

II

(Muud kui seadusandlikud aktid)

OTSUSED

KOMISJONI RAKENDUSMÄÄRUS (EL) 2021/1772,

28. juuni 2021,

mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete piisavat kaitset Ühendkuningriigis

(teatavaks tehtud numbri C(2021) 4800 all)

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrust (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus), ⁽¹⁾ eelkõige selle artikli 45 lõiget 3,

ning arvestades järgmist:

1. SISSEJUHATUS

- (1) Määrusega (EL) 2016/679 on kehtestatud õigusnormid, mis reguleerivad isikuandmete edastamist Euroopa Liidus asuvatelt vastutavatele või volitatud töötajatele kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele sel määral, mil see edastamine kuulub määruse kohaldamisalasse. Andmete rahvusvahelise edastamise normid on sätestatud määruse V peatüki artiklites 44–50. Kuigi isikuandmete liikumine Euroopa Liidust väljaspool asuvasse riiki ja neist riikidest on vajalik rahvusvahelise koostöö ja piiriülese kaubanduse laiendamiseks, ei tohi nende edastamine kolmandatele riikidele kahjustada Euroopa Liidus isikuandmetele pakutava kaitse taset ⁽²⁾.
- (2) Määruse (EL) 2016/679 artikli 45 lõike 3 alusel võib komisjon võtta rakendusaktiga vastu otsuse, et kolmas riik või kolmanda riigi territoorium või kolmanda riigi üks või mitu kindlaksmääratud sektorit või rahvusvaheline organisatsioon tagab isikuandmete kaitse piisava taseme. Kui see tingimus on täidetud, võib isikuandmeid edastada kolmandasse riiki ilma täiendava loata, nagu on sätestatud kõnealuse määruse artikli 45 lõikes 1 ja põhjenduses 103.
- (3) Nagu on täpsustatud määruse (EL) 2016/679 artikli 45 lõikes 2, tuleb kaitse piisavuse otsuse vastuvõtmisel tugineda kolmanda riigi õiguskorra põhjalikule analüüsile, mis hõlmab nii andmete importijate suhtes kohaldatavaid õigusnorme kui ka piiranguid ja kaitsemeetmeid, mis puudutavad avaliku sektori asutuste juurdepääsu isikuandmetele. Komisjon peab oma hinnangus kindlaks määrama, kas kõnealune kolmas riik tagab kaitsetaseme, mis „sisuliselt vastab“ Euroopa Liidus tagatud kaitsetasemele (määruse (EL) 2016/679 põhjendus 104). Nõuded, mille põhjal „sisulist vastavust“ hinnatakse, on kehtestatud Euroopa Liidu õiguses, täpsemalt määruses (EL) 2016/679, ning Euroopa Liidu Kohtu praktikas ⁽³⁾. Sellega seoses on oluline ka Euroopa Andmekaitsekoostöö kaitse piisavuse viitedokument ⁽⁴⁾.

⁽¹⁾ ELT L 119, 4.5.2016, lk 1.

⁽²⁾ Vt määruse (EL) 2016/679 põhjendus 101.

⁽³⁾ Vt kõige hiljutisem otsus kohtuasjas C-311/18: Facebook Ireland ja Schrems (edaspidi „kohtuotsus Schrems II“), ECLI:EU:C:2020:559.

⁽⁴⁾ Euroopa Andmekaitsekoostöö kaitse piisavuse viitedokument, WP 254 rev. 01, kättesaadav aadressil https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

- (4) Nagu on selgitanud Euroopa Liidu Kohus, ei eelda see järeldust identse kaitsetaseme kohta ⁽⁵⁾. Eelkõige võivad vahendid, mida asjaomane kolmas riik isikuandmete kaitseks kasutab, erineda nendest, mida rakendatakse Euroopa Liidus, kui need osutuvad praktikas piisava kaitsetaseme tagamisel tulemuslikuks ⁽⁶⁾. Piisavuse nõue ei eelda seega liidu õigusnormide punkthaaval kordamist. Küsimus on pigem selles, kas välisriigi süsteem tervikuna tagab andmekaitseõiguste sisu, nende tõhusa rakendamise, järelevalve ja maksmapaneku kaudu nõutava isikuandmete kaitse taseme ⁽⁷⁾.
- (5) Komisjon on hoolikalt analüüsinud Ühendkuningriigi õigust ja tavasid. Komisjon teeb põhjendustes 8–270 esitatud tulemustele tuginedes järelduse, et Ühendkuningriik tagab määruse (EL) 2016/679 raames Euroopa Liidust Ühendkuningriiki edastatud isikuandmete piisava kaitsetaseme.
- (6) See järeldus ei puuduta isikuandmeid, mida edastatakse Ühendkuningriigi sissepääsu kontrolliga seotud eesmärkidel või mis kuuluvad muul moel Ühendkuningriigi andmekaitseseaduse 2. lisa lõike 4 punktiga 1 ette nähtud erandi kohaldamisalasse; selle sättega tehakse erand mõnedest andmesubjekti õigustest sissepääsu tulemusliku kontrolli säilitamiseks („sisserände erand“). Sisserände erandi kehtivus ja tõlgendamine Ühendkuningriigi õiguses ei ole üheselt selge, arvestades Inglismaa ja Walesi apellatsioonikohtu 26. mai 2021. aasta otsust. Kuigi apellatsioonikohus nõustus, et andmesubjekti õigusi võib põhimõtteliselt piirata sissepääsu kontrolliga seotud eesmärkidel, kuna see on „avalike huvide üks olulisi aspekte“, leidis kohus, et sisserände erand oma praegusel kujul on Ühendkuningriigi õigusega vastuolus, kuna seadusandlikus aktis puuduvad konkreetsed sätted, milles oleksid sätestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 23 lõikega 2 ette nähtud kaitsemeetmed ⁽⁸⁾. Seda arvesse võttes tuleks käesoleva otsuse kohaldamisalast välja jätta selliste isikuandmete edastamine liidust Ühendkuningriiki, mille suhtes võidakse kohaldada sisserände erandit ⁽⁹⁾. Kui erand on Ühendkuningriigi õigusega kooskõlla viidud, tuleks seda uuesti hinnata, samuti tuleks uuesti hinnata seda, kas on vaja piirata käesoleva otsuse kohaldamisala.
- (7) Käesolev otsus ei tohiks mõjutada määruse (EL) 2016/679 vahetut kohaldamist Ühendkuningriigis asutatud organisatsioonide suhtes, kui on täidetud selle artiklis 3 sätestatud tingimused kõnealuse määruse territoriaalse kohaldamisala kohta.

2. ISIKUANDMETE TÖÖTLEMISE SUHTES KOHALDATAVAD ÕIGUSNORMID

2.1. Põhiseaduslik raamistik

- (8) Ühendkuningriik on parlamentaarne demokraatia, mille riigipea on konstitutsiooniline monarh. Riigil on suveräänne parlament, mis on ülimuslik kõikide muude valitsusasutuste suhtes, parlamendiliikmetest moodustatud ja parlamendi ees aruandekohustuslik täitevvõim ning sõltumatu kohtusüsteem. Täitevvõimu volitused tulenevad tema suutlikkusest saavutada valitud alamkoja usaldus ja ta vastutab parlamendi mõlema koja ees, mille ülesanne on valitsuse kontrollimine ning seaduste arutamine ja vastuvõtmine.

⁽⁵⁾ Otsus kohtuasjas C-362/14: Schrems (edaspidi „kohtuotsus Schrems I“), ECLI:EU:C:2015:650, punkt 73.

⁽⁶⁾ Kohtuotsus Schrems I, punkt 74.

⁽⁷⁾ Vt komisjoni 10. jaanuari 2017. aasta teatis Euroopa Parlamendile ja nõukogule „Isikuandmete vahetamine ja kaitsmine globaliseerunud maailmas“, COM(2017) 7, punkt 3.1, lk 6–7, kättesaadav aadressil <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52017DC0007&from=ET>.

⁽⁸⁾ Apellatsioonikohus (tsiviilosakond), Open Rights Group vs. Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport, [2021] EWCA Civ 800, punktid 53–56. Apellatsioonikohus tühistas kõrge kohtu otsuse, milles oli erandit varasemalt hinnatud määruse (EL) 2016/679 (eelkõige selle artikli 23) ja Euroopa Liidu põhiõiguste harta valguses ning jõutud järeldusele, et erand on õiguspärane (Open Rights Group & Anor, R (taotlusel) vs. Secretary of State for the Home Department & Anor [2019] EWHC 2562).

⁽⁹⁾ Kui kohaldatavad tingimused on täidetud, võib isikuandmeid edastada Ühendkuningriigi sissepääsu kontrolliga seotud eesmärkidel määruse (EL) 2016/679 artiklites 46–49 sätestatud edastamismehhanismide alusel.

