjekts pieprasa labot vai dzēst personas datus vai ierobežot to apstrādi, pārzinim rakstiski jāinformē datu subjekts par to, vai pieprasījums ir ticis apmierināts, un, ja tas ir noraidīts, jāinformē datu subjekts par atteikuma iemesliem un pieejamajiem tiesiskās aizsardzības līdzekļiem (datu subjekta tiesībām lūgt informācijas komisāram izmeklēt, vai ierobežojums ir piemērots likumīgi, tiesībām iesniegt sūdzību informācijas komisāram un tiesībām vērsties tiesā, lai saņemtu izpildes rīkojumu) ([112]).

(62) Ja pārzinis labo personas datus, kas saņemti no citas kompetentās iestādes, tam jāinformē otra iestāde ([113]). Ja pārzinis labo, dzēš vai ierobežo tādu personas datu apstrādi, kurus izpaudis pārzinis, pārzinis par to informē saņēmējus, un saņēmējiem līdzīgi jālabo, jāizdzēš vai jāierobežo personas datu apstrāde (ciktāl viņi par to ir atbildīgi) ([114]).

(63) Turklāt datu subjektam ir tiesības bez nepamatotas kavēšanās saņemt pārziņa informāciju par personas datu aizsardzības pārkāpumu, ja tas var radīt augstu risku personu tiesībām un brīvībām ([115]).

(64) Attiecībā uz visām šīm datu subjekta tiesībām un līdzīgi tam, kas paredzēts Direktīvas (ES) 2016/680 12. pantā, pārzinim ir pienākums nodrošināt, ka visa informācija datu subjektam tiek sniegta kodolīgā, saprotamā un viegli pieejamā veidā ([116]), un, ja iespējams, tā būtu jāsniedz tādā pašā formā kā pieprasījums ([117]). Pārzinim jāizpilda datu subjekta pieprasījums bez nepamatotas kavēšanās, un būtībā jebkurā gadījumā – kamēr no pieprasījuma nav pagājis viens mēnesis ([118]). Ja pārzinim ir pamatotas šaubas par fiziskas personas identitāti, tas var pieprasīt papildu informāciju un atlikt pieprasījuma izskatīšanu līdz identitātes noskaidrošanai. Pārzinis var prasīt saprātīgu maksu vai atteikties rīkoties, ja uzskata pieprasījumu par acīmredzami nepamatotu ([119]). IKB ir sniedzis norādījumus par to, kad pieprasījums uzskatāms par acīmredzami nepamatotu vai pārmērīgu un kad var pieprasīt maksu ([120]).

(65) Turklāt saskaņā ar 2018. gada DAL 53. panta 4. punktu ministrs ar noteikumiem var paredzēt maksimālo maksas apmēru.

([109]) Datu subjekts var pieprasīt, lai pārzinis dzēš personas datus vai ierobežo to apstrādi (bet pārziņa pienākumi dzēst datus vai ierobežot to apstrādi ir spēkā neatkarīgi no tā, vai šāds pieprasījums ir izteikts).

([110]) 2018. gada DAL 46. panta 4. punkts un 47. panta 2. punkts.

([111]) 2018. gada DAL 47. panta 3. punkts.

([112]) 2018. gada DAL 48. panta 1. punkts.

([113]) 2018. gada DAL 48. panta 7. punkts.

([114]) 2018. gada DAL 48. panta 9. punkts.

([115]) 2018. gada DAL 68. pants.

([116]) 2018. gada DAL 52. panta 1. punkts.

([117]) 2018. gada DAL 52. panta 3. punkts.

([118]) 2018. gada DAL 54. pantā ir noteikts, ka jēdziens "piemērojamais laikposms" nozīmē viena mēneša laikposmu vai ilgāku laikposmu, ja tāds ir paredzēts ar noteikumiem, skaitot no attiecīgā brīža (kad pārzinis saņēmis attiecīgo pieprasījumu; kad pārzinis saņēmis pieprasīto informāciju (ja tāda ir) saistībā ar pieprasījumu saskaņā ar DAL 52. panta 4. punktu; vai kad ir samaksāta maksa (ja tāda ir), kas iekasēta saistībā ar pieprasījumu saskaņā ar DAL 53. pantu).

([119]) 2018. gada DAL 53. panta 1. punkts.

([120]) Saskaņā ar IKB norādījumiem pārzinis var lemt par maksas iekasēšanu no datu subjekta, ja tā pieprasījums ir acīmredzami nepamatots vai pārmērīgs, taču tas tik un tā uz to atbild. Maksai ir jābūt saprātīgai, un to ir jāspēj pamatot. Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *Manifestly unfounded and excessive requests*, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

2.4.7.1. Datu subjekta tiesību ierobežojumi un pārredzamības pienākumi

(66) Kompetentā iestāde noteiktos apstākļos var ierobežot konkrētas datu subjekta tiesības: tiesības piekļūt ([121]), tikt informētam ([122]), uzzināt par personas datu aizsardzības pārkāpumu ([123]) un tikt informētam par iemeslu, kāpēc noraidīts pieprasījums veikt labošanu vai dzēšanu ([124]). Līdzīgi Direktīvas (ES) 2016/680 III nodaļā paredzētajai kārtībai kompetentā iestāde var piemērot ierobežojumu tikai tad, ja tas, ņemot vērā datu subjekta pamattiesības un leģitīmās intereses, ir nepieciešams un samērīgs, lai: a) novērstu, ka tiek traucēta oficiāla vai juridiska pārbaude, izmeklēšana vai procedūra; b) novērstu, ka tiek kaitēts noziedzīgu nodarījumu novēršanai, atklāšanai un izmeklēšanai vai saukšanai pie atbildības par tiem vai kriminālsodu izpildei; c) aizsargātu sabiedrisko drošību; d) aizsargātu valsts drošību; e) aizsargātu citu personu tiesības un brīvības.

(67) IKB ir sniedzis norādījumus par minēto ierobežojumu piemērošanu. Saskaņā ar šiem norādījumiem pārziņiem katrā gadījumā jāveic atsevišķa analīze, lai līdzsvarotu fiziskās personas tiesības un kaitējumu, ko nodarītu izpaušana. Jo īpaši tiem jāpamato, ka piemērotais ierobežojums ir nepieciešams un samērīgs, un tie drīkst ierobežot sniegto informāciju tikai tad, ja tiktu kaitēts minētajiem nolūkiem ([125]).

(68) Ir arī vairāki citi norādījumi, ko izdevušas kompetentās iestādes un kas sniedz detalizētu informāciju par visiem datu aizsardzības tiesību aktu aspektiem, tostarp par datu subjektu tiesību ierobežojumu piemērošanu ([126]). Piemēram, attiecībā uz 45. panta 4. punktu Valsts policijas galvenā padomnieka Datu aizsardzības rokasgrāmatā norādīts: "Ir svarīgi atzīmēt, ka ierobežojumus var piemērot tikai tiktāl, cik tie ir nepieciešami, un tikai tik ilgi, cik tas nepieciešams. Līdz ar to nav pieļaujama vispārēja ierobežojuma piemērošana visiem pieteikuma iesniedzēja personas datiem vai ierobežojuma pastāvīga piemērošana. Runājot par pēdējo, bieži vien notiek tā, ka personas dati, kas savākti bez tāda datu subjekta ziņas, kas ir aizdomās turētā persona izmeklēšanā, ir sākotnēji jāaizsargā no to izpaušanas, lai novērstu, ka tiek kaitēts izmeklēšanai tās laikā, bet vēlāk, ja personas dati tiktu izpausti personai iztaujāšanas laikā, to izpaušana nenodarītu kaitējumu. Policijas vienībām ir jāievieš procesi, lai nodrošinātu šo ierobežojumu piemērošanu tikai nepieciešamajā apjomā un ir tikai nepieciešamajam ilgumam." ([127]) Šajos norādījumos sniegti arī piemēri, kad katrs no ierobežojumiem varētu būt piemērojams ([128]).

(69) Turklāt attiecībā uz iespēju "valsts drošības" aizsardzības nolūkā ierobežot kādu no iepriekš minētajām tiesībām pārzinis var pieprasīt Ministru kabineta ministra vai ģenerālprokurora (vai Skotijas ģenerālprokurora) parakstītu apliecinājumu, ka tiesību ierobežojums ir nepieciešams un samērīgs pasākums valsts drošības aizsardzībai ([129]). Apvienotās Karalistes valdība ir izdevusi norādījumus par valsts drošības sertifikātiem saskaņā ar 2018. gada DAL, kuros īpaši uzsvērts, ka jebkuram datu subjektu tiesību ierobežojumam valsts drošības aizsardzības nolūkā ir jābūt samērīgam un nepieciešamam ([130]) (sīkāku informāciju par valsts drošības sertifikātiem skatīt 131.–134. apsvērumā).

([121]) 2018. gada DAL 45. panta 4. punkts.
([122]) 2018. gada DAL 44. panta 4. punkts.
([123]) 2018. gada DAL 68. panta 7. punkts.
([124]) 2018. gada DAL 48. panta 3. punkts.
([125]) Skatīt, piemēram, Rokasgrāmatu par apstrādi tiesībaizsardzības nolūkā attiecībā uz piekļuves tiesībām, kas pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Sk., piemēram, Valsts policijas galvenā padomnieka izdoto Datu aizsardzības rokasgrāmatu policijas datu aizsardzības speciālistiem (sk. 27. zemsvītras piezīmi) vai Smagu krāpšanas gadījumu apkarošanas biroja norādījumus, pieejami vietnē https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Valsts policijas galvenā padomnieka Datu aizsardzības rokasgrāmata, 140. lpp. (sk. 27. zemsvītras piezīmi).
([128]) Valsts policijas galvenā padomnieka Datu aizsardzības rokasgrāmatā ir noteikts, ka "oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras traucēšanas novēršana", visticamāk, attieksies uz personas datiem, kas apstrādāti saistībā ar nāves gadījumu izmeklēšanu, ģimenes tiesas procesu, ar krimināltiesībām nesaistītu iekšējo disciplinārlietu izmeklēšanu, kā arī pārbaudēm, piemēram, neatkarīgu pārbaudi par bērnu seksuālo izmantošanu; savukārt "citu personu tiesību un brīvību aizsardzība" attiecas uz personas datiem, kas attiektos arī uz citām personām, ne vien uz pieteikuma iesniedzēju" (Valsts policijas galvenā padomnieka Datu aizsardzības rokasgrāmata, 140. lpp., sk. 27. zemsvītras piezīmi).
([129]) 2018. gada DAL 79. pants.
([130]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, pieejami vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Turklāt gadījumos, kad datu subjekta tiesībām piemēro ierobežojumu, kompetentajai iestādei bez nepamatotas kavēšanās jāinformē datu subjekts par tā tiesību ierobežošanu, ierobežošanas iemeslu un pieejamajiem tiesiskās aizsardzības līdzekļiem, izņemot, ja šādas informācijas sniegšana kaitētu mērķim, kādēļ ierobežojums piemērots ([131]). Kā papildu garantija attiecībā uz ierobežojumu ļaunprātīgu izmantošanu pārzinim ir noteikts pienākums reģistrēt informācijas ierobežošanas iemeslu un pēc pieprasījuma darīt šo ierakstu pieejamu informācijas komisāram ([132]).

(71) Ja pārzinis atsakās sniegt papildu informāciju par pārredzamību, nodrošināt piekļuvi vai noraida pieprasījumu labot, dzēst vai ierobežot apstrādi, persona var lūgt informācijas komisāram veikt izmeklēšanu par to, vai pārzinis likumīgi piemērojis ierobežojumu ([133]). Attiecīgā persona var arī iesniegt sūdzību informācijas komisāram vai vērsties tiesā, lai tā uzdotu pārzinim izpildīt pieprasījumu ([134]).

2.4.7.2. Automatizēta lēmumu pieņemšana

(72) 2018. gada DAL 49. un 50. pantā attiecīgi ir minētas ar automatizētu lēmumu pieņemšanu saistītās tiesības un piemērojamās garantijas ([135]). Līdzīgi Direktīvas (ES) 2016/680 11. pantā paredzētajam pārzinis pieņemt būtisku lēmumu, balstoties tikai uz personas datu automatizētu apstrādi, var tikai gadījumos, kad to pieprasa vai atļauj tiesību akti ([136]). Lēmums ir būtisks, ja tas radītu nelabvēlīgas juridiskas sekas datu subjektam vai būtiski ietekmētu datu subjektu ([137]).

(73) Ja pārzinim saskaņā ar tiesību aktiem ir pienākums vai atļauja pieņemt būtisku lēmumu, 2018. gada DAL 50. pantā ir noteiktas garantijas, kas attieksies uz šādu lēmumu (to definē kā "atbilstīgu būtisku lēmumu"). Pārzinim pēc iespējas ātrāk ir jāpaziņo datu subjektam, ka šāds lēmums ir pieņemts. Pēc tam datu subjekts mēneša laikā var pieprasīt pārzinim pārskatīt lēmumu vai pieņemt jaunu lēmumu, kas nav balstīts tikai uz automatizētu apstrādi. Pārzinim jāizskata šis pieprasījums un jāinformē datu subjekts par izskatīšanas rezultātu. 2018. gada DAL piešķirtas ministram pilnvaras pieņemt noteikumus par papildu garantijām ([138]). Šādi noteikumi vēl nav pieņemti.

2.4.8. *Tālāka nosūtīšana*

(74) Aizsardzības līmeni, kāds piešķirts personas datiem, kurus no dalībvalsts tiesībaizsardzības iestādes nosūta uz Apvienotās Karalistes tiesībaizsardzības iestādi, nedrīkst samazināt šādu datu tālāka nosūtīšana saņēmējiem trešā valstī. Šāda tālāka nosūtīšana, kas no Apvienotās Karalistes tiesībaizsardzības iestādes skatpunkta ir starptautiska nosūtīšana no Apvienotās Karalistes, būtu jāatļauj tikai tad, ja uz nākamo saņēmēju ārpus Apvienotās Karalistes attiecina noteikumus, kuri nodrošina aizsardzības līmeni, kas ir līdzīgs Apvienotās Karalistes tiesību sistēmas garantētajam.