- (9) Ühendkuningriigi parlament on delegeerinud Šotimaa parlamendile, Walesi parlamendile (Senedd Cymru) ja Põhja-Iirimaa assambleele vastutuse õigusloome eest Šotimaa, Walesi ja Põhja-Iirimaa siseasjades, mida Ühendkuningriigi parlament ei ole enda vastutusalasse jätanud. Kuigi andmekaitse on Ühendkuningriigi parlamendi vastutusalasse kuuluv teema, st kogu riigis kehtivad samad õigusaktid, on muud käesoleva otsuse seisukohast asjakohased valdkonnad delegeeritud. Näiteks on Šotimaa ja Põhja-Iirimaa kriminaalõigussüsteemid, sealhulgas politseitegevus delegeeritud vastavalt Šotimaa parlamendi ja Põhja-Iirimaa assamblee vastutusalasse. Ühendkuningriigil ei ole kodifitseeritud põhiseadust väljakujunenud konstitutiivse dokumendi mõttes. Põhiseaduslikud põhimõtted on välja kujunenud aja jooksul ning tuginevad kohtupraktikale ja eelkõige tavale. Kohtud on tunnustanud teatavate õigusaktide, nagu Magna Carta, 1689. aasta õiguste deklaratsiooni (Bill of Rights) ja 1998. aasta inimõiguste seaduse (Human Rights Act 1998) põhiseaduslikku väärtust. Põhiseaduse osana on üksikisikute põhiõigused arenenud üldise õiguse (*common law*), nimetatud õigusaktide ja rahvusvaheliste lepingute, eelkõige Euroopa inimõiguste konventsiooni kaudu, mille Ühendkuningriik ratifitseeris 1951. aastal. 1987. aastal ratifitseeris Ühendkuningriik ka Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (edaspidi „konventsioon nr 108“) (¹⁰).
- (10) 1998. aasta inimõiguste seadusega lisati Euroopa inimõiguste konventsioonis sisalduvad õigused Ühendkuningriigi õigusesse. Inimõiguste seadusega on kõikidele isikutele antud põhiõigused ja -vabadused, mis on sätestatud Euroopa inimõiguste konventsiooni artiklites 2–12 ja 14, konventsiooni protokoll nr 1 artiklites 1, 2 ja 3 ning protokoll nr 13 artiklis 1, loetuna koostoimes selle konventsiooni artiklitega 16, 17 ja 18. Nende hulka kuuluvad õigus era- ja perekonnaelu austamisele (ja selle osana õigus andmekaitsele) ning õigus õiglasele kohtumenetlusele (¹¹). Eelkõige võivad ametivõimud kõnealuse konventsiooni artikli 8 kohaselt sekkuda eraelu puutumatuse õigusesse üksnes kooskõlas seadusega, kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.
- (11) Vastavalt 1998. aasta inimõiguste seadusele peab ametiasutuste tegevus olema kooskõlas konventsioonist tuleneva õigusega (¹²). Peale selle tuleb esmaseid ja teiseid õigusakte tõlgendada ja jõustada viisil, mis on kooskõlas konventsioonist tulenevate õigustega (¹³).

2.2. Ühendkuningriigi andmekaitseraamistik

- (12) Ühendkuningriik astus Euroopa Liidust välja 31. jaanuaril 2020. Suurbritannia ja Põhja-Iiri Ühendkuningriigi Euroopa Liidust ja Euroopa Aatomienergiaühendusest väljaastumise lepingu (¹⁴) kohaselt kohaldati liidu õigust Ühendkuningriigis üleminekuperioodi jooksul kuni 31. detsembrini 2020. Enne väljaastumist ja üleminekuperioodi jooksul koosnes Ühendkuningriigi isikuandmete kaitse õigusraamistik asjaomastest ELi õigusaktidest (eelkõige Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679 ning Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680 (¹⁵)) ja riiklikest õigusaktidest, eelkõige 2018. aasta andmekaitseadusest, (¹⁶) millega nähti ette siseriiklikud normid (kui see oli määrusega (EL) 2016/679 lubatud), täpsustati ja piirati määruse (EL) 2016/679 normide kohaldamist ning võeti üle direktiiv (EL) 2016/680.

(¹⁰) Algselt rakendati konventsiooni nr 108 põhimõtted Ühendkuningriigi õigusesse 1984. aasta andmekaitseadusega, mis asendati 1998. aasta andmekaitseadusega, mis omakorda asendati 2018. aasta andmekaitseadusega (koostoimes Ühendkuningriigi isikuandmete kaitse üldmäärusega). Samuti allkirjastas Ühendkuningriik 2018. aastal protokoll, millega muudetakse isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (mida tuntakse ka konventsioonina nr 108+), ja tegeleb praegu konventsiooni ratifitseerimisega.

(¹¹) Euroopa inimõiguste konventsiooni artiklid 6 ja 8 (vt ka 1998. aasta inimõiguste seaduse 1. lisa).

(¹²) 1998. aasta inimõiguste seaduse paragrahv 6.

(¹³) 1998. aasta inimõiguste seaduse paragrahv 3.

(¹⁴) Suurbritannia ja Põhja-Iiri Ühendkuningriigi Euroopa Liidust ja Euroopa Aatomienergiaühendusest väljaastumise leping, 2019/C 384 I/01, XT/21054/2019/INIT (ELT C 384I, 12.11.2019, lk 1), kättesaadav aadressil [https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12019W/TXT\(02\)&from=ET](https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=ET).

(¹⁵) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutustele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT L 119, 4.5.2016, lk 89), kättesaadav aadressil <https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016L0680&from=ET>.

(¹⁶) 2018. aasta andmekaitseadus (Data Protection Act (DPA) 2018), kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>.

- (13) Euroopa Liidust väljaastumiseks valmistudes kehtestas Ühendkuningriigi valitsus 2018. aasta Euroopa Liidust väljaastumise seaduse, ⁽¹⁷⁾ millega lisatakse Ühendkuningriigi õigusesse vahetult kohaldatavad liidu õigusaktid ⁽¹⁸⁾. Nende nn jätkuvalt kohaldatavate ELi õigusaktide hulka kuulub tervikuna määrus (EL) 2016/679 (sealhulgas selle põhjendused) ⁽¹⁹⁾. Euroopa Liidust väljaastumise seaduse kohaselt peavad Ühendkuningriigi kohtud tõlgendama muutmata kujul jätkuvalt kohaldatavaid ELi õigusakte kooskõlas Euroopa Liidu Kohtu asjaomase kohtupraktika ja liidu õiguse üldpõhimõtetega sel kujul, mil need kehtisid vahetult enne üleminekuperioodi lõppu (mida nimetatakse vastavalt „jätkuvalt kohaldatavaks ELi kohtupraktikaks“ ja „jätkuvalt kohaldatavateks liidu õiguse üldpõhimõteteks“) ⁽²⁰⁾.
- (14) 2018. aasta Euroopa Liidust väljaastumise seaduse alusel on Ühendkuningriigi ministritel õigus kehtestada seadusandlike aktide kaudu teiseid õigusakte, et teha jätkuvalt kohaldatavatesse Euroopa Liidu õigusaktidesse Ühendkuningriigi Euroopa Liidust väljaastumisest tulenevaid vajalikke muudatusi. Seda õigust kasutati, kui vastu võeti 2019. aasta andmekaitset, eraelu puutumatust, elektroonilist sidet, muudatusi jne käsitlev (EList väljaastumise) määrus (edaspidi „andmekaitse, eraelu puutumatuse ja elektroonilise side määrus“) ⁽²¹⁾. Selle määrusega muudeti määrust (EL) 2016/679, kui see lisati Ühendkuningriigi õigusesse 2018. aasta Euroopa Liidust väljaastumise seaduse, 2018. aasta andmekaitse seaduse ja muude andmekaitsealaste õigusaktidega, et viia see vastavusse siseriikliku kontekstiga ⁽²²⁾.
- (15) Sellest tulenevalt koosneb isikuandmete kaitse õigusraamistik Ühendkuningriigis pärast üleminekuperioodi lõppu järgmisest:
- 2018. aasta Euroopa Liidust väljaastumise lepinguga Ühendkuningriigi õigusesse lisatud Ühendkuningriigi isikuandmete kaitse üldmäärus, mida on muudetud andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega, ⁽²³⁾ ja
 - 2018. aasta andmekaitse seadus, ⁽²⁴⁾ mida on muudetud andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega.
- (16) Kuna Ühendkuningriigi isikuandmete kaitse üldmäärus põhineb ELi õigusaktidel, on Ühendkuningriigi andmekaitse normid paljudes aspektides väga sarnased Euroopa Liidus kohaldatavate vastavate normidega.
- (17) Lisaks 2018. aasta Euroopa Liidust väljaastumise seadusega ministrile antud volitustele antakse 2018. aasta andmekaitse seaduse mitme sättega ministrile õigused võtta vastu teiseid õigusakte, et muuta seaduse teatavaid sätteid või kehtestada lisanorme ⁽²⁵⁾. Seni on minister teostanud 2018. aasta andmekaitse seaduse paragrahvi 137

⁽¹⁷⁾ 2018. aasta Euroopa Liidust väljaastumise seadus (European Union (Withdrawal) Act 2018), kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/2018/16/contents>.

⁽¹⁸⁾ 2018. aasta Euroopa Liidust väljaastumise seaduse eesmärk ja mõju on see, et kõik üleminekuperioodi lõpus Ühendkuningriigi õigusesse lisatud otsekohalduvad liidu õigusaktid lisatakse Ühendkuningriigi õigusesse sel kujul, mil need kehtisid ELi õiguses vahetult enne üleminekuperioodi lõppu, vt 2018. aasta Euroopa Liidust väljaastumise seaduse paragrahv 3.

⁽¹⁹⁾ 2018. aasta Euroopa Liidust väljaastumise seaduse selgitavates märkustes on öeldud: „Kui õigusakt muudetakse käesoleva paragrahvi alusel siseriiklikuks õigusaktiks, saab õigusakti tekst osaks siseriiklikust õigusest. See hõlmab ELi õigusakti tervikteksti (sealhulgas selle põhjendusi)“. (2018. aasta Euroopa Liidust väljaastumise seaduse selgitavad märkused, punkt 83, kättesaadavad aadressil https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Kuna põhjendused ei ole siduvad õigusnormid, siis ei olnud Ühendkuningriigi ametiasutuste esitatud teabe kohaselt vajalik neid muuta nii, nagu andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega muudeti määruse (EL) 2016/679 artikleid.

⁽²⁰⁾ 2018. aasta Euroopa Liidust väljaastumise seaduse paragrahv 6.

⁽²¹⁾ 2019. aasta andmekaitset, eraelu puutumatust, elektroonilist sidet, muudatusi jne käsitlev (EList väljaastumise) määrus (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019), kättesaadav aadressil <https://www.legislation.gov.uk/uksi/2019/419/contents/made> (muudetud 2020. aasta andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega, kättesaadav aadressil <https://www.legislation.gov.uk/ukdsi/2020/9780348213522>).

⁽²²⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitse seaduse muudatused on peamiselt tehnilist laadi, näiteks on välja jäetud viited „liikmesriikidele“ või kohandatud terminoloogiat, näiteks asendades viited määrusele (EL) 2016/679 viidetega Ühendkuningriigi isikuandmete kaitse üldmäärusele. Mõnel juhul olid muudatused vajalikud selleks, et kajastada sätete puhtsiseriiklikku konteksti, näiteks seoses sellega, kes Ühendkuningriigi andmekaitse õigusraamistikus kaitse piisavuse määra vastu võtab (vt 2018. aasta andmekaitse seaduse paragrahv 17A), st minister, mitte Euroopa Komisjon.

⁽²³⁾ Isikuandmete kaitse üldmäärus, Keelingi lisa, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-_MASTER_Keeling_Schedule_with_changes_highlighted_V3.pdf.

⁽²⁴⁾ 2018. aasta andmekaitse seadus, Keelingi lisa, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-_MASTER_Keeling_Schedule_with_changes_highlighted_V3.pdf.

⁽²⁵⁾ Need õigused sisalduvad näiteks 2018. aasta andmekaitse seaduse paragrahvis 16 (õigus teha teatavates kitsalt piiritletud olukordades täiendavaid erandeid Ühendkuningriigi isikuandmete kaitse üldmääruse konkreetsetest sätetest), paragrahvis 17A (õigus võtta vastu kaitse piisavuse määra), paragrahvides 212 ja 213 (õigus algatada õigusaktide koostamist ja kehtestada üleminekusätteid) ning paragrahvis 211 (õigus teha väikeseid ja tulenevaid muudatusi).

kohaseid volitusi ainult selleks, et võtta vastu 2019. aasta andmekaitsemäärus (tasud ja teave, muudatus), milles on sätestatud asjaolud, mille korral peavad vastutavad töötajad maksma Ühendkuningriigi sõltumatule andmekaitseasutusele (teabevolinikule) iga-aastast tasu.

- (18) Samuti on täiendavaid juhiseid Ühendkuningriigi andmekaitsealaste õigusaktide kohta esitatud tegevusjuhendites ja muudes teabevoliniku vastuvõetud juhistes. Kuigi need juhised ei ole ametlikult õiguslikult siduvad, on neil kaal tõlgendamisel ja need näitavad, kuidas andmekaitsealaseid õigusakte kohaldatakse ja volinik nende täitmise praktikas tagab. Eelkõige on 2018. aasta andmekaitseaduse paragrahvidega 121–125 ette nähtud, et volinik koostab tegevusjuhendid andmete jagamise, otseturunduse, eakohase kujunduse ning andmekaitse ja ajakirjanduse kohta.
- (19) Seega on käesoleva otsuse alusel edastatavate andmete suhtes kohaldatav Ühendkuningriigi õigusraamistik oma ülesehituse ja põhielementide poolest väga sarnane Euroopa Liidus kohaldatavale õigusraamistikule. Seda ka seetõttu, et kõnealune raamistik ei tugine mitte üksnes siseriiklikus õiguses sätestatud kohustustele, mida on kujundanud ELi õigus, vaid ka rahvusvahelises õiguses kehtestatud kohustustele, eelkõige kuna Ühendkuningriik järgib Euroopa inimõiguste konventsiooni ja konventsiooni nr 108 ning kuulub Euroopa Inimõiguste Kohtu kohtualluvusse. Seega on need õiguslikult siduvatest rahvusvahelistest õigusaktidest tulenevad kohustused, eelkõige isikuandmete kaitsmine, käesolevas otsuses hinnatava õigusraamistiku eriti oluline element.

2.3. Sisuline ja territoriaalne kohaldamisala

- (20) Sarnaselt määrusele (EL) 2016/679 kohaldatakse Ühendkuningriigi isikuandmete kaitse üldmäärust isikuandmete täielikult või osaliselt automatiseeritud töötlemise suhtes või muu töötlemise suhtes, kui isikuandmed kuuluvad andmete kogumisse ⁽²⁶⁾. Ühendkuningriigi isikuandmete kaitse üldmääruses kasutatud mõisted „isikuandmed“, „andmesubjekt“ ja „töötlemine“ on identsed määruses (EL) 2016/679 kasutatud mõistetega ⁽²⁷⁾. Peale selle kohaldatakse Ühendkuningriigi isikuandmete kaitse üldmäärust teatavate Ühendkuningriigi ametiasutuste ⁽²⁸⁾ valduses olevate isikuandmete struktureerimata käsitsi töötlemise ⁽²⁹⁾ suhtes, kuigi 2018. aasta andmekaitseaduse paragrahvide 24 ja 25 alusel jäetakse kohaldamata need Ühendkuningriigi isikuandmete kaitse üldmääruse kohased põhimõtted ja õigused, mis ei ole selliste isikuandmete puhul asjakohased. Sarnaselt määruses (EL) 2016/679 sätestatule ei kohaldata Ühendkuningriigi isikuandmete kaitse üldmäärust juhul, kui isikuandmeid töötleb üksikisik eranditult isikliku või koduse tegevuse käigus ⁽³⁰⁾.
- (21) Ühendkuningriigi isikuandmete kaitse üldmäärusega on laiendatud määruse kohaldamisala ka andmete töötlemisele sellise tegevuse käigus, mis vahetult enne üleminekuperioodi lõppu jäi väljapoole Euroopa Liidu õigust (nt riigi julgeolek) ⁽³¹⁾ või jäi Euroopa Liidu lepingu V jaotise 2. peatüki (ühise välis- ja julgeolekupoliitika alane tegevus) kohaldamisalasse ⁽³²⁾. Sarnaselt Euroopa Liidu süsteemile ei kohaldata ka Ühendkuningriigi isikuandmete kaitse üldmäärust juhul, kui isikuandmeid töötlevad pädevad asutused süütegude ennetamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil (nn õiguskaitse eesmärgid) – selline töötlemine on

⁽²⁶⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 2 lõiked 1 ja 5.

⁽²⁷⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 4 lõige 1 ja artikkel 2.

⁽²⁸⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 2 lõikega 1A on ette nähtud, et määrust kohaldatakse ka teabevabaduse seaduses määratletud avaliku sektori asutuse valduses olevate isikuandmete struktureerimata käsitsi töötlemise suhtes. Viide teabevabaduse seaduses määratletud avaliku sektori asutustele hõlmab kõiki 2000. aasta teabevabaduse seaduses määratletud avaliku sektori asutusi ja kõiki 2002. aasta teabevabaduse seaduses (Šotimaa) (Šotimaa parlamendi seadus nr 13) määratletud Šotimaa avaliku sektori asutusi. 2018. aasta andmekaitseaduse paragrahvi 21 lõige 5.

⁽²⁹⁾ Artikli 2 lõike 5 punktis b on isikuandmete struktureerimata käsitsi töötlemine määratletud kui selline isikuandmete töötlemine, mis ei ole isikuandmete automatiseeritud või struktureeritud töötlemine.

⁽³⁰⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 2 lõike 2 punkt a.

⁽³¹⁾ Riigi julgeolekuga seotud tegevus kuulub Ühendkuningriigi isikuandmete kaitse üldmääruse kohaldamisalasse üksnes siis, kui seda ei vii ellu pädev asutus õiguskaitse eesmärkidel, millisel juhul kohaldatakse 2018. aasta andmekaitseaduse 3. osa, ega luureteenistuse poolt või nimel; luureteenistuste tegevus on Ühendkuningriigi isikuandmete kaitse üldmääruse kohaldamisalast välja jäetud ja reguleeritud selle määruse artikli 2 lõike 2 punkti c kohaselt 2018. aasta andmekaitseaduse 4. osaga. Näiteks võib politsei viia läbi töötaja turvakontrolli eesmärgiga tagada, et ta on usaldusväärne ja talle võib anda juurdepääsu riigi julgeolekut käsitlevale materjalile. Kuigi politsei on õiguskaitse seisukohast pädev asutus, siis ei toimu andmete töötlemine sel juhul õiguskaitse eesmärkidel ja kohaldatakse Ühendkuningriigi isikuandmete kaitse määrust. Vt „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu H: „National Security Data Protection and Investigatory Powers Framework“ (Riigi julgeolekuga seotud andmekaitse ja uurimisvolituste raamistik), lk 8, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf.

⁽³²⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 2 lõike 1 punktid a ja b.

reguleeritud 2018. aasta andmekaitseseaduse 3. osaga, nagu on Euroopa Liidu õiguse alusel reguleeritud direktiiviga (EL) 2016/680 –, ega juhul, kui isikuandmeid töötlevad luureteenistused (julgeolekuteenistus (Security Service), salaluureteenistus (Secret Intelligence Service) ja valitsusside peakorter (Government Communications Headquarters)), mida on käsitletud 2018. aasta andmekaitseseaduse 4. osas ⁽³³⁾.

- (22) Ühendkuningriigi isikuandmete kaitse üldmääruse territoriaalne kohaldamisala ⁽³⁴⁾ on määratletud üldmääruse artiklis 3 ja sellesse kuuluvad isikuandmete töötlemine (olenemata selle toimumise asukohast) Ühendkuningriigis asuva vastutava töötleja või volitatud töötleja tegevuskoha tegevuse kontekstis ning Ühendkuningriigis asuvate andmesubjektide isikuandmete töötlemine, kui töötlemine on seotud nende andmesubjektidele kaupade või teenuste pakkumise või nende andmesubjektide käitumise jälgimisega ⁽³⁵⁾. See vastab määruse (EL) 2016/679 artikli 3 lähenemisviisile.

2.4. Isikuandmete ning vastutava töötleja ja volitatud töötleja mõistete määratlused

- (23) Määruses (EL) 2016/679 sätestatud isikuandmete, töötlemise, vastutava töötleja, volitatud töötleja ning pseudonümeerimise määratlused on säilitatud Ühendkuningriigi isikuandmete kaitse üldmääruses ilma sisuliste muudatusteta ⁽³⁶⁾. Peale selle on Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 1 määratletud isikuandmete eriliigid samamoodi kui määruses (EL) 2016/679 („isikuandmed, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine, geneetilised andmed, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta“). 2018. aasta andmekaitseseaduse paragrahvis 205 on esitatud biomeetriliste andmete, ⁽³⁷⁾ terviseandmete ⁽³⁸⁾ ja geneetiliste andmete ⁽³⁹⁾ mõisted.