([131]) 2018. gada DAL 44. panta 5. un 6. punkts; 45. panta 5. un 6. punkts; 48. panta 4. punkts.
([132]) 2018. gada DAL 44. panta 7. punkts; 45. panta 7. punkts; 48. panta 6. punkts.
([133]) 2018. gada DAL 51. pants.
([134]) 2018. gada DAL 167. pants.
([135]) Attiecībā uz automatizētās apstrādes jomu 2018. gada DAL paskaidrojuma rakstā ir noteikts: "Šie noteikumi attiecas uz pilnībā automatizētu lēmumu pieņemšanu, nevis uz automatizētu apstrādi. Automatizēta apstrāde (tostarp profilēšana) notiek tad, kad datus apstrādā bez nepieciešamības iesaistīties cilvēkam. Tā tiek regulāri izmantota tiesībaizsardzības iestādēs, lai lielas datu kopas filtrētu līdz apjomam, ko pēc tam var izmantot cilvēks, kas tās apstrādā. Automatizēta lēmumu pieņemšana ir automatizētas apstrādes veids, un tajā galīgo lēmumu pieņem bez cilvēka iejaukšanās" (DAL paskaidrojuma raksts, 204. punkts, sk. 45. zemsvītras piezīmi).
([136]) Papildus DAL paredzētajiem aizsardzības pasākumiem Apvienotās Karalistes tiesiskajā regulējumā pastāv arī citi tiesību aktos noteikti ierobežojumi, kas attiecas uz tiesībaizsardzības iestādēm un liedz veikt tādu automatizētu apstrādi (tostarp profilēšanu), kuras rezultātā notiktu nelikumīga diskriminācija. Ar 1998. gada Cilvēktiesību likumu Apvienotās Karalistes tiesību sistēmā ir iekļautas ECTK paredzētās tiesības, tostarp konvencijas 14. pantā nostiprinātās tiesības – diskriminācijas aizliegums. Tāpat arī 2010. gada Vienlīdzības likums aizliedz diskrimināciju pret cilvēkiem "aizsargātu" iezīmju dēļ (šādas iezīmes cita starpā ir dzimums, ādaskrāsa, invaliditāte utt.)
([137]) 2018. gada DAL 49. panta 2. punkts.
([138]) 2018. gada DAL 50. panta 4. punkts.

(75) Starptautiskās nosūtīšanas kārtību Apvienotajā Karalistē reglamentē 2018. gada DAL 3. daļas 5. nodaļa ([139]), un tā atspoguļo pieeju, kas izmantota Direktīvas (ES) 2016/680 V nodaļā. Konkrēti, lai nosūtītu personas datus uz trešo valsti, kompetentajai iestādei ir jāizpilda trīs nosacījumi: a) nosūtīšanai jābūt nepieciešamai tiesībaizsardzības nolūkā; b) nosūtīšanai jābūt pamatotai ar: i) noteikumiem par aizsardzības līmeņa pietiekamību attiecībā uz trešo valsti, ii) ja tā nav pamatota ar noteikumiem par aizsardzības līmeņa pietiekamību – atbilstošu garantiju esību vai iii) ja tā nav pamatota ar lēmumu par aizsardzības līmeņa pietiekamību vai atbilstošām garantijām, tai jābūt pamatotai ar īpašiem apstākļiem; un c) sūtījuma saņēmējam jābūt: i) attiecīgai iestādei (proti, kompetentās iestādes ekvivalentam) trešā valstī; ii) "attiecīgai starptautiskajai organizācijai", piemēram, starptautiskai organizācijai, kas veic funkcijas, kuras atbilst kādam tiesībaizsardzības nolūkam; vai iii) personai, kas nav attiecīgā iestāde, bet tikai tad, ja nosūtīšana ir absolūti nepieciešama, lai veiktu kādu no tiesībaizsardzības nolūkiem; nekādas attiecīgā datu subjekta pamattiesības un brīvības nav svarīgākas par sabiedrības interesēm, kuru dēļ ir nepieciešama nosūtīšana; personas datu nosūtīšana attiecīgajai iestādei trešā valstī būtu neefektīva vai nepiemērota; un saņēmējs ir informēts par nolūkiem, kādiem datus drīkst apstrādāt ([140]).

(76) Ministrs pieņem noteikumus par aizsardzības līmeņa pietiekamību attiecībā uz trešo valsti, trešās valsts teritoriju vai sektoru trešā valstī, starptautisku organizāciju vai šādas valsts, teritorijas, sektora vai organizācijas aprakstu ([141]). Standarts, kas jāievēro ministram, ir – vai šī teritorija/sektors/organizācija nodrošina pietiekamu personas datu aizsardzības līmeni. 2018. gada DAL 74.A panta 4. punktā ir noteikts, ka šajā nolūkā ministram jāņem vērā vairāki elementi, kas atspoguļo Direktīvas (ES) 2016/680 36. pantā uzskaitītos ([142]). Šajā sakarā kopš pārejas perioda beigām 2018. gada DAL 3. daļa ir "no ES atvasināts valsts tiesību akts", kuru, kā jau minēts, Apvienotās Karalistes tiesas interpretēs saskaņā ar attiecīgo Tiesas judikatūru, kas bija spēkā pirms Apvienotās Karalistes izstāšanās no Savienības, un Savienības tiesību aktu vispārējiem principiem, kas bija spēkā tieši pirms pārejas perioda beigām. Tas ietver "līdzvērtības pēc būtības" standartu, ko tādējādi piemēros Apvienotās Karalistes iestāžu veiktajiem aizsardzības līmeņa pietiekamības novērtējumiem.

(77) Uz šo noteikumu procedūru attiecas 2018. gada DAL 182. pantā paredzētās "vispārējās" prasības procedūrai. Saskaņā ar šo procedūru ministram, ierosinot izstrādāt turpmākos Apvienotās Karalistes noteikumus par

([139]) Šis jaunais regulējums, ieskaitot ministra pilnvaras izdot noteikumus par aizsardzības līmeņa pietiekamību, stājās spēkā pārejas perioda beigās. Tomēr DAPES noteikumi (jo īpaši 21. pielikuma 10.–12. punkts, ko ar šiem noteikumiem iekļauj 2018. gada DAL) paredz, ka atsevišķi personas datu nosūtīšanas gadījumi pārejas perioda beigās un pēc tā tiek uzskatīti par tādiem, kuru pamatā ir noteikumi par aizsardzības līmeņa pietiekamību. Šāda nosūtīšana ietver nosūtīšanu uz trešām valstīm, uz kurām attiecas ES lēmums par aizsardzības līmeņa pietiekamību pārejas perioda beigās, un uz ES dalībvalstīm, EBTA valstīm un Gibraltāra teritoriju, pamatojoties uz to, ka šīs valstis tiesībaizsardzības datu apstrādei piemēro Tiesībaizsardzības direktīvu (EBTA valstis piemēro Direktīvu (ES) 2016/680, ņemot vērā to pienākumus saskaņā ar Šengenas *acquis*). Tas nozīmē, ka pārejas perioda beigās nosūtīšana uz šīm valstīm var turpināties tāpat kā pirms izstāšanās no ES. Pēc pārejas perioda beigām ministram četru gadu laikā ir jāpārskata konstatējumi par aizsardzības līmeņa pietiekamību.

([140]) 2018. gada DAL 73. un 77. pants.

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

([142]) Sk. 2018. gada DAL 74.A panta 4. punktu, kurā noteikts, ka, novērtējot aizsardzības līmeņa pietiekamību, "ministram jo īpaši jāņem vērā: a) tiesiskums, cilvēktiesību un pamatbrīvību ievērošana, attiecīgie tiesību akti, gan vispārējie, gan nozaru tiesību akti, tostarp attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un krimināltiesībām, un publisko iestāžu piekļuvi personas datiem, kā arī šādu tiesību aktu, datu aizsardzības noteikumu, dienesta noteikumu un drošības pasākumu īstenošana, tostarp noteikumi par personas datu tālāku nosūtīšanu uz citu trešo valsti vai starptautisko organizāciju, kas tiek ievēroti attiecīgajā valstī vai starptautiskajā organizācijā, judikatūra, kā arī tas, vai pastāv efektīvas un tiesiski īstenojamas datu subjektu tiesības un efektīva tiesību aizsardzība administratīvā kārtā un tiesā tiem datu subjektiem, kuru personas dati tiek nosūtīti, b) tas, vai attiecīgajā trešā valstī vai attiecībā uz starptautisko organizāciju pastāv un efektīvi darbojas viena vai vairākas neatkarīgas uzraudzības iestādes, kuras ir atbildīgas par datu aizsardzības noteikumu ievērošanas nodrošināšanu un panākšanu, tostarp ar piemērotām izpildes pilnvarām, par palīdzību un konsultācijām datu subjektiem saistībā ar viņu tiesību īstenošanu un par sadarbību ar komisāru, un c) starptautiskās saistības, ko ir uzņēmusies attiecīgā trešā valsts vai starptautiskā organizācija, vai citi pienākumi, kas izriet no juridiski saistošām konvencijām vai instrumentiem, kā arī no tās dalības daudzpusējās vai reģionālās sistēmās, jo īpaši saistībā ar personas datu aizsardzību".

aizsardzības līmeņa pietiekamību, ir jāapspriežas ar informācijas komisāru ([143]). Pēc tam, kad ministrs ir pieņēmis šos noteikumus, tos iesniedz parlamentam un tiem piemēro "noraidošas rezolūcijas" procedūru, saskaņā ar kuru abas parlamenta palātas var pārbaudīt noteikumus un 40 dienu laikā pieņemt priekšlikumu par noteikumu atcelšanu ([144]).

(78) Saskaņā ar 2018. gada DAL 74.B panta 1. punktu noteikumi par aizsardzības līmeņa pietiekamību jāpārskata ne retāk kā reizi četros gados un ministram pastāvīgi jāuzrauga norises trešās valstīs un starptautiskās organizācijās, kas varētu ietekmēt lēmumus par aizsardzības līmeņa pietiekamības noteikumu pieņemšanu vai šādu noteikumu grozīšanu vai atcelšanu. Ja ministrs uzzina, ka kāda valsts vai organizācija vairs nenodrošina pietiekamu personas datu aizsardzības līmeni, viņam, ciktāl nepieciešams, jāgroza vai jāatceļ noteikumi un jāuzsāk apspriešanās ar attiecīgo trešo valsti vai starptautisko organizāciju, lai novērstu aizsardzības līmeņa nepietiekamību.

(79) Līdzīgi kā noteikts Direktīvas (ES) 2016/680 37. pantā, ja nav pieņemti noteikumi par aizsardzības līmeņa pietiekamību, personas datus tiesībaizsardzības jomā var nosūtīt tikai tad, ja ir ieviestas atbilstošas garantijas. Garantijas nodrošina ar a) juridiski saistošu instrumentu, kurā ir ietvertas atbilstošas personas datu aizsardzības garantijas, vai b) pārziņa veiktu novērtējumu, pēc kura, vērtējot visus ar nosūtīšanu saistītos apstākļus, tiek secināts, ka pastāv atbilstošas garantijas, ar kurām aizsargā datus ([145]). Turklāt, ja nosūtīšana ir pamatota ar atbilstošām garantijām, 2018. gada DAL paredz, ka līdztekus IKB parastajai pārraudzības funkcijai kompetentajām iestādēm ir arī jāsniedz IKB konkrēta informācija par nosūtīšanu ([146]).

(80) Ja nosūtīšana nav balstīta uz lēmumu par aizsardzības līmeņa pietiekamību vai atbilstošām garantijām, tā var notikt tikai konkrētos apstākļos jeb tā dēvētajos "īpašajos apstākļos" ([147]). Tas tā ir gadījumos, kad nosūtīšana ir nepieciešama: a) lai aizsargātu datu subjekta vai citas personas vitālas intereses; b) lai pasargātu datu subjekta leģitīmās intereses; c) lai novērstu tiešus un nopietnus draudus sabiedriskajai drošībai trešā valstī; d) atsevišķos gadījumos – jebkādā tiesībaizsardzības nolūkā; vai e) atsevišķos gadījumos – juridiskiem mērķiem (piemēram, saistībā ar tiesvedību vai juridisku konsultāciju saņemšanu) ([148]). Ir jānorāda, ka d) un e) punktu nepiemēro, ja datu subjekta tiesības un brīvības ir svarīgākas par sabiedrības interesēm, lai notiktu nosūtīšana ([149]). Šie apstākļi atbilst īpašām situācijām un nosacījumiem, kas Direktīvas (ES) 2016/680 38. pantā atzīti par "atkāpēm".

(81) Šādās situācijās ir jādokumentē nosūtīšanas datums, laiks un pamatojums, saņēmēja nosaukums un jebkura cita būtiska informācija par saņēmēju, kā arī nosūtīto personas datu apraksts, un pēc pieprasījuma tie ir jāiesniedz informācijas komisāram ([150]).

(82) 2018. gada DAL 78. pantā ir regulēts "secīgas nosūtīšanas" scenārijs, proti, gadījumi, kad personas dati, kas no Apvienotās Karalistes ir nosūtīti uz trešo valsti, vēlāk tiek nosūtīti citai trešai valstij vai starptautiskai organizācijai. Saskaņā ar 78. panta 1. punktu Apvienotās Karalistes pārzinim, kas nosūta datus, ir jāparedz nosacījums datu nosūtīšanai, ka dati netiks tālāk nosūtīti uz trešo valsti, ja to nebūs atļāvis pārzinis, kas veic nosūtīšanu. Turklāt saskaņā ar 78. panta 3. punktu, līdzīgi kā noteikts Direktīvas (ES) 2016/680 35. panta 1. punkta e) apakšpunktā, gadījumos, kad nepieciešama šāda atļauja, piemēro virkni būtisku prasību. Konkrētāk, kompetentajai iestādei, lemjot

([143]) Sk. digitalizācijas, kultūras, mediju un sporta ministra un informācijas komisāra biroja Saprašanās memorandu par IKB lomu saistībā ar jauno Apvienotās Karalistes aizsardzības līmeņa pietiekamības novērtējumu, pieejams vietnē https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Šo 40 dienu laikā abām parlamenta palātām ir iespēja, ja tās vēlas, balsot pret šiem noteikumiem; ja tiks nobalsots par šādu priekšlikumu, noteikumiem vairs nebūs turpmāka juridiska spēka.

([145]) 2018. gada DAL 75. pants.

([146]) Saskaņā ar 2018. gada DAL 75. panta 3. punktu, ja datu nosūtīšana notiek, pamatojoties uz atbilstošām garantijām: a) nosūtīšanai jābūt dokumentētai, b) dokumentācija pēc pieprasījuma jāiesniedz komisāram un c) dokumentācijā jo īpaši jāietver i) nosūtīšanas datums un laiks, ii) saņēmēja nosaukums un cita būtiska informācija par saņēmēju, iii) nosūtīšanas pamatojums un iv) nosūtīto personas datu apraksts.

([147]) Rokasgrāmata par apstrādi tiesībaizsardzības nolūkā *Are there any special circumstances?*, pieejama vietnē https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

([148]) 2018. gada DAL 76. pants.

([149]) 2018. gada DAL 76. pants.

([150]) 2018. gada DAL 76. panta 3. punkts.

par to, vai atļaut vai neatļaut nosūtīšanu, ir jāpārliecinās, ka tālāka nosūtīšana ir nepieciešama tiesībaizsardzības nolūkā, un tai cita starpā būtu jāņem vērā: a) to apstākļu nopietnība, kuru dēļ pieprasīta atļauja, b) nolūks, kādam personas dati sākotnēji nosūtīti, un c) personas datu aizsardzības standarti, kas ir spēkā trešā valstī vai starptautiskā organizācijā, uz kuru personas dati tiktu nosūtīti.

(83) Turklāt tad, ja dati, kas tiek tālāk nosūtīti no Apvienotās Karalistes, sākotnēji tikuši nosūtīti no Eiropas Savienības, tiek piemērotas papildu garantijas.