2.5. Kaitsemeetmed, õigused ja kohustused

2.5.1. Töötlemise seaduslikkus ja õiglus

- (24) Isikuandmeid tuleb töödelda seaduslikult ja õiglaselt.
- (25) Ühendkuningriigi õiguses on seaduslikkuse, õigluse ja läbipaistvuse põhimõtted ning seadusliku töötlemise alused tagatud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktiga a ja artikli 6 lõikega 1, mis on identsed määruse (EL) 2016/679 vastavate sätetega ⁽⁴⁰⁾. 2018. aasta andmekaitseseaduse paragrahviga 8 on täiendatud artikli 6 lõike 1 punkti e sättega, millega on ette nähtud, et isikuandmete töötlemine Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti e alusel (töötlemine on vajalik avalikes huvides oleva

⁽³³⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 2 lõike 2 punktid b ja c.

⁽³⁴⁾ Sama territoriaalne kohaldamisala kehtib isikuandmete töötlemise suhtes Ühendkuningriigi isikuandmete kaitse üldmäärust täiendava 2018. aasta andmekaitseseaduse 2. osa alusel (paragrahvi 207 lõige 1A).

⁽³⁵⁾ See tähendab eeskätt seda, et 2018. aasta andmekaitseseadust ja sellest tulenevalt ka käesolevat otsust ei kohaldata Briti krooni sõltkondade (Jersey, Guernsey ja Mani saar) ning Ühendkuningriigi ülemereterritooriumide, nagu näiteks Falklandi saarte ja Gibraltari territooriumi suhtes.

⁽³⁶⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 4 lõiked 1, 2, 5, 7 ja 8.

⁽³⁷⁾ „Biomeetrilised andmed“ – konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust isikut kordumatult tuvastada või kinnitavad selle isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed.

⁽³⁸⁾ „Terviseandmed“ – isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas talle tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema tervisliku seisundi kohta.

⁽³⁹⁾ „Geneetilised andmed“ – isikuandmed, mis on seotud isiku päritud või omandatud geneetiliste omadustega, mis annavad ainulaadset teavet isiku füsioloogia ja tervise kohta ning mis tulenevad eelkõige asjaomase isiku bioloogilise proovi analüüsist saadud isikuandmetest.

⁽⁴⁰⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 6 lõike 1 kohaselt on töötlemine seaduslik üksnes juhul kui ja sel määral, mil a) andmesubjekt on andnud nõusoleku oma isikuandmete töötlemiseks ühel või mitmel konkreetsel eesmärgil; b) isikuandmete töötlemine on vajalik andmesubjekti osalusel sõlmitud lepingu täitmiseks või lepingu sõlmimisele eelnevate meetmete võtmiseks vastavalt andmesubjekti taotlusele; c) isikuandmete töötlemine on vajalik vastutava töötleja seadusjärgse kohustuse täitmiseks; d) isikuandmete töötlemine on vajalik andmesubjekti või mõne muu füüsilise isiku eluliste huvide kaitsmiseks; e) isikuandmete töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks või f) isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, välja arvatud juhul, kui sellise huvi kaaluvad üles andmesubjekti huvid või põhiõigused ja -vabadused, mille nimel tuleb kaitsta isikuandmeid, eriti juhul kui andmesubjekt on laps.

ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks) hõlmab isikuandmete töötlemist, mis on vajalik õigusemõistmiseks, parlamendi kummagi koja ülesande täitmiseks, seaduse või õigusnormiga isikule antud ülesande täitmiseks või riigi, ministri või ministeeriumi ülesande täitmiseks või tegevuseks, millega toetatakse või edendatakse demokraatlikku kaasatust.

- (26) Samuti on Ühendkuningriigi isikuandmete kaitse üldmääruses muutmata kujul säilitatud nõusoleku (mis on üks seadusliku töötlemise alus) kohta määruse (EL) 2016/679 artiklis 7 sätestatud tingimused, see tähendab, et vastutav töötleja peab suutma tõendada, et andmesubjekt on andnud nõusoleku, nõusoleku saamiseks kirjaliku taotluse esitamisel tuleb kasutada selget ja lihtsat keelt, andmesubjekt peab olema õigus nõusolek igal ajal tagasi võtta ning selle hindamisel, kas nõusolek on antud vabatahtlikult, tuleb võtta arvesse asjaolu, kas lepingu täitmise tingimuseks on nõusolek isikuandmete töötlemiseks, mis ei ole vajalik kõnealuse lepingu täitmiseks. Peale selle on Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 8 kohaselt lapse nõusolek infoühiskonna teenuste pakkumise kontekstis seaduslik üksnes siis, kui laps on vähemalt 13-aastane. See jääb määruse (EL) 2016/679 artikliga 8 kehtestatud vanusevahemikku.

2.5.2. Isikuandmete eriliikide töötlemine

- (27) Andmete eriliikide töötlemisel tuleks kohaldada konkreetseid kaitsemeetmeid.
- (28) Ühendkuningriigi isikuandmete kaitse üldmäärus ja 2018. aasta andmekaitseseadus sisaldavad erinorme isikuandmete eriliikide töötlemise kohta, mis on määratletud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 1 samamoodi kui määruses (EL) 2016/679 (vt põhjendus 23). Vastavalt Ühendkuningriigi isikuandmete kaitse üldmääruse artiklile 9 on andmete eriliikide töötlemine põhimõtteliselt keelatud, välja arvatud juhul, kui kohaldatakse konkreetset erandit.
- (29) Need erandid (mis on loetletud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõigetes 2 ja 3) ei erine sisuliselt määruse (EL) 2016/679 artikli 9 lõigetes 2 ja 3 sätestatud eranditest. Kui andmesubjekt ei ole andnud isikuandmete eriliikide töötlemiseks sõnaselget nõusolekut, siis on nende isikuandmete töötlemine lubatud ainult konkreetsetel ja piiratud asjaoludel. Enamikul juhtudel peab tundlike andmete töötlemine olema vajalik konkreettsel eesmärgil, mis on määratletud asjaomases sättes (vt artikli 9 lõike 2 punktid b, c, f, g, h, i ja j).
- (30) Kui Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 2 on nõutud seadusjärgset luba või viidatud avalikule huvile, siis 2018. aasta andmekaitseseaduse paragrahvis 10 on koos selle seaduse 1. lisaga täiendavalt täpsustatud tingimused, mis peavad olema erandi kasutamiseks täidetud. Näiteks kui tundlike andmeid töödeldakse rahvatervise kaitsmise eesmärgil (Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt i), siis 1. lisa 1. osa lõike 3 punktiga b on ette nähtud, et lisaks vajalikkuse hindamisele peab andmeid „töötleva või selle eest vastutava tervishoiutöötaja“ või peab neid „töötleva teine isik, kellel lasub konfidentsiaalsuskohustus seaduse või õigusnormi alusel“, sealhulgas üldise õiguse kohaselt väljakujunenud konfidentsiaalsuskohustus.
- (31) Seoses tundlike andmete töötlemisega olulise avaliku huviga seotud põhjustel (Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt g) on 2018. aasta andmekaitseseaduse 1. lisa 2. osas esitatud täielik loetelu eesmärkidest, mida võib käsitada olulise avaliku huvina, ning sätestatud iga eesmärgi kohta täiendavad eritingimused. Näiteks tunnistatakse olulise avaliku huvina rassilise ja etnilise mitmekesisuse edendamist organisatsioonide kõrgemate ametnike tasandil. Tundlike andmete töötlemise suhtes sellel konkreettsel eesmärgil kehtivad üksikasjalikud nõuded, muu hulgas peab töötlemine toimuma osana kõrgemale ametikohale värvatavate sobilike isikute kindlakstegemise protsessist ning olema vajalik rassilise ja etnilise mitmekesisuse edendamiseks ja ei tohi olla tõenäoline, et see tekitab andmesubjektile olulist kahju või kannatusi.
- (32) 2018. aasta andmekaitseseaduse paragrahvi 11 lõikes 1 on sätestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 3 kirjeldatud asjaoludel toimuva isikuandmete töötlemise tingimused seoses saladuse hoidmise kohustusega. Need hõlmavad asjaolusid, mille korral andmeid töötleb või selle eest vastutab tervishoiu- või sotsiaaltöötaja või neid töötleb teine isik, kellel lasub konfidentsiaalsuskohustus seaduse või õigusnormi alusel.
- (33) Lisaks tuleb paljude Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 2 loetletud erandite korral kasutada sobilikke ja konkreetseid kaitsemeetmeid. Sõltuvalt töötlemise laadist ning andmesubjekti õigustele ja vabadustele kaasneva ohu tasemest on 2018. aasta andmekaitseseaduse 1. lisa sisalduvate töötlemistingimustega kehtestatud mitmesugused kaitsemeetmed. 1. lisa on eraldi sätestatud tingimused iga töötlemisolukorra kohta.

- (34) Mõnel juhul on 2018. aasta andmekaitseseadusega reguleeritud ja piiratud tundlike andmete liike, mida tohib töödelda vastavalt konkreetsele õiguslikule alusele, mida tuleb järgida. Näiteks on 1. lisa lõikega 8 lubatud tundlike andmete töötlemine võrdsete võimaluste ja võrdse kohtlemise edendamiseks. Sellele töötlemistingimusele saab tugineda üksnes juhul, kui andmed näitavad rassilist või etnilist päritolu, usulisi või filosoofilisi veendumusi või seksuaalset sättumust või kui tegemist on terviseandmetega.
- (35) Mõnel juhul on 2018. aasta andmekaitseseaduses kehtestatud piirang selle kohta, mis liiki vastutav töötleja tohib töötlemistingimust kasutada. Näiteks on 1. lisa lõikega 23 ette nähtud tundlike andmete töötlemine seoses valitud esindajate vastustega avalikkusele. Sellele töötlemistingimusele võib tugineda ainult juhul, kui vastutav töötleja on valitud esindaja või tegutseb tema nimel.
- (36) Teistel juhtudel on 2018. aasta andmekaitseseadusega kehtestatud piirangud selliste andmesubjektide liikide kohta, kelle puhul võib töötlemistingimusele tugineda. Näiteks on 1. lisa lõikega 21 reguleeritud tundlike andmete töötlemine tööandjapensioni skeemide jaoks. Sellele tingimusele võib tugineda üksnes juhul, kui asjaomane andmesubjekt on skeemiga liitunud isiku vend või õde, vanem, vanavanem või vanavanavanem.
- (37) Peale selle peab vastutav töötleja Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 2 sätestatud ning 2018. aasta andmekaitseseaduse paragrahvis 10 ja 1. lisa täiendavalt täpsustatud eranditele tuginedes enamikul juhtudel koostama asjakohaseid tegevuspõhimõtteid käsitleva dokumendi. Selles tuleb kirjeldada vastutava töötleja menetlusi, millega tagatakse Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 5 kehtestatud põhimõtete järgimine. Ühtlasi tuleb selles esitada andmete säilitamise ja kustutamise põhimõtted ning märkida nende tõenäoline säilitamisaeg. Vastutavad töötlejad peavad seda dokumenti vastavalt vajadusele läbi vaatama ja ajakohastama. Vastutav töötleja peab tegevuspõhimõtteid käsitlevat dokumenti säilitama kuus kuud pärast töötlemise lõpuleviimist ja tegema selle taotluse korral kättesaadavaks teabevinikule ⁽⁴¹⁾.
- (38) 2018. aasta andmekaitseseaduse 1. lisa lõike 41 kohaselt tuleb tegevuspõhimõtteid käsitlevale dokumendile alati lisada andmete töötlemise põhjalikum kirjeldus. Kirjeldada tuleb tegevuspõhimõtteid käsitlevas dokumendis sisalduvate kohustuste täitmist, st kas andmed kustutatakse või säilitatakse kooskõlas tegevuspõhimõtetega. Kui tegevuspõhimõtteid ei ole järgitud, siis tuleb dokumenteerida selle põhjused. Kirjeldada tuleb ka töötlemise vastavust Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 6 (töötlemise seaduslikkus) nõuetele ning märkida, millisele 2018. aasta andmekaitseseaduse 1. lisa nimetatud konkreetsele tingimusele tuginetakse.
- (39) Samuti on Ühendkuningriigi isikuandmete kaitse üldmääruses sarnaselt määrusele (EL) 2016/679 sätestatud üldised kaitsemeetmed seoses andmete eriliikide teatavate töötlemistoimingutega. Ühendkuningriigi isikuandmete kaitse üldmääruse artikliga 35 on ette nähtud, et andmete eriliikide ulatusliku töötlemise korral tuleb koostada andmekaitsealane mõjuhindang. Kui vastutava töötleja või volitatud töötleja põhitegevuseks on andmete eriliikide ulatuslik töötlemine, peab ta Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 37 kohaselt määrama andmekaitseametniku.
- (40) Mis puudutab süüteoasjades süüdimõistvaid kohtuotsuseid ja süütegudega seotud isikuandmeid, siis on Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 10 identne määruse (EL) 2016/679 artikliga 10. Selle artikli järgi on süüteoasjades süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmeid lubatud töödelda üksnes ametiasutuste järelevalve all või siis, kui töötlemine on lubatud siseriikliku õigusega, milles on sätestatud asjakohased kaitsemeetmed andmesubjektide õiguste ja vabaduste kaitseks.
- (41) 2018. aasta andmekaitseseaduse paragrahvis 10 lõikes 5 on sätestatud, et kui süütegudes süüdimõistvate kohtuotsuste ja süütegudega seotud isikuandmeid ei töödelda ametiasutuse järelevalve all, siis võib selline töötlemine toimuda ainult konkreetsetel eesmärkidel / konkreetsetes olukordades, mis on sätestatud 2018. aasta andmekaitseseaduse 1. lisa 1., 2. ja 3. osas, ja selle suhtes kehtivad iga nimetatud eesmärgi/olukorra kohta kehtestatud erinõuded. Näiteks võib mittetulundusühing töödelda süütegudes süüdimõistvate kohtuotsustega seotud andmeid juhul, kui a) töötlemine toimub poliitilise, filosoofilise, religioosse või ametiühingulise suunitlusega sihtasutuse, ühenduse või muu mittetulundusühenduse õiguspärase tegevuse raames, mille suhtes kehtivad asjakohased kaitsemeetmed, ja b) tingimusel, et i) töötlemine käsitleb ainult asjaomase ühenduse liikmeid või endisi liikmeid või isikuid, kes on kõnealuse ühendusega püsivalt seotud tema tegevuse eesmärkide tõttu, ning ii) isikuandmeid ei avalikustata väljaspool seda ühendust ilma andmesubjekti nõusolekuta.

⁽⁴¹⁾ 2018. aasta andmekaitseseaduse 1. lisa lõiked 38–40.

- (42) Peale selle on 2018. aasta andmekaitseseaduse 1. lisa 3. osas sätestatud täiendavad asjaolud, mille korral võib kasutada süüdimõistvate kohtuotsustega seotud andmeid ja mis vastavad määruse (EL) 2016/679 ja Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 2 kehtestatud tundlike andmete töötlemise õiguslikele alustele (nt andmesubjekti nõusolek, isiku elulised huvid, kui andmesubjekt on füüsiliselt või õiguslikult võimetu nõusolekut andma, töötlemine on vajalik õigusnõude koostamiseks, esitamiseks või kaitsmiseks jne).

2.5.3. Eesmärgi piirang, õigus, võimalikult väheste andmete kogumine, säilitamise piirang ja andmete turvalisus

- (43) Isikuandmeid tuleks töödelda konkreetsel eesmärgil ja kasutada seejärel üksnes määral, mil see on kooskõlas töötlemise eesmärgiga.
- (44) See põhimõte on ette nähtud määruse (EL) 2016/679 artikli 5 lõike 1 punktiga b, mis on muutmata kujul säilitatud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktis b. Ka määruse (EL) 2016/679 artikli 6 lõikes 4 sätestatud nõuetele vastava töötlemise lisatingimused on sisuliste muutusteta säilitatud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 6 lõike 4 punktides a–e.
- (45) Peale selle peavad isikuandmed olema õiged ja vajaduse korral ajakohastatud. Samuti peavad need olema piisavad ja asjakohased, ei tohi olla nende töötlemise eesmärgi seisukohast ülemääraseks ning põhimõtteliselt ei tohi neid säilitada kauem, kui on isikuandmete töötlemise eesmärgil vajalik.
- (46) Võimalikult väheste andmete kogumise, õigsuse ja säilitamise piirangu põhimõtted on sätestatud määruse (EL) 2016/679 artikli 5 lõike 1 punktides c–e ning säilitatud muutmata kujul Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktides c–e.
- (47) Ühtlasi tuleks isikuandmeid töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsiminek, hävimise või kahjustumise eest. Sel eesmärgil peaksid ettevõtjad võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleks hinnata, võttes arvesse tehnika taset ja seonduvaid kulusid.
- (48) Ühendkuningriigi õiguses on andmete turvalisus tagatud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 5 lõike 1 punktis f sätestatud usaldusväärsuse ja konfidentsiaalsuse põhimõtte kaudu ning töötlemise turvalisust käsitlevas artiklis 32. Need sätted on identsed määruse (EL) 2016/679 vastavate sätetega. Peale selle on Ühendkuningriigi isikuandmete kaitse üldmäärusega ette nähtud, et isikuandmetega seotud rikkumisest tuleb teavitada järelevalveasutust (artikkel 33) ja andmesubjekti (artikkel 34) samadel tingimustel kui need, mis on kehtestatud määruse (EL) 2016/679 artiklites 33 ja 34.

2.5.4. Läbipaistvus

- (49) Andmesubjekte tuleks teavitada nende isikuandmete töötlemise põhitunnustest.
- (50) See on tagatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklitega 13 ja 14, millega on lisaks läbipaistvuse üldpõhimõttele ette nähtud andmesubjektile esitatavat teavet käsitlevad normid⁽⁴²⁾. Määruse (EL) 2016/679 vastavate artiklitega võrreldes ei ole Ühendkuningriigi isikuandmete kaitse üldmäärusega nendes normides sisulisi muudatusi tehtud. Nii nagu määruse (EL) 2016/679 alusel kehtib aga ka nimetatud artiklites esitatud läbipaistvusnõude puhul mitu 2018. aasta andmekaitseseaduses sätestatud erandit (vt põhjendused 55–72).

⁽⁴²⁾ Artikli 13 lõike 1 punktis f ja artikli 14 lõike 1 punktis f esitatud viited kaitse piisavust käsitlevatele komisjoni otsustele on asendatud viidetega Ühendkuningriigi samaväärsetele õigusaktidele, st 2018. aasta andmekaitseseaduse kohastele kaitse piisavuse määrustele. Peale selle on artikli 14 lõike 5 punktides c–d esitatud viited liidu või liikmesriigi õigusele asendatud viidetega siseriiklikule õigusele (näidetena sellisest siseriiklikust õigusest, mis võib kuuluda artikli 14 lõike 5 punkti c kohaldamisalasse, on Ühendkuningriik nimetanud 2013. aasta vanametalliga kauplemise seaduse paragrahvi 7, milles on sätestatud vanametallilitsentside registreerimise eeskirjad, või 2006. aasta äriühingute seaduse 35. osa, milles on sätestatud äriregistri pidaja tegevuse eeskirjad). Samamoodi võib artikli 14 lõike 5 punkti d kohaldamisalasse jääv siseriiklik õigus hõlmata näiteks õigusakte, milles on sätestatud ametisadalust reguleerivad normid, või töölepingutes sisalduvaid kohustusi või üldise õiguse kohast konfidentsiaalsuskohustust (näiteks seoses tervishoiu-, personali-, sotsiaaltöötajate ja teiste isikute töödeldavate isikuandmetega).