(84) Pirmkārt, 2018. gada DAL 73. panta 1. punkta b) apakšpunktā – līdzīgi kā Direktīvas (ES) 2016/680 35. panta 1. punkta c) apakšpunktā – ir noteikts, ka gadījumā, ja dalībvalsts personas datus sākotnēji nosūtījusi vai citādi darījusi pieejamus pārzinim vai citai kompetentajai iestādei, minētajai dalībvalstij vai jebkurai personai, kas atrodas minētajā dalībvalstī un ir kompetenta iestāde Direktīvas (ES) 2016/680 mērķiem, ir jābūt devušai nosūtīšanas atļauju saskaņā ar minētās dalībvalsts tiesību aktiem.

(85) Tomēr, līdzīgi Direktīvas (ES) 2016/680 35. panta 2. punktam, šāda atļauja nav vajadzīga, ja a) nosūtīšana ir nepieciešama, lai novērstu tiešus un nopietnus draudus dalībvalsts vai trešās valsts sabiedriskajai drošībai vai dalībvalsts būtiskām interesēm, un b) atļauju nevar saņemt laikus. Šādā gadījumā nekavējoties jāinformē dalībvalsts iestāde, kas būtu bijusi atbildīga par lēmumu pieņemšanu par nosūtīšanas atļaušanu ([151]).

(86) Otrkārt, tāda pati pieeja attiecas uz datiem, kas sākotnēji nosūtīti no Eiropas Savienības uz Apvienoto Karalisti un tad tālāk nosūtīti no Apvienotās Karalistes uz trešo valsti, kura savukārt pēc tam veiktu to tālāku nosūtīšanu uz vēl kādu trešo valsti. Šādā gadījumā saskaņā ar 78. panta 4. punktu Apvienotās Karalistes kompetentā iestāde nevar dot piekrišanu pēdējai minētajai nosūtīšanai, kā noteikts 78. panta 1. punktā, ja vien "dalībvalsts [kura sākotnēji nosūtījusi attiecīgos datus] vai jebkura persona, kas atrodas minētajā dalībvalstī un ir kompetenta iestāde Tiesībaizsardzības direktīvas mērķiem, nav devusi nosūtīšanas atļauju saskaņā ar minētās dalībvalsts tiesību aktiem". Šīs ir nozīmīgas garantijas, jo tās ļauj dalībvalstu iestādēm nodrošināt aizsardzības nepārtrauktību atbilstoši ES datu aizsardzības tiesību aktiem visā "nosūtīšanas ķēdē".

(87) Jauno starptautiskās nosūtīšanas regulējumu sāka piemērot pārejas perioda beigās ([152]). Tomēr 21. pielikuma 10.–12. punktā (ieviesti ar *DPPC* noteikumiem) ir paredzēts, ka pēc pārejas perioda beigām konkrētu personas datu nosūtīšanu uzskata par tādu, kas ir pamatota ar noteikumiem par aizsardzības līmeņa pietiekamību. Šāda nosūtīšana ietver nosūtīšanu uz dalībvalsti, EBTA valsti, trešo valsti, par kuru pārejas perioda beigās ir pieņemts ES lēmums par aizsardzības līmeņa pietiekamību, un Gibraltāra teritoriju. Tādēļ nosūtīšana uz šīm valstīm var turpināties tā, kā tā notika pirms Apvienotās Karalistes izstāšanās no Savienības. Pārejas perioda beigās ministram četru gadu laikā (proti, līdz 2024. gada decembra beigām) ir jāpārskata minētie konstatējumi par aizsardzības līmeņa pietiekamību. Kā paskaidrojušas Apvienotās Karalistes iestādes, lai gan ministram šāda pārskatīšana ir jāveic līdz 2024. gada decembra beigām, pārejas noteikumi neietver noteikumu par spēka zaudēšanu, tādēļ attiecīgie pārejas noteikumi automātiski nezaudēs spēku, ja pārskatīšana līdz 2024. gada decembra beigām netiks pabeigta.

2.4.9. *Pārskatatbildība*

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

(89) Šis princips ir atspoguļots 2018. gada DAL 56. pantā, ar ko tiek ieviests vispārējs pārziņa pārskatatbildības pienākums, proti, pienākums īstenot atbilstīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu un spētu pierādīt, ka personas datu apstrāde atbilst 2018. gada DAL 3. daļas prasībām. Īstenotie pasākumi ir jāpārskata un vajadzības gadījumā jāatjaunina, un, ja tie ir samērīgi attiecībā uz apstrādi, tajos jāiekļauj atbilstīga datu aizsardzības politika.

([151]) 2018. gada DAL 73. panta 5. punkts.

([152]) Šā jaunā regulējuma piemērojamība ir jāinterpretē, ņemot vērā 782. pantu Tirdzniecības un sadarbības nolīgumā starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses (L 444, 31.12.2020., 14. lpp.) ("ES un Apvienotās Karalistes TSN"), kas pieejams vietnē https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=CELEX:22020A1231(01)&from=LV.

(90) Līdzīgi kā Direktīvas (ES) 2016/680 IV nodaļā, 2018. gada DAL 55.–71. pantā ir paredzēti dažādi mehānismi, kā nodrošināt pārskatatbildību un ļaut pārziņiem un apstrādātājiem pierādīt atbilstību. Konkrēti, pārziņiem tiek prasīts īstenot datu aizsardzības pasākumus integrēti un pēc noklusējuma, proti, nodrošināt datu aizsardzības principu efektīvu īstenošanu, un pārziņiem tiek prasīts reģistrēt visas apstrādes darbību kategorijas, par kurām pārzinis ir atbildīgs (tostarp informācija par pārziņa identitāti, datu aizsardzības speciālista kontaktinformācija, apstrādes nolūki, izpaušanas saņēmēju kategorijas un datu subjektu kategoriju apraksts, kā arī personas dati), un glabāt reģistrus, lai tiem pēc pieprasījuma varētu piekļūt informācijas komisārs. Pārzinim un apstrādātājam ir arī jāglabā žurnāli par noteiktām apstrādes darbībām un tie jādara pieejami informācijas komisāram ([153]). Pārziņiem ir arī īpaši noteikts pienākums sadarboties ar informācijas komisāru tā uzdevumu izpildē.

(91) 2018. gada DAL arī nosaka papildu prasības apstrādei, kas var radīt augstu risku fizisku personu tiesībām un brīvībām. Tās ietver pienākumu veikt novērtējumu par ietekmi uz datu aizsardzību un pirms apstrādes apspriesties ar informācijas komisāru, ja novērtējums liecina, ka apstrāde radītu augstu risku personu tiesībām un brīvībām (ja netiek veikti riska mazināšanas pasākumi).

(92) Turklāt pārziņiem ir jāieceļ datu aizsardzības speciālists, ja vien pārzinis nav tiesa vai cita tiesu iestāde, kas rīkojas tieslietu jomā ([154]). Pārzinim jānodrošina, ka datu aizsardzības speciālists ir iesaistīts visos ar personas datu aizsardzību saistītajos jautājumos, ka tam ir nepieciešamie resursi un piekļuve personas datiem un apstrādes darbībām un ka tas savus uzdevumus var veikt patstāvīgi. Datu aizsardzības speciālista uzdevumi ir noteikti 2018. gada DAL 71. pantā, un to vidū ir informācijas un konsultāciju sniegšana, atbilstības uzraudzība, kā arī sadarbība ar informācijas komisāru un tā kontaktpunkta pienākumu izpilde. Veicot uzdevumus, datu aizsardzības speciālistam ir jāņem vērā ar apstrādes darbībām saistītie riski, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus.

2.5. **Pārraudzība un izpilde**

2.5.1. *Neatkarīga pārraudzība*

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

(94) Apvienotajā Karalistē pārraudzību un izpildes nodrošināšanu attiecībā uz atbilstību Apvienotās Karalistes VDAR un 2018. gada DAL veic informācijas komisārs ([155]). Informācijas komisārs pārrauga arī personas datu apstrādi, ko veic kompetentās iestādes, uz kurām attiecas 2018. gada DAL 3. daļa ([156]). Informācijas komisārs ir "individuāls komersants": atsevišķs tiesību subjekts, ko veido viena persona. Informācijas komisāra darbā to atbalsta birojs. 2020. gada 31. martā informācijas komisāra birojā bija 768 pastāvīgie darbinieki ([157]). Informācijas komisāru atbalsta Digitalizācijas, kultūras, mediju un sporta ministrija (*DCMS*) ([158]).

([153]) 2018. gada DAL 62. pants.
([154]) 2018. gada DAL 69. pants.
([155]) Direktīvas (ES) 2016/680 36. panta 2. punkta b) apakšpunkts.
([156]) 2018. gada DAL 116. pants.
([157]) Informācijas komisāra gada pārskats un finanšu pārskati par 2019.–2020. gadu, pieejami vietnē https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.
([158]) Attiecības starp abām pusēm regulē pārvaldības nolīgums. Konkrēti, *DCMS* kā atbalstošās ministrijas galvenie pienākumi ir šādi: nodrošināt, lai IKB tiktu piešķirts atbilstošs finansējums un resursi; pārstāvēt IKB intereses parlamentā un citās valdības ministrijās; nodrošināt, ka ir ieviests stabils valsts datu aizsardzības regulējums; un sniegt IKB norādījumus un atbalstu korporatīvajos jautājumos, piemēram, par nekustamo īpašumu, nomu un iepirkumiem (2018.–2021. gada pārvaldības nolīgums, pieejams vietnē https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Komisāra neatkarība ir skaidri noteikta Apvienotās Karalistes VDAR 52. pantā, kas atspoguļo Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 ([159]) 52. panta 1.–3. punktā noteiktās prasības. Komisāram, veicot uzdevumus un īstenojot savas pilnvaras saskaņā ar Apvienotās Karalistes VDAR, ir jārīkojas pilnīgi neatkarīgi, attiecībā uz šiem uzdevumiem un pilnvarām ir jābūt brīvam no tiešas vai netiešas ārējas ietekmes, un viņš nedrīkst lūgt un ne no viena pieņemt nekādus norādījumus. Komisāram ir arī jāatturas no jebkādas darbības, kas nav savienojama ar viņa pienākumiem, un, esot amatā, viņš nedrīkst uzņemties nekādu nesavienojamu algotu vai nealgotu darbu.

(96) Nosacījumi informācijas komisāra iecelšanai un atbrīvošanai no amata ir izklāstīti 2018. gada DAL 12. pielikumā. Informācijas komisāru ieceļ karaliene pēc valdības ieteikuma, pamatojoties uz godīgu un atklātu konkursu. Kandidātam ir jāpiemīt atbilstošai kvalifikācijai, prasmēm un kompetencei. Saskaņā ar Pārvaldības kodeksu par valsts amatpersonu iecelšanu amatā ([160]) padomdevēja novērtēšanas komisija izveido to kandidātu sarakstu, kurus var iecelt amatā. Pirms digitalizācijas, kultūras, mediju un sporta ministrs pieņem galīgo lēmumu, attiecīgajai parlamenta komitejai ir jāveic pirmsiecelšanas pārbaude. Komitejas nostāja tiek publiskota ([161]).

(97) Informācijas komisāra amata pilnvaru termiņš ir līdz septiņiem gadiem. Informācijas komisāru no amata var atbrīvot Viņas Majestāte pēc tam, kad abas parlamenta palātas ir izdarījušas uzrunu ([162]). Nevienai no parlamenta palātām nevar iesniegt pieprasījumu par informācijas komisāra atbrīvošanu no amata, ja vien ministrs nav iesniedzis parlamentam ziņojumu, kurā minēts, ka viņš ir pārliecināts, ka informācijas komisārs ir vainojams nopietnā pārkāpumā un/vai komisārs vairs neatbilst komisāra funkciju veikšanai nepieciešamajiem nosacījumiem ([163]).

(98) Informācijas komisāram ir trīs finansējuma avoti: i) pārziņu maksājumi par datu aizsardzību, kurus nosaka ar ministra izdotiem noteikumiem ([164]) un kuri veido 85–90 % no biroja gada budžeta ([165]); ii) dotācijas, ko informācijas komisāram var izmaksāt valdība un ko galvenokārt izmanto, lai finansētu informācijas komisāra darbības izmaksas, kas nav saistītas ar datu aizsardzību ([166]); iii) maksa par pakalpojumiem ([167]). Pašlaik šādas maksas netiek iekasētas.

(99) Informācijas komisāra vispārīgās funkcijas saistībā ar personas datu apstrādi, kas ietilpst 2018. gada DAL 3. daļas darbības jomā, ir noteiktas 2018. gada DAL 13. pielikumā. Šie uzdevumi ietver 2018. gada DAL 3. daļas uzraudzību un izpildes nodrošināšanu, sabiedrības informētības veicināšanu, ieteikumus parlamentam, valdībai un citām iestādēm par likumdošanas un administratīvajiem pasākumiem, pārziņu un apstrādātāju informētības veicināšanu par viņu pienākumiem, informācijas sniegšanu datu subjektam par datu subjekta tiesību īstenošanu un

([159]) Eiropas Parlamenta un Padomes Regula (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) (OV L 119, 4.5.2016., 1. lpp.).

([160]) Pārvaldības kodekss par valsts amatpersonu iecelšanu amatā, pieejams vietnē https://www.gov.uk/government/publications/governance-code-for-public-appointments.

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

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

([163]) 2018. gada DAL 12. pielikuma 3. punkts.

([164]) 2018. gada DAL 137. pants.

([165]) 2018. gada DAL 137. un 138. pantā ir ietvertas vairākas garantijas, lai nodrošinātu, ka maksas tiek noteiktas atbilstošā līmenī. Konkrēti, 2018. gada DAL 137. panta 4. punktā ir uzskaitīti aspekti, kas ministram jāņem vērā, izstrādājot noteikumus par summu, ko maksā dažādas organizācijas. 2018. gada DAL 138. panta 1. punktā un 182. pantā ir ietverta arī juridiska prasība ministram pirms noteikumu pieņemšanas apspriesties ar informācijas komisāru un citiem to personu pārstāvjiem, kuras varētu ietekmēt noteikumi, lai varētu ņemt vērā to viedokļus. Turklāt saskaņā ar 2018. gada DAL 138. panta 2. punktu informācijas komisāram ir jāpārrauga Maksas noteikumu darbība, un viņš var iesniegt ministram priekšlikumus par grozījumiem, kas jāveic noteikumos. Visbeidzot, izņemot gadījumus, kad noteikumi pieņemti tikai tādēļ, lai ņemtu vērā mazumtirdzniecības cenu indeksa pieaugumu (tādā gadījumā uz tiem attiecas noraidošas rezolūcijas procedūra), uz noteikumiem attiecas apstiprinošas rezolūcijas procedūra, un tos nevar pieņemt, kamēr tie nav apstiprināti ar katras parlamenta palātas rezolūciju.