2.5.5. Üksikisiku õigused

- (51) Andmesubjektidel peaksid olema teatavad õigused, mida nad saavad maksma panna vastutava töötleja või volitatud töötleja suhtes, eeskätt õigus andmetega tutvuda, õigus töötlemine vaidlustada ning õigus lasta andmeid parandada ja kustutada. Samal ajal võivad selliste õiguste suhtes kehtida piirangud, kui need on avaliku julgeoleku kaitsmiseks või muul olulisel üldise avaliku huvi eesmärgil vajalikud ja proportsionaalsed.

2.5.5.1. Sisulised õigused

- (52) Ühendkuningriigi isikuandmete kaitse üldmäärusega on üksikisikutele antud samad kohtulikult kaitstavad õigused kui määrusega (EL) 2016/679. Sätted, millega on ette nähtud üksikisikute õigused, on sisuliste muudatusteta säilitatud Ühendkuningriigi isikuandmete kaitse üldmääruses.
- (53) Nende õiguste hulka kuuluvad andmesubjekti õigus andmetega tutvuda (Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 15), õigus andmete parandamisele (artikkel 16), õigus andmete kustutamisele (artikkel 17), õigus isikuandmete töötlemise piiramisele (artikkel 18), kohustus teatada isikuandmete parandamisest, kustutamisest või isikuandmete töötlemise piiramisest (artikkel 19), andmete ülekandmise õigus (artikkel 20) ja õigus esitada vastuväiteid (artikkel 21) ⁽⁴³⁾. Viimane sisaldab ka andmesubjekti õigust esitada vastuväide isikuandmete töötlemisele otseturunduse eesmärgil, mis on sätestatud määruse (EL) 2016/679 artikli 21 lõigetes 2 ja 3. Peale selle peab teabevinik koostama 2018. aasta andmekaitseaduse paragrahvi 122 alusel tegevusjuhendi otseturundamiseks kooskõlas andmekaitsealaste õigusaktide (ning 2003. aasta eraelu puutumatust ja elektroonilist sidet (elektroonilise side direktiivi) käsitleva määruse (Privacy and Electronic Communications (EC Directive) Regulations 2003)) nõuetega ning muud otseturunduses hea tava edendamise suunised, mida volinik asjakohaseks peab. Teabeviniku büroo koostab praegu otseturundust käsitlevat juhendit ⁽⁴⁴⁾.
- (54) Isikuandmete kaitse üldmääruse artiklis 22 sätestatud andmesubjekti õigus, et tema kohta ei võetaks vastu otsust, mis põhineb üksnes automatiseeritud töötlusel ja toob kaasa teda puudutavaid õiguslikke tagajärgi või avaldab talle märkimisväärset mõju, on samuti säilitatud ilma sisuliste muudatusteta Ühendkuningriigi isikuandmete kaitse üldmääruses. Lisatud on aga uus lõige 3A, milles viidatakse, et 2018. aasta andmekaitseaduse paragrahvis 14 on sätestatud meetmed andmesubjektide õiguste, vabaduste ja õigustatud huvide kaitsmiseks juhul, kui andmete töötlemine toimub Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 22 lõike 2 punkti b alusel. Seda kohaldatakse üksnes juhul, kui sellise otsuse näol on tegemist Ühendkuningriigi õiguse kohase loa või nõudega, mitte juhul, kui otsus on vajalik lepingu alusel või andmesubjekt on andnud selle tegemiseks sõnaselge nõusoleku. Kui kohaldatakse 2018. aasta andmekaitseaduse paragrahvi 14, siis peab vastutav töötleja niipea, kui on mõistlikult teostatav, teavitama andmesubjekti kirjalikult sellest, et tehtud on üksnes automatiseeritud töötlusel põhinev otsus. Andmesubjektil on õigus taotleda, et vastutav töötleja kaaluks otsust ühe kuu jooksul alates teate saamisest uuesti või teeks uue otsuse, mis ei põhine üksnes automatiseeritud töötlusel. Ministril on õigus võtta vastu täiendavaid kaitsemeetmeid seoses automatiseeritud otsuste tegemisega. Seda õigust ei ole seni veel kasutatud.

2.5.5.2. Üksikisiku õiguste piirangud ja muud sätted

- (55) 2018. aasta andmekaitseaduses on sätestatud mitu üksikisiku õiguste piirangut, mis jäävad Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 23 raamistikku. Selles raamistikus ei kehtestata mingeid piiranguid seoses Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 21 lõigetes 2 ja 3 sätestatud õigusega esitada vastuväiteid otseturunduse suhtes ega artiklis 22 sätestatud õigusega, et isiku kohta ei võeta vastu otsust, mis põhineb üksnes automatiseeritud töötlusel.
- (56) Neid piiranguid on üksikasjalikult kirjeldatud 2018. aasta andmekaitseaduse 2.–4. lisas. Ühendkuningriigi ametiasutused on selgitanud, et nad lähtuvad kahest põhimõttest: spetsiifilisuse põhimõte (mille puhul järgitakse detailset lähenemisviisi, jagades laiad piirangud mitmeks konkreetsemaks sätteks) ja tingimuslikkuse põhimõte (iga sätet täiendatakse piirangute või tingimuste vormis kaitsemeetmetega, et vältida kuritarvitamist) ⁽⁴⁵⁾.

⁽⁴³⁾ Artikli 17 lõike 1 punktis e ja lõike 3 punktis b esitatud viited ELi või liikmesriigi õigusele on asendatud viidetega siseriiklikule õigusele (näidetena sellisest siseriiklikust õigusest, mis võib kuuluda artikli 17 lõike 1 punkti e kohaldamisalasse, on Ühendkuningriik nimetanud 2006. aasta haridusmäärust (õpilaste andmed) (Inglismaa), millega nõutakse õpilaste nimede kustutamist koolide registrist pärast nende koolist lahkumist, või 1983. aasta meditsiiniaduse paragrahvi 34F, milles on sätestatud normid nimede kustutamise kohta perearstide ja eriarstide registritest).

⁽⁴⁴⁾ Juhendi kavand on esitatud aadressil <https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf>.

⁽⁴⁵⁾ „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu E „Restrictions“ (Piirangud), lk 1, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

- (57) Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 23 lõikes 1 kirjeldatud piirangud on kavandatud eesmärgiga tagada nende kohaldamine üksnes kindlaksmääratud asjaoludel, kui see on demokraatlikus ühiskonnas vajalik ja proportsionaalne nende õiguspärase eesmärgiga. Peale selle saab andmekaitsekorra erandeid kooskõlas piirangute tõlgendamise valdkonnas välja kujunenud kohtupraktikaga kohaldada konkreetse juhtumi puhul üksnes siis, kui see on vajalik ja proportsionaalne ⁽⁴⁶⁾. Vajalikkust tuleb hinnata „rangelt ning sekkumine andmesubjekti õigustesse peab olema proportsionaalne avalikule huvile avalduva ohu raskusastmega. Seepärast hõlmab see klassikalist proportsionaalsuse analüüsi ⁽⁴⁷⁾.“
- (58) Nende piirangute eesmärgid vastavad määruse (EL) 2016/679 artiklis 23 loetletud eesmärkidele, välja arvatud riigi julgeoleku ja riigikaitsega seotud eesmärgid, mis on reguleeritud 2018. aasta andmekaitseseaduse paragrahviga 26, kuid mille suhtes kehtivad samad vajalikkuse ja proportsionaalsuse nõuded (vt põhjendused 63–66).
- (59) Teatavad piirangud, näiteks kuriteo ennetamise või avastamisega, õigusrikkujate kinnipidamise või vastutusele võtmisega ning maksude või tollimaksude hindamise või kogumisega seotud piirangud ⁽⁴⁸⁾ võimaldavad piirata kõiki üksikisiku õigusi ja läbipaistvuskohustusi (välja arvatud artikli 21 lõike 2 ja artikli 22 kohased õigused). Muude piirangute kohaldamisalasse kuuluvad läbipaistvuskohustus ja juurdepääsuõiguse, näiteks kutsesaladust käsitlevad piirangud, ⁽⁴⁹⁾ õigus vabastusele nõudest esitada teavet, mille tulemuseks on enda süüstamine, ⁽⁵⁰⁾ ja ärirahandus, eeskätt siseteabe alusel kauplemise ennetamine ⁽⁵¹⁾. Üksikute piirangutega lubatakse piirata vastutava töötleja kohustust teavitada andmesubjekti andmetega seotud rikkumistest ja eesmärgi piirangu ning töötlemise seaduslikkuse, õigluse ja läbipaistvuse põhimõtteid ⁽⁵²⁾.
- (60) Mõni neist piiranguist kehtib teatavat liiki isikuandmete töötlemise suhtes automaatselt ja täielikult (näiteks ei kohaldata läbipaistvuskohustust ja üksikisiku õigusi juhul, kui isikuandmeid töödeldakse eesmärgiga hinnata isiku sobivust kohtunikuametisse nimetamiseks või kui isikuandmeid töötleb kohus või õigust mõistvat funktsiooni täitev isik).
- (61) Enamikul juhtudel on 2018. aasta andmekaitseseaduse 2. lisa asjaomases punktis aga täpsustatud, et piirangut kohaldatakse üksnes juhul, kui (ja sel määral, mil) sätete kohaldamine „tõenäoliselt kahjustaks“ piirangu õiguspärasest eesmärgi: näiteks ei kohaldata Ühendkuningriigi isikuandmete kaitse üldmääruses loetletud sätteid isikuandmete suhtes, mida töödeldakse kuriteo ennetamise või avastamise, õigusrikkujate kinnipidamise või vastutusele võtmise ning maksude või tollimaksude hindamise või kogumise eesmärgil „sel määral, mil nende sätete kohaldamine tõenäoliselt kahjustaks“ asjaomaseid eesmärke ⁽⁵³⁾.
- (62) Ühendkuningriigi kohtud on tõenäolise kahjustamise kriteeriumit järjekindlalt tõlgendanud kui „väga suurt ja kaalukat võimalust kahjustada kindlakstehtud avalikku huvi“ ⁽⁵⁴⁾. Sellist piirangut, mille suhtes kehtib tõenäolise kahjustamise nõue, saab kohaldada üksnes juhul kui ja sellises ulatuses, milles on olemas väga suur ja kaalukas võimalus, et teatava õiguse teostamine kahjustaks kõnealust avalikku huvi. Vastutav töötleja peab iga juhtumi puhul eraldi hindama, kas need tingimused on täidetud ⁽⁵⁵⁾.
- (63) Lisaks 2018. aasta andmekaitseseaduse 2. lisa esitatud piirangutele on 2018. aasta andmekaitseseaduse paragrahvis 26 kehtestatud erand, mida võib kohaldada Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseseaduse teatavate sätete suhtes, kui nimetatud erand on vajalik riigi julgeoleku kaitsmiseks või riigikaitse eesmärgil. Seda erandit kohaldatakse andmekaitsepõhimõtete (v.a seaduslikkuse põhimõtte), läbipaistvuskohustuste, andmesubjekti õiguste, andmetega seotud rikkumistest teatamise, andmete rahvusvahelise edastamise eeskirjade, teabevolniku teatavate kohustuste ja õiguste ning õiguskaitsevahendeid,