([166]) Pārvaldības nolīgumā ir precizēts, ka "ministrs var veikt maksājumus IK no parlamenta piešķirtajiem līdzekļiem saskaņā ar 2018. gada DAL 12. pielikuma 9. punktu. Pēc apspriešanās ar IK *DCMS* izmaksā IK attiecīgas summas (dotācijas) IKB administratīvo izmaksu segšanai un IK funkciju izpildei vairāku konkrētu uzdevumu, tostarp informācijas brīvības, sakarā" (2018.–2021. gada pārvaldības nolīgums, 1.12. punkts, sk. 158. zemsvītras piezīmi).

([167]) 2018. gada DAL 134. pants.

izmeklēšanas veikšanu. Lai saglabātu tiesu iestāžu neatkarību, informācijas komisāram nav atļauts īstenot pilnvaras attiecībā uz personas datu apstrādi, ko veic persona, kas rīkojas tiesu varas ietvaros, vai tiesa vai tribunāls, kas rīkojas tiesu varas ietvaros. Tomēr pārraudzību pār tiesu iestādēm nodrošina īpašas struktūras, kā sīkāk iztirzāts turpmāk.

2.5.1.1. Izpildes panākšana, ieskaitot sankcijas

(100) Komisāram ir vispārējas izmeklēšanas, korektīvas, atļaujas došanas un padomdevēja pilnvaras attiecībā uz personas datu apstrādi, uz kuru attiecas 2018. gada DAL 3. daļa. Komisāram ir pilnvaras paziņot pārzinim vai apstrādātājam par iespējamo 3. daļas pārkāpumu, izdot brīdinājumus pārzinim vai apstrādātājam, ka ar paredzētajām apstrādes darbībām varētu pārkāpt 3. daļas noteikumus, un izteikt pārzinim vai apstrādātājam rājienu, ja ar apstrādes darbībām ir pārkāpti 3. daļas noteikumi. Turklāt komisārs pēc savas iniciatīvas vai pēc pieprasījuma var sniegt atzinumus Apvienotās Karalistes parlamentam, valdībai vai citām iestādēm un struktūrām, kā arī sabiedrībai par jebkuru jautājumu, kas saistīts ar personas datu aizsardzību ([168]).

(101) Turklāt komisāram ir pilnvaras:

— uzdot pārzinim un apstrādātājam (konkrētos gadījumos – jebkurai citai personai) sniegt nepieciešamo informāciju ar informatīvu paziņojumu ("informatīvais paziņojums") ([169]),

— veikt izmeklēšanu un revīzijas, sniedzot novērtējuma paziņojumu, kurā var pieprasīt pārzinim vai apstrādātājam, lai tas atļauj komisāram iekļūt konkrētās telpās, apskatīt vai pārbaudīt dokumentus vai iekārtas, iztaujāt personas, kas pārziņa vārdā apstrādā personas datus ("novērtējuma paziņojums") ([170]),

— citādi iegūt piekļuvi pārziņu un apstrādātāju dokumentiem un iekļūt to telpās saskaņā ar 2018. gada DAL 154. pantu ("iekļūšanas un pārbaudes pilnvaras"),

— īstenot korektīvās pilnvaras, tostarp izsakot brīdinājumus un rājienus, vai dot rīkojumus ar izpildes paziņojumu, ar kuru pārziņiem/apstrādātājiem pieprasa veikt konkrētas darbības vai atturēties no to veikšanas ("izpildes paziņojums") ([171]), un

— uzlikt administratīvos naudas sodus soda paziņojuma veidā ("soda paziņojums") ([172]).

(102) IKB regulatīvās rīcības politikā ir izklāstīti apstākļi, kādos komisārs izdod attiecīgi informatīvu, novērtējuma, izpildes un soda paziņojumu ([173]). Izpildes paziņojumā var noteikt prasības, kuras komisārs uzskata par piemērotām pārkāpuma novēršanai. Soda paziņojumā ir noteikts, ka personai jāsamaksā informācijas komisāram paziņojumā norādītā summa. Soda paziņojumu var izdot, ja nav ievēroti konkrēti 2018. gada DAL noteikumi ([174]), vai arī izdot pārzinim vai apstrādātājam, kas nav izpildījis informatīvā paziņojumā, novērtējuma paziņojumā vai izpildes paziņojumā noteikto.

(103) Konkrētāk, nosakot, vai pārzinim vai apstrādātājam ir jāpiemēro sods, un nosakot soda apmēru, informācijas komisāram ir jāņem vērā 2018. gada DAL 155. panta 3. punktā uzskaitītie jautājumi, tostarp pārkāpuma raksturs un smagums, tas, vai pārkāpums izdarīts apzināti vai aiz nolaidības, jebkura pārziņa vai apstrādātāja rīcība, lai

([168]) 2018. gada DAL 13. pielikuma 2. punkts.
([169]) 2018. gada DAL 142. pants (ievērojot 2018. gada DAL 143. pantā noteiktos ierobežojumus).
([170]) 2018. gada DAL 146. pants (ievērojot 2018. gada DAL 147. pantā noteiktos ierobežojumus).
([171]) 2018. gada DAL149.–151. pants (ievērojot 2018. gada DAL 152. pantā noteiktos ierobežojumus).
([172]) 2018. gada DAL 155. pants (ievērojot 2018. gada DAL 156. pantā noteiktos ierobežojumus).
([173]) Regulatīvās rīcības politika, pieejama vietnē https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Konkrēti, IKB var izdot soda paziņojumu par 2018. gada DAL 149. panta 2., 3., 4. vai 5. punktā noteiktajām neatbilstībām.

mazinātu datu subjektiem nodarītos zaudējumus, pārziņa vai apstrādātāja atbildības pakāpe (ņemot vērā pārziņa vai apstrādātāja īstenotos tehniskos un organizatoriskos pasākumus), pārziņa vai apstrādātāja attiecīgie iepriekšējie pārkāpumi; ar pārkāpumu skarto personas datu kategorijas un tas, vai sods būtu iedarbīgs, samērīgs un atturošs.

(104) Maksimālais soda naudas apmērs, ko var uzlikt ar soda paziņojumu, ir a) 17 500 000 GBP par datu aizsardzības principu (2018. gada DAL 35., 36. un 37. pants, 38. panta 1. punkts, 39. panta 1. punkts un 40. pants), pārredzamības pienākuma un individuālo tiesību (2018. gada DAL 44., 45., 46., 47., 48., 49., 52. un 53. pants) un personas datu starptautiskās nosūtīšanas principu (2018. gada DAL 73., 75., 76., 77. un 78. pants) neievērošanu un b) 8 700 000 GBP citos gadījumos ([175]). Maksimālais soda naudas apmērs, ko var uzlikt ar soda paziņojumu saistībā ar informatīvā paziņojuma, novērtējuma paziņojuma vai izpildes paziņojuma neizpildi, ir 17 500 000 GBP.

(105) Saskaņā ar jaunākajiem gada pārskatiem (2018.–2019. ([176]), 2019.–2020. gads ([177])) informācijas komisārs ir veicis vairākas izmeklēšanas saistībā ar personas datu apstrādi kriminālizmeklēšanas iestādēs. Piemēram, komisārs veica izmeklēšanu un 2019. gada oktobrī publicēja atzinumu par sejas atpazīšanas tehnoloģiju izmantošanu tiesībaizsardzības iestāžu vajadzībām publiskās vietās. Īpaša uzmanība izmeklēšanā tika pievērsta sejas atpazīšanas iespēju izmantošanai tiešraidē Dienvidvelsas policijā un Metropoles policijas dienestā (*MPS*). Turklāt komisārs izmeklēja *MPS* "bandu matricu" ([178]) un konstatēja virkni nopietnu datu aizsardzības tiesību aktu pārkāpumu, kas varēja mazināt sabiedrības uzticību matricai un datu izmantošanai.

(106) Informācijas komisārs 2018. gada novembrī izdeva izpildes paziņojumu, un *MPS* pēc tam veica nepieciešamos pasākumus, lai paaugstinātu drošību un pārskatatbildību un nodrošinātu, ka dati tiek izmantoti samērīgi.

(107) Vēl viens nesen veiktas izpildes darbības piemērs ir komisāra 2018. gada maijā piespriestais 325 000 GBP naudas sods valsts prokuratūrai par nešifrētu DVD nozaudēšanu, kuros bija policijas interviju ieraksti. Turklāt informācijas komisārs veica izmeklēšanu par plašākiem tematiem, piemēram, 2020. gada pirmajā pusgadā – par mobilo tālruņu izrakstu izmantošanu policijas darba vajadzībām un cietušo personu datu apstrādi policijā.

(108) Papildus minētajām informācijas komisāra izpildes pilnvarām daži datu aizsardzības tiesību aktu pārkāpumi ir noziedzīgi nodarījumi, tāpēc par tiem var piemērot kriminālsodus (2018. gada DAL 196. pants). Tas attiecas, piemēram, uz personas datu iegūšanu vai izpaušanu bez pārziņa piekrišanas un panākšanu, ka personas dati tiek izpausti citai personai bez pārziņa piekrišanas ([179]); informācijas, kas ir anonimizēti personas dati, atkārtotu identificēšanu, ja tai nav piekritis par personas datu anonimizēšanu atbildīgais pārzinis ([180]); komisāra pilnvaru īstenošanas apzinātu kavēšanu saistībā ar personas datu pārbaudi saskaņā ar starptautiskajām saistībām ([181]), nepatiesu ziņu sniegšanu, atbildot uz informatīvu paziņojumu, vai informācijas iznīcināšanu saistībā ar informatīviem un novērtējuma paziņojumiem ([182]).

(109) Saskaņā ar 2018. gada DAL 139. pantu informācijas komisāram ir arī pienākums sniegt katrai parlamenta palātai vispārēju pārskatu par likumā paredzēto funkciju izpildi ([183]).

([175]) 2018. gada DAL 157. pants.

([176]) Informācijas komisāra 2018.–2019. gada pārskats un finanšu pārskati, pieejami vietnē https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Informācijas komisāra 2019.–2020. gada pārskats (sk. 157. zemsvītras piezīmi).

([178]) Datubāze, kurā tika reģistrēti izlūkdati par iespējamiem bandu locekļiem un ar bandām saistītos noziegumos cietušajiem.

([179]) 2018. gada DAL 170. pants.

([180]) 2018. gada DAL 171. pants.

([181]) 2018. gada DAL 119. pants.

([182]) 2018. gada DAL 144. un 148. pants.

([183]) Kā noteikts pārvaldības nolīgumā, gada pārskatā ir: i) jāietver visas sabiedrības, meitasuzņēmumi vai kopuzņēmumi, kas ir IKB kontrolē; ii) jānodrošina atbilstība Valsts kases Finanšu pārskatu sniegšanas rokasgrāmatai (*FReM*); iii) jāietver pārvaldības ziņojums, kurā izklāstīti veidi, kā grāmatvedis gada laikā pārvaldījis un kontrolējis organizācijā izmantotos resursus, tādējādi parādot, cik labi organizācija pārvalda riskus savu mērķu un uzdevumu sasniegšanai; iv) jāizklāsta galvenās darbības un darbības rezultāti iepriekšējā finanšu gadā, kā arī kopsavilkuma veidā jāizklāsta nākotnes plāni (2018.–2021. gada pārvaldības nolīgums, 3.26. punkts, sk. 158. zemsvītras piezīmi).

2.5.2. *Tiesu iestāžu pārraudzība*

(110) Tiesu un tiesu iestāžu veiktās personas datu apstrādes pārraudzība ir divējāda. Ja tiesu iestādes amatpersona vai tiesa neīsteno tiesu varu, pārraudzību nodrošina informācijas komisārs. Ja pārzinis īsteno tiesu varu, IKB nevar īstenot pārraudzību ([184]), un pārraudzību veic īpašas struktūras. Tas atspoguļo Direktīvas (ES) 2016/680 32. pantā izmantoto pieeju.

(111) Konkrēti, otrajā scenārijā šādu pārraudzību pār Anglijas un Velsas tiesām un Anglijas un Velsas pirmā un augstākā līmeņa tribunāliem nodrošina Tiesu datu aizsardzības kolēģija ([185]). Turklāt lords augstais tiesnesis un tribunālu galvenais tiesnesis ir izdevuši Paziņojumu par privātumu ([186]), kurā izklāstīts, kā Anglijas un Velsas tiesas apstrādā personas datus tiesas funkciju veikšanai. Līdzīgu paziņojumu ir izdevušas Ziemeļīrijas ([187]) un Skotijas tiesu iestādes ([188]).

(112) Turklāt Ziemeļīrijas lords augstais tiesnesis ir iecēlis Augstās tiesas tiesnesi par datu uzraudzības tiesnesi (DUT) Ziemeļīrijā ([189]). Tas ir arī izdevis norādījumus Ziemeļīrijas tiesu iestādēm par to, kā rīkoties datu nozaudēšanas vai iespējamas nozaudēšanas gadījumā un kā risināt ar to saistītos jautājumus ([190]).

(113) Skotijā lords priekšsēdētājs ir iecēlis datu uzraudzības tiesnesi, kas izmeklē visas sūdzības datu aizsardzības jomā. Tas ir noteikts saskaņā ar tiesu iestāžu sūdzību izskatīšanas noteikumiem, kas atbilst Anglijā un Velsā spēkā esošajiem noteikumiem ([191]).

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

([184]) 2018. gada DAL 117. pants.

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

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

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

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

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

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

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

2.5.3. *Tiesiskās aizsardzības līdzekļi*

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

(116) Pirmkārt, datu subjektam ir tiesības iesniegt sūdzību informācijas komisāram, ja datu subjekts uzskata, ka saistībā ar viņa personas datiem ir pārkāpta 2018. gada DAL 3. daļa ([192]). Kā aprakstīts 100. un 109. apsvērumā, informācijas komisārs ir pilnvarots novērtēt pārziņa un apstrādātāja atbilstību 2018. gada DAL, neatbilstības gadījumā pieprasīt tiem veikt nepieciešamos pasākumus vai atturēties no to veikšanas un uzlikt naudas sodu.

(117) Otrkārt, 2018. gada DAL paredz tiesības uz tiesiskās aizsardzības līdzekli pret informācijas komisāru. Ja komisārs "nevirza" ([193]) datu subjekta iesniegto sūdzību, sūdzības iesniedzējam ir pieejami tiesiskās aizsardzības līdzekļi, jo viņš var vērsties pirmā līmeņa tribunālā ([194]), lai tas uzdotu komisāram veikt atbilstošus pasākumus sakarā ar sūdzību vai informēt sūdzības iesniedzēju par sūdzības virzību ([195]). Turklāt jebkura persona, kurai komisārs ir izdevis kādu no iepriekš minētajiem paziņojumiem (informatīvu, novērtējuma, izpildes vai soda paziņojumu), var to pārsūdzēt pirmā līmeņa tribunālā. Ja tribunāls uzskata, ka komisāra lēmums neatbilst tiesību aktiem vai ka informācijas komisāram vajadzēja citādi izmantot savu rīcības brīvību, tribunālam ir jāatļauj pārsūdzība vai jānosaka aizstājējs paziņojums vai lēmums, ko informācijas komisārs būtu varējis izdot vai pieņemt ([196]).

(118) Treškārt, personas var tieši panākt tiesisko aizsardzību pret pārziņiem un apstrādātājiem tiesā saskaņā ar 2018. gada DAL 167. pantu. Ja pēc datu subjekta pieteikuma tiesa ir pārliecinājusies, ka ir pārkāptas datu subjekta tiesības, ko paredz datu aizsardzības tiesību akti, tiesa var uzdot pārzinim, kas apstrādā datus, vai apstrādātājam, kas rīkojas minētā pārziņa vārdā, veikt rīkojumā noteiktos pasākumus vai atturēties no rīkojumā noteikto pasākumu veikšanas. Turklāt saskaņā ar 2018. gada DAL 169. pantu jebkura persona, kas cietusi kaitējumu datu aizsardzības tiesību aktu (tostarp 2018. gada DAL 3. daļas) prasību pārkāpuma dēļ, izņemot Apvienotās Karalistes VDAR, ir tiesīga saņemt no pārziņa vai apstrādātāja kompensāciju par šo kaitējumu, izņemot gadījumu, kad pārzinis vai apstrādātājs pierāda, ka tas nekādā veidā nav atbildīgs par notikumu, kas izraisījis kaitējumu. Kaitējums ietver gan finansiālus zaudējumus, gan kaitējumu, kas nav saistīts ar finansiāliem zaudējumiem, piemēram, spriedzi.

(119) Ceturtkārt, ja kāda persona uzskata, ka publiskās iestādes ir pārkāpušas tās tiesības, tostarp tiesības uz privātumu un datu aizsardzību, tā var saņemt kompensāciju Apvienotās Karalistes tiesās saskaņā ar 1998. gada Cilvēktiesību likumu. Pārziņi saskaņā ar 2018. gada DAL 3. daļu, proti, kompetentās iestādes, vienmēr ir publiskas iestādes 1998. gada Cilvēktiesību likuma nozīmē. Persona, kas apgalvo, ka publiska iestāde ir rīkojusies (vai plāno rīkoties) veidā, kas nav savienojams ar konvencijā paredzētajām tiesībām un līdz ar to ir prettiesisks saskaņā ar 1998. gada Cilvēktiesību likuma 6. panta 1. punktu, var celt prasību pret iestādi attiecīgajā tiesā vai tribunālā vai paļauties uz attiecīgajām tiesībām jebkurā tiesvedībā, ja attiecīgā persona ir (vai būtu) cietusi no nelikumīgas darbības ([197]).

([192]) 2018. gada DAL 165. pants.

([193]) 2018. gada DAL 166. pants jo īpaši attiecas uz šādām situācijām: a) komisārs neveic atbilstošus pasākumus, lai atbildētu uz sūdzību, b) komisārs nesniedz sūdzības iesniedzējam informāciju par sūdzības virzību vai par sūdzības iznākumu, līdz pagājis trīs mēnešu periods, kas sākas no brīža, kad komisārs saņēmis sūdzību, vai c) ja komisārs sūdzības izskatīšanu šajā periodā nav pabeidzis – nesniedz sūdzības iesniedzējam šādu informāciju turpmākajā trīs mēnešu periodā.

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

([195]) 2018. gada DAL 166. pants.

([196]) 2018. gada DAL 161. un 162. pants.

([197]) Sk. 2016. gada policijas lietu *Brown v Commissioner*, kurā tiesa par labu prasītājai, kas bija cēlusi prasību pret policiju, piesprieda atlīdzību saistībā ar datu aizsardzību. Tiesa lēma par labu prasītājai, apmierinot viņas prasību par 1998. gada DAL paredzēto pienākumu pārkāpumu, 1998. gada CTL (un ar to saistīto tiesību, kas minētas ECTK 8. pantā) pārkāpumu un deliktu – privātās informācijas ļaunprātīgu izmantošanu (atbildētājs beigās atzina, ka ir pārkāpis DAL un ECTK, tāpēc spriedums bija vērsts uz piemērota tiesiskās aizsardzības līdzekļa noteikšanu). Šo pārkāpumu rezultātā tiesa par labu prasītājai piesprieda atlīdzināt zaudējumus naudā.

(120) Ja tiesa konstatē, ka kāda publiskas iestādes darbība ir nelikumīga, tā var apmierināt šādu prasību vai atzīt tiesiskās aizsardzības līdzekli, vai savu pilnvaru ietvaros izdot rīkojumu, ko tā uzskata par taisnīgu un piemērotu ([198]). Tiesa var arī pasludināt primāra tiesību akta normu par nesaderīgu ar ECTK garantētajām tiesībām.

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

2.6. **Tālāka apmaiņa**

(122) Apvienotās Karalistes tiesību akti atļauj tiesībaizsardzības iestādei veikt datu apmaiņu ar citām iestādēm tādiem nolūkiem, kam tie sākotnēji netika vākti (t. s. "tālākā apmaiņa"), ievērojot konkrētus nosacījumus.

(123) Līdzīgi tam, kas paredzēts Direktīvas (ES) 2016/680 4. panta 2. punktā, 2018. gada DAL 36. panta 3. punktā ir atļauts (sākotnējam vai citam pārzinim) personas datus, ko kompetentā iestāde vāc tiesībaizsardzības nolūkā, turpmāk apstrādāt jebkuram citam tiesībaizsardzības nolūkam, ja pārzinis ar tiesību aktu ir pilnvarots apstrādāt datus citam nolūkam un apstrāde ir nepieciešama un samērīga ([199]). Šajā gadījumā visas garantijas, kas paredzētas 2018. gada DAL 3. daļā un analizētas iepriekš, attiecas uz saņēmējas iestādes veikto apstrādi.

(124) Apvienotās Karalistes tiesību sistēmā dažādi tiesību akti skaidri pieļauj tālāku apmaiņu. Konkrēti, i) 2017. gada Digitālās ekonomikas likums ļauj veikt apmaiņu starp publiskajām iestādēm vairākos nolūkos, piemēram, ja ir notikusi pret publisko sektoru vērsta krāpšana, kas publiskajai iestādei radītu zaudējumus vai to risku ([200]), vai ja pastāv parāds publiskajai iestādei vai valstij ([201]); ii) 2013. gada Noziedzības un tiesu likums ļauj apmainīties ar informāciju ar Valsts noziedzības apkarošanas aģentūru (VNAA) ([202]), lai apkarotu un izmeklētu smagu un organizētu noziedzību un sauktu pie atbildības par to; iii) 2007. gada Smago noziegumu likums ļauj publiskajām iestādēm izpaust informāciju krāpšanas apkarošanas organizācijām, lai novērstu krāpšanu ([203]).

(125) Ar šiem tiesību aktiem ir tieši paredzēts, ka informācijas apmaiņai ir jāatbilst 2018. gada DAL noteikumiem. Turklāt Policijas kolēģija ir izdevusi Atļauto profesionālo praksi informācijas apmaiņā ([204]), lai palīdzētu policijai ievērot tās datu aizsardzības pienākumus saskaņā ar Apvienotās Karalistes VDAR, DAL un 1998. gada Cilvēktiesību likumu. Informācijas apmaiņas atbilstību piemērojamajam datu aizsardzības tiesiskajam regulējumam, protams, var pārskatīt tiesā ([205]).

(126) Turklāt līdzīgi tam, ko paredz Direktīvas (ES) 2016/680 9. pants, 2018. gada DAL paredz, ka personas datus, kas ievākti jebkādā tiesībaizsardzības nolūkā, var apstrādāt ar tiesībaizsardzību nesaistītiem nolūkiem, ja apstrādi atļauj tiesību akti ([206]). Šis apmaiņas veids aptver divus scenārijus: 1) krimināllizmeklēšanas iestāde apmainās ar datiem ar tiesībaizsardzības iestādi, kas nav krimināltiesiska un izlūkošanas aģentūra (piemēram, finanšu vai nodokļu iestāde, konkurences iestāde, jauniešu sociālais dienests); 2) krimināllizmeklēšanas iestāde apmainās datiem ar izlūkošanas

([198]) 1998. gada Cilvēktiesību likuma 8. panta 1. punkts.
([199]) 2018. gada DAL 36. panta 3. punkts.
([200]) 2017. gada Digitālās ekonomikas likuma 56. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2017/30/contents.
([201]) 2017. gada Digitālās ekonomikas likuma 48. pants.
([202]) 2013. gada Noziedzības un tiesu likuma 7. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2013/22/contents.
([203]) 2007. gada Smago noziegumu likuma 68. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2007/27/contents.
([204]) Atļautā profesionālā prakse informācijas apmaiņā, pieejama vietnē https://www.app.college.police.uk/app-content/information-management/sharing-police-information.
([205]) Sk., piemēram, lietu *M v the Chief Constable of Sussex Police* (2019), EWHC 975 (Admin), kurā Augstajai tiesai tika lūgts izskatīt datu apmaiņu starp policiju un Uzņēmējdarbības noziegumu mazināšanas partnerību (*BCRP*) – organizāciju, kas ir pilnvarota pārvaldīt izraidīšanas paziņojumu sistēmu, ar ko personām liedz iekļūt tās biedru komerctelpās. Tiesa pārskatīja datu apmaiņu, kas notika, pamatojoties uz vienošanos, kuras mērķis bija aizsargāt sabiedrību un novērst noziedzību, un secināja, ka lielākā daļa datu apmaiņas aspektu ir likumīgi, izņemot saistībā ar kādu sensitīvu informāciju, kas tiek izplatīta starp policiju un *BCRP*. Cits piemērs ir lieta *Cooper v NCA* (2019), EWCA Civ 16, kurā Apelācijas tiesa apstiprināja datu apmaiņu starp policiju un Smagās organizētās noziedzības apkarošanas aģentūru (SONAA), kas ir tiesībaizsardzības iestāde un pašlaik ietilpst VNAA.
([206]) 2018. gada DAL 36. panta 4. punkts.

aģentūru. Pirmajā scenārijā personas datu apstrāde ietilps Apvienotās Karalistes VDAR, kā arī 2018. gada DAL 2. daļas darbības jomā. Kā norādīts lēmumā, kas pieņemts saskaņā ar Regulu (ES) 2016/679, Apvienotās Karalistes VDAR un 2018. gada DAL 2. daļā paredzētās garantijas nodrošina tādu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Savienībā nodrošinātajam aizsardzības līmenim ([207]).

(127) Otrajā scenārijā juridiskais pamats, kas atļauj kriminālizmeklēšanas iestādes savākto datu apmaiņu ar izlūkošanas aģentūru valsts drošības nolūkos, ir 2008. gada Pretterorisma likums (2008. gada PTL) ([208]). Saskaņā ar 2008. gada PTL ikviena persona var sniegt informāciju kādam no izlūkdienestiem, lai pildītu jebkuru no šā dienesta funkcijām, ieskaitot "valsts drošību".

(128) Attiecībā uz nosacījumiem, saskaņā ar kuriem var veikt datu apmaiņu valsts drošības nolūkiem, Izlūkdienestu likums un Drošības dienestu likums ierobežo izlūkdienestu spēju iegūt datus līdz apjomam, kas ir nepieciešams, lai pildītu to likumā noteiktās funkcijas. Kompetentajām iestādēm, uz kurām attiecas 2018. gada DAL 3. daļa un kuras vēlas apmainīties ar datiem ar izlūkdienestiem, papildus minēto aģentūru obligātajām funkcijām, kas noteiktas Izlūkdienestu likumā un Drošības dienestu likumā ([209]), būs jāņem vērā vairāki faktori/ierobežojumi. 2008. gada PTL 20. pantā ir precizēts, ka datu apmaiņai saskaņā ar 2008. gada PTL 19. pantu tik un tā jāatbilst datu aizsardzības tiesību aktiem; tas nozīmē, ka piemēro visus 2018. gada DAL paredzētos ierobežojumus un prasības. Turklāt tiesībaizsardzības iestādes un izlūkdienesti ir publiskās iestādes 1998. gada Cilvēktiesību likuma nozīmē, un tādējādi šīm iestādēm jānodrošina, ka tās rīkojas saskaņā ar ECTK garantētajām tiesībām, tostarp tās 8. pantu. Vārdu sakot, šīs prasības nozīmē, ka visai datu apmaiņai starp tiesībaizsardzības iestādēm un izlūkdienestiem jāatbilst datu aizsardzības tiesību aktiem un ECTK.

(129) Valsts drošības nolūkos izlūkdienestu veiktajai tādu personas datu apstrādei, kas saņemti vai iegūti no tiesībaizsardzības iestādēm, piemēro vairākus nosacījumus un garantijas ([210]). 2018. gada DAL 4. daļu piemēro visu veidu apstrādei, ko veic izlūkdienesti vai kas tiek veikta to vārdā. Tajā ir noteikti galvenie datu aizsardzības principi

([207]) Komisijas Īstenošanas lēmums par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/679, C(2021) 4800.

([208]) 2008. gada Pretterorisma likuma 19. pants, pieejams vietnē https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) 1994. gada Izlūkdienestu likuma 2. panta 2. punktā (sk. https://www.legislation.gov.uk/ukpga/1994/13/contents) ir noteikts, ka "izlūkdienesta priekšnieks ir atbildīgs par šā dienesta efektivitāti, un viņa pienākums ir nodrošināt: a) kārtību, kā panākt, lai izlūkdienests nesaņem citu informāciju kā vien to, kas vajadzīga tā funkciju pareizai izpildei, un lai šis dienests neizpauž nekādu informāciju, izņemot, ja tas ir nepieciešams: i) šim nolūkam; ii) valsts drošības interesēs; iii) smagu noziegumu novēršanas vai atklāšanas nolūkā; vai iv) jebkura kriminālprocesa nolūkā; un b) ka izlūkdienests neveic nekādas darbības, lai sekmētu kādas Apvienotās Karalistes politiskās partijas intereses", savukārt 1989. gada Drošības dienestu likuma 2. panta 2. punktā (sk. https://www.legislation.gov.uk/ukpga/1989/5/contents) ir noteikts, ka "ģenerāldirektors ir atbildīgs par dienesta efektivitāti, un viņa pienākums ir nodrošināt: a) kārtību, kā panākt, lai dienests nesaņem citu informāciju kā vien to, kas vajadzīga tā funkciju pareizai izpildei, un lai šis dienests neizpauž nekādu informāciju, izņemot, ja tas ir nepieciešams šim nolūkam vai smagu noziegumu novēršanai vai atklāšanai vai jebkurā kriminālprocesā, un b) ka dienests neveic nekādas darbības, lai sekmētu kādas politiskas partijas intereses; un c) ka ir vienošanās ar Valsts noziedzības apkarošanas aģentūras ģenerāldirektoru par to, kā dienesta rīcību saskaņā ar šā likuma 1. panta 4. punktu saskaņot ar policijas vienību, Valsts noziedzības apkarošanas aģentūras un citu tiesībaizsardzības iestāžu darbību".