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

⁽⁴⁷⁾ Guriev vs. Community Safety Development (United Kingdom) Ltd, [2016], EWHC 643 (QB), punkt 43. Vt selle kohta ka Lin vs. Commissioner of Police for the Metropolis, [2015], EWHC 2484 (QB), punkt 80.

⁽⁴⁸⁾ 2018. aasta andmekaitseseaduse 2. lisa lõige 2.

⁽⁴⁹⁾ 2018. aasta andmekaitseseaduse 2. lisa lõige 19.

⁽⁵⁰⁾ 2018. aasta andmekaitseseaduse 2. lisa lõige 20.

⁽⁵¹⁾ 2018. aasta andmekaitseseaduse 2. lisa lõige 21.

⁽⁵²⁾ Näiteks on lubatud õigust andmetega seotud rikkumistest teavitamisele piirata üksnes seoses kuritegude ja maksustamise (2018. aasta andmekaitseseaduse 2. lisa lõige 2), parlamentaarse puutumatuse (2. lisa lõige 13) ning ajakirjanduslikul, akadeemilisel, kunstilisel või kirjanduslikel eesmärkidel töötlemisega (2. lisa lõige 26).

⁽⁵³⁾ 2018. aasta andmekaitseseaduse 2. lisa lõige 2.

⁽⁵⁴⁾ R (Lord) vs. siseminister, [2003], EWHC 2073 (Admin), punkt 100, ja Guriev vs. Community Safety Development (United Kingdom) Ltd, [2016], EWHC 643 (QB), punkt 43.

⁽⁵⁵⁾ Open Rights Group & Anor, R (On the Application Of) vs. Secretary of State for the Home Department & Anor, punkt 31.

vastutust ja karistusi käsitlevate õigusnormide suhtes, välja arvatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 83 kehtestatud trahvide määramise üldtingimusi käsitleva sätte ja artiklis 84 kehtestatud karistusi käsitleva sätte suhtes. Peale selle on 2018. aasta andmekaitseaduse paragrahviga 28 muudetud artikli 9 lõike 1 kohaldamist, et võimaldada Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 9 lõikes 1 sätestatud isikuandmete eriliikide töötlemist sel määral, mil töötlemine toimub riigi julgeoleku kaitsmiseks või riigikaitse eesmärkidel, ning kui on kehtestatud asjakohased meetmed andmesubjektide õiguste ja vabaduste kaitsmiseks ⁽⁵⁶⁾.

- (64) Erandit võib kohaldada ainult sel määral, mil see on vajalik riigi julgeoleku kaitsmiseks või riigikaitse eesmärgil. Nagu ka muude 2018. aasta andmekaitseaduses sätestatud erandite puhul, peab vastutav töötleja erandit kaaluma ja sellele tuginema iga juhtumi puhul eraldi. Peale selle peab erandi kohaldamine olema kooskõlas inimõiguste normidega (mis on sätestatud 1998. aasta inimõiguste seaduses), mille kohaselt peab igasugune sekkumine eraelu puutumatuse õigustesse olema demokraatlikus ühiskonnas vajalik ja proportsionaalne ⁽⁵⁷⁾.
- (65) Erandi sellist tõlgendamist on kinnitanud teabevinik, kes on andnud välja põhjalikud suunised riigi julgeoleku ja riigikaitse erandi kohaldamise kohta, kusjuures suunistes on selgelt kirjas, et vastutav töötleja peab erandit kaaluma ja kohaldama iga juhtumi puhul eraldi ⁽⁵⁸⁾. Eeskätt on suunistes rõhutatud, et „tegu ei ole üldise erandiga“ ning et sellele tuginemiseks „ei piisa sellest, kui andmeid töödeldakse riigi julgeolekuga seotud eesmärgil“. Vastupidi, vastutav töötleja, kes sellele erandile tugineb, peab „tõendama, et on olemas tegelik võimalus, et riigi julgeolekut kahjustatakse“, ning vajaduse korral peab vastutav töötleja „esitama [teabevinikule] tõendid selle kohta, miks ta seda erandit kasutas“. Suunistes on esitatud kontrollnimekiri ja hulk näiteid, et selgitada, millistel tingimustel saab seda erandit kohaldada.
- (66) Asjaolu, et andmeid töödeldakse riigi julgeoleku või riigikaitse eesmärkidel, ei ole seega iseenesest erandi kohaldamiseks piisav. Vastutav töötleja peab kaaluma tegelikke tagajärgi riigi julgeolekule juhul, kui ta peab teatavat andmekaitseaset järgima. Erandit võib kohaldada ainult nende konkreetsete sätete suhtes, mille puhul on kindlaks tehtud, et nende kohaldamine kujutaks endast ohtu riigi julgeolekule, ning erandit tuleb kohaldada võimalikult kitsalt ⁽⁵⁹⁾.
- (67) Seda lähenemisviisi on kinnitanud teabeküsimuste kohus ⁽⁶⁰⁾. Kohtuotsuses *Baker vs. Secretary of State for the Home Department* leidis teabeküsimuste kohus, et ebaseaduslik on kohaldada riigi julgeoleku erandit üldise erandina luureteenistuste saadud juurdepääsutaotluste suhtes. Selle asemel tuleb erandit kohaldada iga juhtumi puhul eraldi, hinnates iga päringu sisu ja võttes arvesse üksikisikute õigust nende eraelu austamisele ⁽⁶¹⁾.

⁽⁵⁶⁾ Ühendkuningriigi ametiasutuste esitatud teabe põhjal kohaldavad vastutavad töötledjad juhul, kui andmeid töödeldakse riigi julgeoleku kontekstis, töötlemise suhtes tõhustatud kaitse- ja turbemeetmeid, mis annavad tunnistust sellest, et tegu on tundliku tegevusega. See, millised kaitsemeetmed on asjakohased, sõltub konkreetse andmetöötlustoiminguga kaasnevatest ohtudest. Kaitsemeetmeteks võivad olla andmetele juurdepääsu piiramine, nii et nendega saavad tutvuda ainult asjakohase juurdepääsuloaga volitatud isikud, ranged piirangud andmete jagamisele ning salvestamis- ja menetlemistoimingute suhtes kohaldatavad ranged turbestandardid.

⁽⁵⁷⁾ Vt ka *Guriev vs. Community Safety Development (United Kingdom) Ltd*, [2016], EWHC 643 (QB), punkt 45; *Lin vs. Commissioner of the Police for the Metropolis*, [2015], EWHC 2484 (QB), punkt 80.

⁽⁵⁸⁾ Vt teabeviniku suunised riigi julgeoleku ja riigikaitse erandi kohta, kättesaadavad aadressil <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/>

⁽⁵⁹⁾ Ühendkuningriigi ametiasutuste esitatud näite kohaselt on juhul, kui terrorismis kahtlustatav isik, keda MI5 aktiivselt uurib, esitab siseministeeriumile juurdepääsutaotluse (näiteks kuna tal on siseministeeriumiga vaidlus sisserändega seotud küsimustes), vaja kaitsta andmesubjektile avalikustamise eest pooleliolevaid uurimisi käsitlevaid andmeid, mida MI5 võib olla siseministeeriumiga jaganud ning mis võivad kahjustada tundlikke allikaid, meetodeid või tehnikaid ja/või mille tulemusel võib suurendada oht, mida isik kujutab. Sellistel asjaoludel on tõenäoline, et paragrahvi 26 kohase erandi kohaldamise künnis on täidetud ja riigi julgeoleku kaitsmiseks on vaja kasutada teabe avaldamise erandit. Kui aga siseministeeriumil on isiku kohta ka selliseid isikuandmeid, mis ei ole seotud MI5 uurimisega, ja selle teabe esitamine ei ohusta riigi julgeolekut, siis ei ole riigi julgeoleku erand isikule teabe avaldamise kaalumisel kohaldatav. Teabevinik valmistas praegu ette suuniseid selle kohta, millist lähenemisviisi peaksid vastutavad töötledjad paragrahvi 26 kohase erandi kasutamisel järgima. Eelduste kohaselt avaldatakse suunised 2021. aasta märtsi lõpuks.

⁽⁶⁰⁾ Teabeküsimuste kohus (Information Tribunal) asutati 1984. aasta andmekaitseaduse alusel, selleks et lahendada kaebusi andmekaitseasjades. 2010. aastal sai teabeküsimuste kohtust Ühendkuningriigi erikohtute süsteemi struktuuri reformimise käigus osa esimese astme kohtu (First-tier Tribunal) halduskollegiumist.

⁽⁶¹⁾ Vt kohtuotsus *Baker vs. Secretary of State for the Home Department*, [2001], UKIT NSA2.