([210]) Garantijas un izlūkdienestu pilnvaru ierobežojumus reglamentē arī 2016. gada Izmeklēšanas pilnvaru likums, kas kopā ar 2000. gada Anglijas, Velsas un Ziemeļīrijas Izmeklēšanas pilnvaru regulēšanas likumu un 2000. gada Skotijas Izmeklēšanas pilnvaru regulēšanas likumu nosaka šādu pilnvaru izmantošanas juridisko pamatu. Tomēr šīs pilnvaras nav nozīmīgas saistībā ar "tālāku apmaiņu", jo tās attiecas uz izlūkošanas aģentūru tieši veiktu personas datu vākšanu. Ar Izmeklēšanas pilnvaru likumu piešķirto izlūkošanas aģentūru pilnvaru novērtējumu skatīt Komisijas Īstenošanas lēmumā par personas datu pietiekamu aizsardzību Apvienotajā Karalistē, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/679, C(2021) 4800.

(likumīgums, godprātība un pārredzamība ([211]); mērķa ierobežojums ([212]); datu minimizēšana ([213]); precizitāte ([214]); datu glabāšanas ierobežojumi ([215]) un drošība ([216])), kā arī paredzēti nosacījumi īpašu kategoriju datu apstrādei ([217]), datu subjekta tiesības ([218]), prasība par datu integrētu aizsardzību ([219]) un reglamentēta personas datu starptautiska nosūtīšana ([220]).

(130) Tajā pašā laikā 2018. gada DAL 110. pantā ir paredzēts atbrīvojums no konkrētiem 2018. gada DAL 4. daļas noteikumiem, ja šāds atbrīvojums ir nepieciešams, lai aizsargātu valsts drošību. 2018. gada DAL 110. panta 2. punktā ir uzskaitīti noteikumi, kuriem ir atļauts piemērot atbrīvojumu. Tie ietver datu aizsardzības principus (izņemot likumīguma principu), datu subjekta tiesības, pienākumu informēt informācijas komisāru par datu aizsardzības pārkāpumu, informācijas komisāra pārbaudes pilnvaras saskaņā ar starptautiskajām saistībām, noteiktas informācijas komisāra izpildes pilnvaras, noteikumus, kas paredz, ka noteikti datu aizsardzības pārkāpumi ir krimināli sodāmi, un noteikumus, kas attiecas uz īpašiem apstrādes nolūkiem, piemēram, žurnālistikas, akadēmiskiem vai mākslas nolūkiem. Šo atbrīvojumu var izmantot, pamatojoties uz katra gadījuma atsevišķu analīzi ([221]). Kā paskaidrojušas Apvienotās Karalistes iestādes un kā apliecina Apvienotās Karalistes tiesu judikatūra, "a) pārzinim ir jāņem vērā faktiskās sekas attiecībā uz valsts drošību vai aizsardzību, ja tam bija jāievēro konkrētais datu aizsardzības noteikums un ja tas varēja saprātīgi ievērot parasto noteikumu, neietekmējot valsts drošību vai aizsardzību" ([222]). IKB pārrauga, vai atbrīvojums ir izmantots pareizi ([223]).

([211]) Saskaņā ar 2018. gada DAL 86. panta 6. punktu, lai noteiktu apstrādes godprātību un pārredzamību, ir jāņem vērā datu iegūšanas paņēmieni. Šajā ziņā godprātības un pārredzamības prasība ir izpildīta, ja dati tiek iegūti no personas, kam ar likumu ir atļauts vai noteikts pienākums tos sniegt.

([212]) Saskaņā ar 2018. gada DAL 87. pantu apstrādes nolūkiem jābūt konkrētiem, skaidriem un leģitīmiem. Datus nedrīkst apstrādāt ar to vākšanas nolūku nesaderīgā veidā. Saskaņā ar 87. panta 3. punktu personas datu turpmāku saderīgu apstrādi var atļaut tikai tad, ja pārzinim ar tiesību aktu ir atļauts apstrādāt datus šādā nolūkā un apstrāde ir nepieciešama un samērīga ar šādu nolūku. Apstrādi uzskata par saderīgu, ja apstrāde tiek veikta arhivēšanas nolūkā sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkā vai statistikas nolūkā, kā arī tai piemēro atbilstošas garantijas (2018. gada DAL 87. panta 4. punkts).

([213]) Personas datiem jābūt atbilstīgiem, būtiskiem un ne pārmērīgiem (2018. gada DAL 88. pants).

([214]) Personas datiem jābūt precīziem un atjauninātiem (2018. gada DAL 89. pants).

([215]) Personas datus nedrīkst glabāt ilgāk, nekā nepieciešams (2018. gada DAL 90. pants).

([216]) Sestais datu aizsardzības princips paredz, ka personas dati ir jāapstrādā tā, lai apstrāde ietvertu atbilstošu drošības pasākumu veikšanu attiecībā uz riskiem, kas rodas, apstrādājot personas datus. Riski ietver (ne tikai) nejaušu vai neatļautu piekļuvi personas datiem vai to iznīcināšanu, nozaudēšanu, izmantošanu, grozīšanu vai izpaušanu (2018. gada DAL 91. pants). 107. pantā ir arī noteikts, ka 1) katram pārzinim jāievieš atbilstoši drošības pasākumi, kas ir piemēroti personas datu apstrādes riskiem, un 2) automatizētas apstrādes gadījumā katrs pārzinis un katrs apstrādātājs īsteno preventīvus vai mīkstinošus pasākumus, pamatojoties uz riska izvērtējumu.

([217]) 2018. gada DAL 86. panta 2. punkta b) apakšpunkts un 10. pielikums.

([218]) 2018. gada DAL 4. daļas 3. nodaļa, jo īpaši tiesības: piekļūt datiem, labot un dzēst tos, iebilst pret apstrādi un nebūt automatizētas lēmumu pieņemšanas subjektam, iejaukties automatizētā lēmumu pieņemšanā un tikt informētam par lēmumu pieņemšanu. Turklāt pārzinim jāsniedz datu subjektam informācija par tā personas datu apstrādi.

([219]) 2018. gada DAL 103. pants.

([220]) 2018. gada DAL 109. pants. Personas datu nosūtīšana starptautiskām organizācijām vai valstīm ārpus Apvienotās Karalistes ir iespējama, ja šāda nosūtīšana ir nepieciešams un samērīgs pasākums, ko veic likumā noteikto pārziņa funkciju izpildei vai citiem nolūkiem, kas paredzēti konkrētos 1989. gada Drošības dienestu likuma un 1994. gada Izlūkdienestu likuma pantos.

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

([222]) Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, H sadaļa "Valsts drošības datu aizsardzības un izmeklēšanas pilnvaru regulējums", 15.–16. lpp., pieejams vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Sk. arī lietu *Baker v Secretary of State* (sk. iepriekš 220. zemsvītras piezīmi), kurā tribunāls atcēla iekšlietu ministra izdoto valsts drošības sertifikātu un apstiprināja valsts drošības izņēmuma piemērošanu, ņemot vērā, ka nebija iemesla paredzēt vispārēju izņēmumu attiecībā uz pienākumu atbildēt uz piekļuves pieprasījumiem un ka šāda izņēmuma atļaušana visās situācijās bez katra gadījuma atsevišķas analīzes pārsniedza to, kas ir nepieciešams un samērīgs valsts drošības aizsardzībai.

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

(131) Turklāt attiecībā uz iespēju valsts drošības aizsardzības nolūkā ierobežot kādas no iepriekš minētajām tiesībām 2018. gada DAL 79. pantā ir paredzēta iespēja, ka pārzinis var pieprasīt Ministru kabineta ministra vai ģenerālprokurora parakstītu apliecinājumu, ka šādu tiesību ierobežojums ir vai jebkurā laikā ir bijis nepieciešams un samērīgs pasākums valsts drošības aizsardzībai ([224]). Apvienotās Karalistes valdība ir izdevusi norādījumus par valsts drošības sertifikātiem saskaņā ar 2018. gada DAL, kuros īpaši uzsvērts, ka jebkādiem datu subjektu tiesību ierobežojumiem valsts drošības aizsardzības nolūkā jābūt samērīgiem un nepieciešamiem ([225]). Visi valsts drošības sertifikāti jāpublicē IKB tīmekļa vietnē ([226]).

(132) Sertifikātam jābūt izdotam uz laiku, kas nepārsniedz piecus gadus, un izpildvarai tas regulāri jāpārskata ([227]). Sertifikātā norāda personas datus vai personas datu kategorijas, kam piemēro atbrīvojumu, kā arī 2018. gada DAL noteikumus, uz kuriem attiecas atbrīvojums ([228]).

(133) Svarīgi ņemt vērā, ka valsts drošības sertifikāti nedod papildu pamatu datu aizsardzības tiesību ierobežošanai valsts drošības apsvērumu dēļ. Citiem vārdiem sakot, pārzinis vai apstrādātājs var paļauties uz sertifikātu tikai tad, ja tas ir secinājis, ka ir nepieciešams atsaukties uz atbrīvojumu sakarā ar valsts drošību, kas jāpiemēro katrā gadījumā atsevišķi. Pat tad, ja uz konkrēto jautājumu attiecas valsts drošības sertifikāts, IKB var izmeklēt, vai konkrētajā gadījumā paļaušanās uz atbrīvojumu sakarā ar valsts drošību ir bijusi pamatota ([229]).

(134) Jebkura persona, kuru tieši ietekmē sertifikāta izsniegšana, var pārsūdzēt sertifikātu ([230]) Augstākajā tribunālā ([231]) vai, ja sertifikātā dati identificēti ar vispārīgu aprakstu, apstrīdēt sertifikāta piemērošanu konkrētiem datiem ([232]).

(135) Tribunāls pārskata lēmumu izdot sertifikātu un lemj, vai sertifikāta izdošanai ir bijis pamatots iemesls ([233]). Tas var vērtēt dažādus jautājumus, tostarp nepieciešamību, samērīgumu un likumīgumu, ņemot vērā ietekmi uz datu subjektu tiesībām un līdzsvarojot tās ar nepieciešamību aizsargāt valsts drošību. Tādējādi tribunāls var noteikt, ka sertifikāts neattiecas uz konkrētiem personas datiem, kas ir pārsūdzības priekšmets ([234]).

([224]) Ar 2018. gada DAL ir atcelta iespēja izdot apliecinājumu saskaņā ar 1998. gada Datu aizsardzības likuma 28. panta 2. punktu. Tomēr joprojām ir iespējams izdot "vecos" apliecinājumus, ja vien ir izvirzīts vēsturisks apstrīdēšanas prasījums saskaņā ar 1998. gada likumu (sk. 2018. gada DAL20. pielikuma 5. daļas 17. punktu). Tomēr šādu iespēju, šķiet, izmantot var ļoti reti – vien atsevišķos gadījumos, piemēram, gadījumā, kad datu subjekts apstrīd to, ka atbrīvojums sakarā ar valsts drošību izmantots attiecībā uz apstrādi, ko veikusi publiska iestāde uz 1998. gada likuma pamata. Jāņem vērā, ka šādos gadījumos pilnā apmērā piemērojams 1998. gada DAL 28. pants, tātad arī datu subjekta iespēja apstrīdēt sertifikātu. Patlaban saskaņā ar 1998. gada DAL nav izdots neviens valsts drošības sertifikāts.

([225]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem saskaņā ar 2018. gada Datu aizsardzības likumu, pieejami vietnē https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) 2018. gada DAL 130. pantā ir noteikts, ka IKB var nolemt nepublicēt sertifikāta tekstu vai daļu no tā, ja tas būtu pretrunā valsts drošības interesēm vai sabiedrības interesēm vai varētu apdraudēt kādas personas drošību. Šādos gadījumos IKB tomēr publicē informāciju par to, ka sertifikāts ir izdots.

([227]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, 15. punkts, sk. 225. zemsvītras piezīmi.

([228]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, 5. punkts, 225. zemsvītras piezīme.

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

([230]) 2018. gada DAL 111. panta 3. punkts.

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

([232]) 2018. gada DAL 111. panta 5. punkts.

([233]) Lietā *Baker v Secretary of State* (sk. 221. zemsvītras piezīmi) Informācijas tribunāls atcēla iekšlietu ministra izdoto valsts drošības sertifikātu, ņemot vērā, ka nebija iemesla paredzēt vispārēju izņēmumu attiecībā uz pienākumu atbildēt uz piekļuves pieprasījumiem un ka šāda izņēmuma atļaušana visās situācijās bez katra gadījuma atsevišķas analīzes pārsniedza to, kas ir nepieciešams un samērīgs valsts drošības aizsardzībai.

([234]) Apvienotās Karalistes valdības norādījumi par valsts drošības sertifikātiem, 25. punkts, 224. zemsvītras piezīme.

(136) Atšķirīgs iespējamo ierobežojumu kopums saskaņā ar 2018. gada DAL 11. pielikumu attiecas uz dažiem 2018. gada DAL 4. daļas noteikumiem ([235]), ar ko aizsargā citus svarīgus vispārēju sabiedrības interešu vai aizsargātu interešu mērķus, piemēram, parlamentārās privilēģijas, advokāta un klienta saziņas konfidencialitāti, tiesvedības norisi vai bruņoto spēku kaujas efektivitāti. Atbrīvojumi šo noteikumu piemērošanā tiek paredzēti attiecībā uz noteiktām informācijas kategorijām ("balstīti uz kategoriju") vai tiktāl, ciktāl šo noteikumu piemērošana varētu kaitēt aizsargātajām interesēm ("balstīti uz aizskārumu") ([236]). Uz atbrīvojumiem, kas balstīti uz aizskārumu, var atsaukties tikai tiktāl, ciktāl norādītā datu aizsardzības noteikuma piemērošana varētu kaitēt konkrētajām interesēm. Tāpēc atbrīvojuma izmantošana vienmēr ir jāpamato, atsaucoties uz attiecīgo aizskārumu, kas varētu rasties konkrētajā gadījumā. Uz kategoriju balstītus atbrīvojumus var izmantot tikai attiecībā uz konkrētu, precīzi definētu informācijas kategoriju, kurai piešķirts atbrīvojums. To nolūks un sekas ir līdzīgi vairākiem Apvienotās Karalistes VDAR izņēmumiem (saskaņā ar 2018. gada DAL 2. pielikumu), kas savukārt atspoguļo VDAR 23. pantā paredzētos izņēmumus.

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

(138) Personas datu apstrādi, ko veic izlūkdienesti saskaņā ar 2018. gada DAL 4. daļu, pārrauga informācijas komisārs ([237]).

(139) Informācijas komisāra vispārīgās funkcijas saistībā ar izlūkdienestu veikto personas datu apstrādi saskaņā ar 2018. gada DAL 4. daļu ir noteiktas 2018. gada DAL 13. pielikumā. Šie uzdevumi jo īpaši ietver, bet ne tikai, 2018. gada DAL 4. daļas uzraudzību un izpildes nodrošināšanu, sabiedrības informētības veicināšanu, ieteikumus parlamentam, valdībai un citām iestādēm par likumdošanas un administratīvajiem pasākumiem, pārziņu un apstrādātāju informētības veicināšanu par viņu pienākumiem, informācijas sniegšanu datu subjektam par datu subjekta tiesību īstenošanu un izmeklēšanas veikšanu.

(140) Attiecībā uz 2018. gada DAL 3. daļu komisāram ir pilnvaras paziņot pārziņiem par iespējamu pārkāpumu un izdot brīdinājumus, ka ar apstrādi, iespējams, pārkāpj noteikumus, un, ja pārkāpums ir apstiprinājies, izteikt rājienu. Tas var arī izdot izpildes un soda paziņojumus par konkrētu tiesību akta noteikumu pārkāpumiem ([238]). Tomēr atšķirībā no citām 2018. gada DAL daļām komisārs nevar izdot novērtējuma paziņojumu valsts drošības iestādei ([239]).

(141) Turklāt 2018. gada DAL 110. pantā ir paredzēts izņēmums attiecībā uz noteiktu komisāra pilnvaru izmantošanu, ja tas ir nepieciešams valsts drošības aizsardzības nolūkos. Tas ietver komisāra pilnvaras izdot (jebkādus) paziņojumus saskaņā ar DAL (informatīvos, novērtējuma, izpildes un soda paziņojumus), pilnvaras veikt pārbaudes saskaņā ar

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

([236]) Saskaņā ar Apvienotās Karalistes paskaidrojuma dokumentu "uz kategoriju balstīti" ir šādi atbrīvojumi: i) informācija par valsts goda apbalvojumu un titulu piešķiršanu; ii) advokāta un klienta saziņas konfidencialitāte; iii) konfidenciālas atsauksmes par darbu, mācībām vai izglītību un iv) eksāmenu jautājumi un atzīmes. Izņēmumi, kas ir "balstīti uz aizskārumu", attiecas uz šādiem jautājumiem: i) noziedzības novēršanu vai atklāšanu; likumpārkāpēju aizturēšanu un saukšanu pie atbildības; ii) parlamentāro privilēģiju; iii) tiesvedību; iv) valsts bruņoto spēku kaujas efektivitāti; v) Apvienotās Karalistes ekonomisko labklājību; vi) sarunām ar datu subjektu; vii) zinātniskas vai vēsturiskas pētniecības vai statistikas nolūkiem; viii) arhivēšanu sabiedrības interesēs. Apvienotās Karalistes paskaidrojuma dokuments aizsardzības līmeņa pietiekamības apspriešanai, H sadaļa "Valsts drošība", 13. lpp., sk. 222. zemsvītras piezīmi.

([237]) 2018. gada DAL 116. pants.

([238]) Saskaņā ar 2018. gada DAL 149. panta 2. punktu, skatot to kopā ar 155. pantu, izpildes un soda paziņojumus pārzinim vai apstrādātājam var izsniegt saistībā ar to, ka pārkāpta 2018. gada DAL 4. daļas 2. nodaļa (apstrādes principi), 2018. gada DAL 4. daļas noteikums, kas piešķir tiesības datu subjektam, 2018. gada DAL 108. pantā noteiktās prasības ziņot komisāram par personas datu aizsardzības pārkāpumu, kā arī 2018. gada DAL 109. pantā noteiktie principi par personas datu nosūtīšanu uz trešām valstīm, valstīm, kas nav konvencijas dalībvalstis, un starptautiskām organizācijām. (Sīkāk par izpildes un soda paziņojumiem sk. 102.–103. apsvērumā.)

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

starptautiskajām saistībām, iekļūšanas un pārbaudes pilnvaras, kā arī noteikumus par nodarījumiem ([240]). Kā paskaidrots 136. apsvērumā, šie izņēmumi tiks piemēroti tikai tad, ja tie būs nepieciešami un samērīgi, un katrā gadījumā tos apsvērs atsevišķi. Šo izņēmumu piemērošanu var pārskatīt tiesā ([241]).

(142) IKB un Apvienotās Karalistes izlūkdienesti ir parakstījuši saprašanās memorandu ([242]), ar ko izveido sistēmu sadarbībai vairākos jautājumos, tostarp attiecībā uz paziņojumiem par datu aizsardzības pārkāpumiem un datu subjektu sūdzību izskatīšanu. Jo īpaši tajā paredzēts, ka, saņemot sūdzību, IKB novērtēs, vai pienācīgi izdarīta atsauce uz atbrīvojumu sakarā ar valsts drošību. Atbildes uz IKB pieprasījumiem, kas iesniegti saistībā ar individuālu sūdzību izskatīšanu par attiecīgajiem Apvienotās Karalistes valdības norādījumiem par valsts drošības sertifikātiem saskaņā ar Datu aizsardzības likumu, ir jāsniedz 20 darba dienu laikā, izmantojot atbilstošus drošus kanālus, ja ir iesaistīta klasificēta informācija. No 2018. gada aprīļa līdz šim brīdim IKB no fiziskām personām ir saņēmis 21 sūdzību par izlūkdienestiem. Katra sūdzība tika novērtēta, un datu subjektam tika paziņots tās rezultāts ([243]).

(143) Turklāt Izlūkošanas un drošības komiteja (IDK) īsteno parlamentāro pārraudzību pār datu apstrādi, ko veic izlūkošanas aģentūras. Šīs komitejas juridiskais pamats ir 2013. gada Tiesiskuma un drošības likums (2013. gada TDL) ([244]). Ar minēto likumu IDK ir izveidota kā Apvienotās Karalistes parlamenta komiteja. IDK sastāv no locekļiem, kas pieder pie kādas no parlamenta palātām un ko pēc apspriešanās ar opozīcijas līderi ieceļ premjerministrs ([245]). IDK ir jāsagatavo gada pārskats parlamentam par tās funkciju izpildi, kā arī citi ziņojumi, ko tā uzskata par lietderīgiem ([246]).

(144) Kopš 2013. gada IDK ir piešķirtas lielākas pilnvaras, tostarp drošības dienestu operatīvās darbības pārraudzība. Saskaņā ar 2013. gada TDL 2. pantu IDK uzdevums ir pārraudzīt valsts drošības dienestu izdevumus, pārvaldību, politiku un darbību. 2013. gada TDL paredz, ka IDK var veikt operatīvo jautājumu izmeklēšanu, ja tie nav saistīti ar

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

([241]) Sk., piemēram, lietu *Baker v Secretary of State for the Home Department* (sk. 221. zemsvītras piezīmi).

([242]) IKB un Apvienotās Karalistes izlūkdienestu kopienas saprašanās memorands, sk. 231. zemsvītras piezīmi.

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

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

([245]) 2013. gada TDL 1. pants. Ministri nav tiesīgi kļūt par locekļiem. Locekļi ieņem savu amatu IDK uz tā parlamenta pilnvaru laiku, kura laikā viņi ir iecelti. Viņus var atbrīvot no amata ar tās palātas rezolūciju, kura tos iecēlusi, vai ja viņi vairs nav deputāti, vai ja viņi kļūst par ministriem. Loceklis var arī atkāpties no amata.

([246]) Komitejas ziņojumi un paziņojumi ir pieejami tiešsaistē vietnē http://isc.independent.gov.uk/committee-reports. 2015. gadā IDK izdeva ziņojumu "Privātums un drošība: mūsdienīgs un pārredzams tiesiskais regulējums" (sk. https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), kurā tā vērtēja tiesisko regulējumu attiecībā uz izlūkošanas aģentūru izmantotajām novērošanas metodēm un nāca klajā ar vairākiem ieteikumiem, kas pēc tam tika izskatīti un iekļauti Izmeklēšanas pilnvaru likumprojektā, kurš kļuva par likumu – 2016. gada IPL. Valdības atbilde uz Privātuma un drošības ziņojumu ir pieejama vietnē https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

tobrīd notiekošajām operācijām ([247]). Saprašanās memorandā, par kuru vienojās premjerministrs un IDK ([248]), ir sīki izklāstīti elementi, kas jāņem vērā, apsverot, vai darbība nav saistīta ar kādu notiekošu operāciju ([249]). Premjerministrs var arī lūgt IDK izmeklēt notiekošās operācijas, un tā var pārskatīt aģentūru brīvprātīgi sniegto informāciju.

(145) Saskaņā ar 2013. gada TDL 1. pielikumu IDK var lūgt jebkuram no trīs izlūkdienestiem, lai tā vadītājs sniedz jebkādu informāciju. Aģentūrai šāda informācija ir jādara pieejama, ja vien ministrs to neaptur ar veto ([250]). Apvienotās Karalistes iestādes paskaidroja, ka praksē IDK tiek atteikts sniegt ļoti maz informācijas ([251]).

(146) Attiecībā uz tiesisko aizsardzību, pirmkārt, saskaņā ar 2018. gada DAL 165. panta 2. punktu, ja datu subjekts uzskata, ka saistībā ar personas datiem, kas attiecas uz viņu, ir pārkāpta 2018. gada DAL 4. daļa, tostarp ļaunprātīgi izmantotas valsts drošības atkāpes un ierobežojumi, datu subjekts var iesniegt sūdzību IKB.

(147) Turklāt saskaņā ar 2018. gada DAL 4. daļu personām ir tiesības vērsties Augstajā tiesā (Skotijā – "*Court of Session*"), lai saņemtu rīkojumu, ar ko pārzinim uzdod ievērot tiesības piekļūt datiem ([252]), iebilst pret apstrādi ([253]) un labot vai dzēst datus.

(148) Personām ir tiesības arī pieprasīt kompensāciju par kaitējumu, kas nodarīts tādēļ, ka pārzinis vai apstrādātājs pārkāpis 2018. gada DAL 4. daļas prasības ([254]). Kaitējums ietver gan finansiālus zaudējumus, gan kaitējumu, kas nav saistīts ar finansiāliem zaudējumiem, piemēram, spriedzi ([255]).

(149) Visbeidzot, persona var iesniegt sūdzību Izmeklēšanas pilnvaru tribunālam par jebkādu Apvienotās Karalistes izlūkošanas aģentūru rīcību vai rīcību to vārdā ([256]). Izmeklēšanas pilnvaru tribunāls (IPT) ir izveidots ar 2000. gada Anglijas, Velsas un Ziemeļīrijas Izmeklēšanas pilnvaru regulēšanas likumu un 2000. gada Skotijas Izmeklēšanas pilnvaru regulēšanas likumu (2000. gada IPRL) un ir neatkarīgs no izpildvaras ([257]). Saskaņā ar 2000. gada IPRL 65. pantu IPT locekļus uz pieciem gadiem amatā ieceļ Viņas Majestāte.

(150) Tribunāla locekli no amata var atbrīvot Viņas Majestāte pēc abu parlamenta palātu ([258]) uzrunas ([259]).

(151) Lai iesniegtu prasību IPT ("prasības attiecībā uz tiesībām vērsties tribunālā"), saskaņā ar 2000. gada IPRL 65. pantu personai ir jābūt pārliecībai, ka i) ir notikusi izlūkdienesta rīcība attiecībā uz šo personu, jebkuru tās īpašumu, jebkuru veikto vai saņemto, vai paredzēto saziņu, vai to, ka tā ir izmantojusi jebkuru pasta pakalpojumu, telesakaru pakalpojumu vai telesakaru sistēmu ([260]), un ii) šī rīcība ir notikusi "apstrīdamos

([247]) 2013. gada TDL 2. pants.
([248]) Saprašanās memorands starp premjerministru un IDK, pieejams vietnē http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Saprašanās memorands starp premjerministru un IDK, 14. punkts, sk. 248. zemsvītras piezīmi.
([250]) Ministrs var uzlikt veto informācijas izpaušanai tikai divu iemeslu dēļ: ja informācija ir sensitīva un valsts drošības interesēs to nedrīkst izpaust IDK; ja tā ir tāda informācija, ka gadījumā, ja ministram to pieprasītu iesniegt Pārstāvju palātas īpašajai nozaru komitejai, ministrs uzskatītu (ne tikai valsts drošības apsvērumu dēļ) par pareizu to nedarīt (2013. gada TDL 1. pielikuma 4. punkta 2. apakšpunkts).
([251]) Apvienotās Karalistes paskaidrojuma dokuments, H sadaļa "Valsts drošība", 43. lpp.
([252]) 2018. gada DAL 94. panta 11. punkts.
([253]) 2018. gada DAL 99. panta 4. punkts.
([254]) 2018. gada DAL 169. pants, kas ļauj prasību iesniegt "personai, kurai nodarīts kaitējums datu aizsardzības tiesību aktu prasību pārkāpuma dēļ".
([255]) 2018. gada DAL 169. panta 5. punkts.
([256]) Sk. IPRL 65. panta 2. punkta b) apakšpunktu.
([257]) Saskaņā ar 2000. gada IPRL 3. pielikumu locekļiem ir jābūt noteiktai pieredzei tieslietu jomā un viņi var tikt iecelti atkārtoti.
([258]) 2000. gada IPRL 3. pielikuma 1. punkta 5. apakšpunkts.
([259]) Attiecībā uz jēdzienu "uzruna" sk. 183. zemsvītras piezīmi.
([260]) 2000. gada IPRL 65. panta 4. punkts.

apstākļos" ([261]) vai "to ir veikuši izlūkdienesti vai tā ir notikusi viņu uzdevumā" ([262]). Tā kā jo īpaši šis "pārliecības" standarts ir interpretēts salīdzinoši plaši ([263]), prasības attiecībā uz tiesībām vērsties tribunālā ir relatīvi zemas.

(152) Ja tribunāls izskata tam iesniegtu sūdzību, tā pienākums ir izmeklēt, vai personas, par kurām sūdzībā ir izvirzīti kādi apgalvojumi, ir rīkojušās attiecībā uz sūdzības iesniedzēju, kā arī izmeklēt iestādi, kas, iespējams, varētu būt iesaistījusies pārkāpumos, un to, vai apgalvotā rīcība vispār ir notikusi ([264]). Ja tribunāls izskata kādu lietu, tam, pieņemot nolēmumu šajā lietā, ir jāpiemēro tie paši principi, kas tiktu piemēroti tiesai, izskatot pieteikumu par pārskatīšanu tiesā ([265]).

(153) Tribunālam ir jāinformē sūdzības iesniedzējs par to, vai ir pieņemts tam labvēlīgs lēmums vai nē ([266]). Saskaņā ar 2000. gada IPRL 67. panta 6. un 7. punktu tribunālam ir pilnvaras izdot pagaidu rīkojumus un paredzēt atlīdzināšanu vai izdot citu rīkojumu, ko tas uzskata par piemērotu ([267]). Saskaņā ar 2000. gada IPRL 67.A pantu tribunāla nolēmumu var pārsūdzēt, ja tribunāls vai attiecīgā apelācijas tiesa ir to atļāvusi.

(154) Konkrēti, personas var iesniegt prasību IPT – un saņemt kompensāciju –, ja tās uzskata, ka publiskā iestāde ir rīkojusies (vai plāno rīkoties) ar ECTK tiesībām, tostarp tiesībām uz privātumu un datu aizsardzību, nesaderīgā veidā, kas tādējādi ir prettiesisks saskaņā ar 1998. gada Cilvēktiesību likuma 6. panta 1. punktu. IPT ir atzīta ekskluzīva jurisdikcija attiecībā uz visām Cilvēktiesību likuma prasībām, kas saistītas ar izlūkošanas aģentūrām. Kā norādījusi Augstā tiesa, tas nozīmē, ka "jautājumu par to, vai saskaņā ar konkrētās lietas faktiem ir noticis Cilvēktiesību likuma pārkāpums, principā var izvirzīt un izskatīt neatkarīga tiesa, kurai ir pieejami visi attiecīgie materiāli, tostarp slepeni materiāli. (..) Šajā kontekstā mēs arī paturam prātā, ka tagad ir paredzēta iespēja pārsūdzēt IPT lēmumu attiecīgajā apelācijas tiesā (Anglijā un Velsā tā būtu Apelācijas tiesa) un ka Augstākā tiesa nesen nolēma, ka IPT principā ir pakļauts tiesas kontrolei: sk. *R (Privacy International) v Investigatory Powers Tribunal* (2019), UKSC 22; (2019) 2 WLR 1219" ([268]). Ja IPT konstatē, ka kāda publiskas iestādes darbība ir nelikumīga, tas var apmierināt šādu prasību vai atzīt tiesiskās aizsardzības līdzekli, vai savu pilnvaru ietvaros izdot rīkojumu, ko tas uzskata par taisnīgu un piemērotu ([269]).

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

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

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

([264]) 2000. gada IPRL 67. panta 3. punkts.

([265]) 2000. gada IPRL 67. panta 2. punkts.

([266]) 2000. gada IPRL 68. panta 4. punkts.

([267]) Minētais var ietvert rīkojumu, ar ko pieprasa iznīcināt jebkādu publiskās iestādes rīcībā esošo informāciju, kas attiecas uz kādu personu.

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

([269]) 1998. gada Cilvēktiesību likuma 8. panta 1. punkts.

(155) Pēc valsts tiesiskās aizsardzības līdzekļu izsmelšanas indivīds var saņemt kompensāciju, vēršoties Eiropas Cilvēktiesību tiesā par ECTK garantēto tiesību, tostarp tiesību uz privātumu un datu aizsardzību, pārkāpumiem.

(156) No iepriekš minētā izriet, ka saskaņā ar šo lēmumu nosūtīto datu apmaiņu, ko veic Apvienotās Karalistes kriminālizmeklēšanas iestādes ar citām publiskajām iestādēm, tostarp izlūkošanas aģentūrām, reglamentē ierobežojumi un nosacījumi, kas nodrošina, ka šāda tālāka apmaiņa būs nepieciešama un samērīga un ka uz to attieksies īpašas datu aizsardzības garantijas saskaņā ar 2018. gada DAL. Turklāt datu apstrādi, ko veic attiecīgās publiskās iestādes, pārrauga neatkarīgas struktūras, un skartajām personām ir pieejami efektīvi tiesiskās aizsardzības līdzekļi.

3. **SECINĀJUMS**

(157) Komisija uzskata, ka 2018. gada DAL 3. daļa attiecībā uz personas datiem, kurus krimināltiesību aktu piemērošanas nolūkā Savienības kompetentās iestādes nosūta Apvienotās Karalistes kompetentajām iestādēm, nodrošina personas datu aizsardzības līmeni, kurš pēc būtības ir līdzvērtīgs Direktīvā (ES) 2016/680 garantētajam līmenim.

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

(159) 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, tostarp saistībā ar personas datu apmaiņu starp tiesībaizsardzības iestādēm un citām publiskajām iestādēm, piemēram, valsts drošības iestādēm, būs tikai tāds, kas ir absolūti nepieciešams attiecīgā leģitīmā mērķa sasniegšanai, un ka pastāv efektīva tiesiskā aizsardzība pret šādu ierobežošanu.

(160) Tādēļ būtu jāpieņem lēmums, ka Apvienotā Karaliste nodrošina pietiekamu aizsardzības līmeni Direktīvas (ES) 2016/680 36. panta 2. punkta nozīmē, kas interpretēts, ņemot vērā Pamattiesību hartu.

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

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

(162) 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.

(163) Tādējādi lēmums par aizsardzības līmeņa pietiekamību, ko Komisija pieņēmusi saskaņā ar Direktīvas (ES) 2016/680 36. panta 3. punktu, ir saistošs visām dalībvalstu struktūrām, kurām tas adresēts, tostarp to neatkarīgajām uzraudzības iestādēm. Konkrēti, šā lēmuma piemērošanas laikā nosūtīšana no pārziņa vai apstrādātāja Savienībā pārziņiem vai apstrādātājiem Apvienotajā Karalistē var notikt bez nepieciešamības saņemt jebkādu turpmāku atļauju.

(164) Vienlaikus būtu jāatgādina, ka saskaņā ar Direktīvas (ES) 2016/680 47. panta 5. punktu un kā Tiesa paskaidrojusi spriedumā *Schrems* lietā, 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 ([270]).

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

5. ŠĀ LĒMUMA UZRAUDZĪBA, APTURĒŠANA, ATCELŠANA VAI GROZĪŠANA

(165) Saskaņā ar Direktīvas (ES) 2016/680 36. panta 4. punktu Komisijai pēc šā lēmuma pieņemšanas pastāvīgi jāuzrauga attiecīgās norises Apvienotajā Karalistē, lai novērtētu, vai tā joprojām nodrošina pēc būtības līdzvērtīgu aizsardzības līmeni. Šāda uzraudzība šajā gadījumā ir īpaši svarīga, jo Apvienotā Karaliste pārvaldīs, piemēros un īstenos jaunu datu aizsardzības režīmu, uz kuru vairs neattiecas Savienības tiesību akti un kurš varētu attīstīties. Šajā saistībā īpaša uzmanība tiks pievērsta tam, kā Apvienotās Karalistes noteikumi par personas datu nosūtīšanu uz trešām valstīm tiek piemēroti praksē, tai skaitā noslēdzot starptautiskus nolīgumus, un tam, kā tas varētu ietekmēt saskaņā ar šo lēmumu nosūtīto datu aizsardzības līmeni, kā arī individuālo tiesību īstenošanas efektivitātei jomās, uz ko attiecas šis lēmums. Komisija, īstenojot uzraudzību, cita starpā ņems vērā jaunāko judikatūru un IKB un citu neatkarīgu struktūru veikto pārraudzību.

(166) Lai sekmētu šo uzraudzību, Apvienotās Karalistes iestādēm būtu bez kavēšanās un regulāri jāinformē Komisija par visām būtiskajām Apvienotās Karalistes tiesību sistēmas izmaiņām, kas ietekmē tiesisko regulējumu, uz kuru attiecas šis lēmums, kā arī par šajā lēmumā novērtētās personas datu apstrādes prakses maiņu, it īpaši aspektos, kas minēti 165. apsvērumā.

(167) 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 Eiropas Savienības Apvienotās Karalistes kompetentajām iestādēm. 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.

(168) Ja pieejamā informācija, jo īpaši informācija, kas iegūta, uzraugot šo lēmumu, vai informācija, ko sniedz Apvienotās Karalistes vai dalībvalstu iestādes, atklāj, ka Apvienotās Karalistes nodrošinātais aizsardzības līmenis, iespējams, vairs nav pietiekams, Komisijai par to būtu nekavējoties jāinformē Apvienotās Karalistes kompetentās iestādes un jāpieprasa, lai noteiktā termiņā, kas nav garāks par trim mēnešiem, tiktu veikti attiecīgi pasākumi. Nepieciešamības gadījumā minēto termiņu var pagarināt par noteiktu laiku, ņemot vērā attiecīgās problēmas un/vai veicamo pasākumu būtību.

(169) 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 Direktīvas (ES) 2016/680 58. panta 2. punktā minēto procedūru, lai daļēji vai pilnībā apturētu vai atceltu šo lēmumu.

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

(171) Pienācīgi pamatotu, nenovēršamu steidzamu iemeslu dēļ Komisija izmantos iespēju saskaņā ar Direktīvas (ES) 2016/680 58. panta 3. punktā minēto procedūru pieņemt nekavējoties piemērojamus īstenošanas aktus, ar kuriem aptur, atceļ vai groza lēmumu.

6. ŠĀ LĒMUMA DARBĪBAS TERMIŅŠ UN ATJAUNOŠANA

(172) Būtu jāņem vērā, ka, beidzoties Izstāšanās līgumā paredzētajam pārejas periodam, tiklīdz vairs nepiemēros ES un Apvienotās Karalistes Tirdzniecības un sadarbības nolīguma 782. pantā paredzēto pagaidu noteikumu, Apvienotā Karaliste pārvaldīs, piemēros un īstenos jaunu datu aizsardzības regulējumu, kas atšķiras no tā, kurš bija spēkā, kad tai bija saistoši Eiropas Savienības tiesību akti. Tas jo īpaši var ietvert grozījumus vai izmaiņas šajā lēmumā vērtētajā datu aizsardzības regulējumā, kā arī citas attiecīgas norises.

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

(174) 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 Direktīvas (ES) 2016/680 58. panta 2. punktā minēto procedūru.

7. **NOSLĒGUMA APSVĒRUMI**

(175) Eiropas Datu aizsardzības kolēģija ir publiskojusi savu atzinumu ([271]), un tas tika ņemts vērā, sagatavojot šo lēmumu.

(176) Šajā lēmumā paredzētie pasākumi ir saskaņā ar atzinumu, ko sniegusi komiteja, kura izveidota ar Direktīvas (ES) 2016/680 58. pantu.

(177) Saskaņā ar 6.a pantu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots LES un LESD, Īrijai nav saistoši Direktīvā (ES) 2016/680 un līdz ar to šajā īstenošanas lēmumā paredzētie noteikumi, kuri saistīti ar personas datu apstrādi, ko veic dalībvalstis, īstenojot darbības, uz kurām attiecas LESD trešās daļas V sadaļas 4. vai 5. nodaļas darbības joma, tad, ja Īrijai nav saistoši noteikumi, ar ko reglamentē tādus tiesu sadarbības veidus krimināllietās vai tādus policijas iestāžu sadarbības veidus, kuros ir jāievēro noteikumi, kas paredzēti, pamatojoties uz LESD 16. pantu. Turklāt saskaņā ar Padomes Īstenošanas lēmumu (ES) 2020/1745 ([272]) Direktīva (ES) 2016/680 stājas spēkā un to provizoriski piemēro Īrijā no 2021. gada 1. janvāra. Tādēļ Īrijai šis īstenošanas lēmums ir saistošs saskaņā ar tādiem pašiem nosacījumiem, kādi attiecas uz Direktīvas (ES) 2016/680 piemērošanu Īrijā, kā minēts Īstenošanas lēmumā (ES) 2020/1745 par Šengenas *acquis*, kurā tā piedalās.

(178) Saskaņā ar 2. un 2.a pantu 22. protokolā par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānijai nav saistoši Direktīvas (ES) 2016/680 noteikumi un līdz ar to arī šis īstenošanas lēmums, kā arī tā piemērošana saistībā ar personas datu apstrādi dalībvalstīs, kad tās veic darbības, uz kurām attiecas LESD trešās daļas V sadaļas 4. vai 5. nodaļa. Tomēr, tā kā Direktīva (ES) 2016/680 ir balstīta uz Šengenas *acquis*, Dānija saskaņā ar minētā protokola 4. pantu 2016. gada 26. oktobrī paziņoja par tās lēmumu īstenot Direktīvu (ES) 2016/680. Tādējādi saskaņā ar starptautiskajām tiesībām Dānijai šā īstenošanas lēmuma īstenošana ir saistoša.

(179) Attiecībā uz Norvēģiju un Islandi ar šo īstenošanas lēmumu pilnveido Šengenas *acquis* noteikumus, kā paredzēts nolīgumā, kas noslēgts starp Eiropas Savienības Padomi, Islandes Republiku un Norvēģijas Karalisti par abu valstu asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā ([273]).

(180) Attiecībā uz Šveici ar šo īstenošanas lēmumu pilnveido Šengenas *acquis* noteikumus, kā paredzēts Nolīgumā starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā ([274]).

(181) Attiecībā uz Lihtenšteinu – ar Protokolu starp Eiropas Savienību, Eiropas Kopienu, Šveices Konfederāciju un Lihtenšteinas Firstisti par Lihtenšteinas Firstistes pievienošanos Nolīgumam starp Eiropas Savienību, Eiropas Kopienu un Šveices Konfederāciju par Šveices Konfederācijas asociēšanu Šengenas *acquis* īstenošanā, piemērošanā un pilnveidošanā šis īstenošanas lēmums ir Šengenas *acquis* noteikumu pilnveidojums ([275]),

([271]) *Opinion 15/2021 regarding the European Commission draft implementing decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom*, pieejams vietnē https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_lv.

([272]) Padomes Īstenošanas lēmumu (ES) 2020/1745 (2020. gada 18. novembris) par Šengenas acquis noteikumu par datu aizsardzību īstenošanu un dažu Šengenas *acquis* noteikumu provizorisku īstenošanu Īrijā (OV L 393, 23.11.2020., 3. lpp.).

([273]) OV L 176, 10.7.1999., 36. lpp.

([274]) OV L 53, 27.2.2008., 52. lpp.

([275]) OV L 160, 18.6.2011., 21. lpp.

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Apvienotā Karaliste Direktīvas (ES) 2016/680 36. panta mērķiem nodrošina pietiekamu aizsardzības līmeni tādiem personas datiem, ko no Eiropas Savienības nosūta Apvienotās Karalistes publiskajām iestādēm, kuras atbild par to, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus.

2. pants

Ikreiz, kad kompetentās uzraudzības iestādes dalībvalstīs nolūkā aizsargāt personas attiecībā uz viņu personas datu apstrādi īsteno savas pilnvaras atbilstoši Direktīvas (ES) 2016/680 47. pantam attiecībā uz datu nosūtīšanu Apvienotās Karalistes publiskajām iestādēm 1. pantā noteiktajā piemērošanas jomā, attiecīgā dalībvalsts nekavējoties informē Komisiju.

3. pants

1. Komisija nepārtraukti uzrauga to, kā tiek piemērots tiesiskais regulējums, kas ir šā lēmuma pamatā, tai skaitā nosacījumi, ar kādiem tiek veikta datu tālāka nosūtīšana un tiek īstenotas individuālās tiesības, lai novērtētu, vai Apvienotā Karaliste turpina nodrošināt pietiekamu aizsardzības līmeni 1. panta nozīmē.

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

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

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

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

4. pants

Šis lēmums zaudē spēku 2025. gada 27. jūnijā, ja vien tā termiņš netiek pagarināts saskaņā ar Direktīvas (ES) 2016/680 58. panta 2. punktā minēto procedūru.

5. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē, 2021. gada 28. jūnijā

Komisijas vārdā –
Komisijas loceklis
Didier REYNDERS