2.5.6. Piirangud seoses ajakirjanduslikul, kunstilisel, akadeemilisel ja kirjanduslikul eesmärgil ning arhiveerimise ja uuringute eesmärgil töödeldavate isikuandmetega

- (68) Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 85 lõikega 2 lubatakse teha ajakirjanduslikul, kunstilisel, akadeemilisel ja kirjanduslikul eesmärgil töödeldavate isikuandmete suhtes erand mitmest Ühendkuningriigi isikuandmete kaitse üldmääruse sättest. 2018. aasta andmekaitseseaduse 2. lisa 5. osas on sätestatud erandid nimetatud eesmärkidel toimuva töötlemise korral. Sellega on ette nähtud erandid andmekaitse põhimõtetest (välja arvatud usaldusväärsuse ja konfidentsiaalsuse põhimõte), töötlemise õiguslikest alustest (sealhulgas andmete eriliigid, süüteoasjades süüdimõistvaid kohtuotsuseid jne käsitlevad andmed), nõusoleku andmise tingimustest, läbipaistvuskohustustest, andmesubjektide õigustest, kohustusest teavitada andmetega seotud rikkumistest ning nõudest konsulteerida enne kõrge riskitasemega töötlemist teabevolnikuga ning andmete rahvusvahelise edastamise eeskirjadest⁽⁶²⁾. Sellega seoses ei erine Ühendkuningriigi isikuandmete kaitse üldmäärus sisuliselt määrusest (EL) 2016/679, mille artikliga 85 on samuti ette nähtud võimalus teha andmete ajakirjanduslikul eesmärgil või akadeemilise, kunstilise või kirjandusliku eneseväljenduse eesmärgil töötlemise puhul erand mitmest määruse (EL) 2016/679 nõudest. 2018. aasta andmekaitseseaduse sätteid, eelkõige 2. lisa 5. osa, on Ühendkuningriigi isikuandmete kaitse üldmäärusega vastavuses.
- (69) Tasakaalu hindamine Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 85 alusel on põhiliselt seotud sellega, kas erandid põhjenduses 68 nimetatud andmekaitse normidest on „vajalikud, et ühitada õigus isikuandmete kaitsele sõna- ja teabevabadusega“⁽⁶³⁾. Vastavalt 2018. aasta andmekaitseseaduse 2. lisa lõike 26 punktidele 2 ja 3 hindab Ühendkuningriik selle tasakaalu saavutamisel seda, kas arvamuseks on „mõistlik alus“. Selleks et erand oleks põhjendatud, peab vastutaval töötlejal olema mõistlik alus arvata, et i) avaldamine on avalikes huvides ja ii) isikuandmete kaitse üldmääruse asjakohase sätte kohaldamine ei oleks kooskõlas ajakirjanduslike, akadeemiliste, kunstiliste või kirjanduslike eesmärkidega. Nagu kinnitab kohtupraktika,⁽⁶⁴⁾ on arvamuse mõistliku aluse hindamisel nii subjektiivne kui ka objektiivne element: ei piisa sellest, kui vastutav töötleja tõendab, et tema enda arvamuse kohaselt ei oleks sätte järgimine eesmärkidega kooskõlas. Tema arvamusel peab olema mõistlik alus, see tähendab, et niimoodi võiks arvata mõistlik isik, kes teab asjaomaseid fakte. Seepärast peab vastutav töötleja täitma oma arvamuse kujundamisel hoolsuskohustust, et ta suudaks tõendada selle mõistlikku alust. Ühendkuningriigi ametiasutuste esitatud selgituste kohaselt tuleb „arvamuse mõistlikku alust“ hinnata iga erandi puhul eraldi⁽⁶⁵⁾. Kui tingimused on täidetud, loetakse erand Ühendkuningriigi õiguse alusel vajalikuks ja proportsionaalseks.
- (70) Kooskõlas 2018. aasta andmekaitseseaduse paragrahviga 124 peab teabevolnik koostama andmekaitset ja ajakirjandust käsitleva tegevusjuhendi. Juhendi koostamine on pooleli. 1998. aasta andmekaitseseaduse alusel on välja antud seda küsimust käsitlevad suunised, milles on eelkõige rõhutatud, et erandile tuginemiseks ei piisa üksnes väitest, et sätte järgimine oleks ajakirjandusliku tegevuse seisukohast ebamugav, vaid esitada tuleb

⁽⁶²⁾ Vt Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 85 ning 2018. aasta andmekaitseseaduse 2. lisa 5. osa lõike 26 punkt 9.

⁽⁶³⁾ Kooskõlas 2018. aasta andmekaitseseaduse 2. lisa 5. osa lõike 26 punktiga 2 kohaldatakse erandit isikuandmete erieesmärkidel (ajakirjanduslikel, akadeemilistel, kunstilistel ja kirjanduslikel eesmärkidel) töötlemise suhtes, kui töötlemise eesmärk on see, et isik avaldab ajakirjanduslikku, akadeemilist, kunstilist või kirjanduslikku materjali ning kui vastutaval töötlejal on mõistlik alus arvata, et selle materjali avaldamine oleks avalikes huvides. Selle otsustamisel, kas avaldamine oleks avalikes huvides, peab vastutav töötleja arvestama sõna- ja teabevabadusega seotud avaliku huvi erilist tähtsust. Peale selle peab vastutav töötleja võtma arvesse kõnealuse avaldamise puhul asjakohaseid tegevusjuhendeid või suuniseid (BBC toimetamissuunised, Ofcomi ringhäälingukodeks ja toimetajate tegevusjuhend). Lisaks peab vastutaval töötlejal olema erandi kohaldamiseks mõistlik alus arvata, et asjaomase sätte järgimine ei oleks kooskõlas erieesmärkidega (2018. aasta andmekaitseseaduse 2. lisa lõike 26 punkt 3).

⁽⁶⁴⁾ Kohtuotsuse NTI vs. Google, [2018], EWHC 799 (QB) punktis 102 käsitleti seda, kas vastutaval töötlejal oli mõistlik alus arvata, et avaldamine oli avalikes huvides ja et asjaomaste sätete järgimine ei olnud kooskõlas erieesmärkidega. Kohus leidis, et 1998. aasta andmekaitseseaduse paragrahvi 32 lõike 1 punktidel b ja c on subjektiivne ja objektiivne element: vastutav töötleja peab tõendama, et tema arvamuse kohaselt oleks avaldamine avalikes huvides ja et see arvamus on objektiivselt mõistlik, ning ta peab tõendama subjektiivset arvamust, et selle sätte järgimine, millest ta erandit taotleb, ei oleks kooskõlas asjaomase erieesmärgiga.

⁽⁶⁵⁾ Näide arvamuse mõistliku aluse hindamise kohta on esitatud teabevolniku 1998. aasta andmekaitseseaduse alusel tehtud otsuses määrata trahv äriühingule True Visions Productions. Teabevolnik nõustus, et meediaettevõtjast vastutaval töötlejal oli subjektiivne arvamus, mille kohaselt andmekaitse esimene põhimõte (õigus ja seaduslikkus) ei olnud kooskõlas ajakirjanduslike eesmärkidega. Teabevolnik ei nõustunud aga sellega, et see arvamus oli objektiivselt mõistlik. Teabevolniku otsus on kättesaadav aadressil <https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf>.

selge argument, mille kohaselt kõnealune säte takistab vastutustundlikku ajakirjandustegevust ⁽⁶⁶⁾. Samuti on Ühendkuningriigi telekommunikatsioonivaldkonna reguleeriv asutus OFCOM ja BBC oma toimetamissuunistes avaldanud juhised avaliku huvi hindamise ning avaliku huvi ja üksikisiku eraelu puutumatusega seotud huvi tasakaalustamise kohta ⁽⁶⁷⁾. Eelkõige on suunistes esitatud näiteid teabest, mida võib seoses avaliku huviga arvesse võtta, ja selgitatud vajadust tõendada, et juhtumi konkreetsetel asjaoludel kaalub avalik huvi üles eraelu puutumatuse õiguse.

- (71) Sarnaselt isikuandmete kaitse üldmääruse artiklis 89 sätestatule võib avalikes huvides toimuva arhiveerimise eesmärgil ning teadus- ja ajaloouringute või statistilisel eesmärgil toimuva isikuandmete töötlemise suhtes teha erandi ka mitmest Ühendkuningriigi isikuandmete kaitse üldmääruses loetletud sättest ⁽⁶⁸⁾. Uuringute ja statistika puhul on võimalik teha erand Ühendkuningriigi isikuandmete kaitse üldmääruse sätetest, mis on seotud andmete töötlemise kinnitamisega, andmetele juurdepääsemisega ja kaitsemeetmetega kolmandatesse riikidesse edastamisega, õigusega andmete parandamisele, töötlemise piiramisega ja töötlemisele vastuväite esitamisega. Seoses avalikes huvides toimuva arhiveerimisega on võimalikud ka erandid kohustusest teatada isikuandmete parandamisest või kustutamisest või töötlemise piiramisest ning erandid andmete ülekandmise õigusest.
- (72) 2018. aasta andmekaitseseaduse 2. lisa lõike 27 punkti 1 ja lõike 28 punkti 1 kohaselt on erandid Ühendkuningriigi isikuandmete kaitse üldmääruses loetletud sätetest võimalikud juhul, kui sätte kohaldamine „takistaks või tõsiselt kahjustaks“ asjaomase eesmärgi saavutamist ⁽⁶⁹⁾.
- (73) Arvestades seda, kuidas need erandid mõjutavad konkreetsete õiguste tulemuslikku teostamist, võetakse kõiki nimetatud erandite tõlgendamise ja praktikas kohaldamisega seotud olulisi arengusuundi (lisaks sisserände tulemusliku kontrolli säilitamise erandile, nagu on selgitatud põhjenduses 6), kaasa arvatud arenguid kohtupraktikas ning teabevolniku suunistes ja täitemeetmetes, nõuetekohaselt arvesse käesoleva otsuse üle pideva järelevalve teostamisel ⁽⁷⁰⁾.

2.5.7. Andmete edasisaatmise piirangud

- (74) Euroopa Liidust Ühendkuningriigis asuvatele vastutavatele töötlejatele või volitatud töötlejatele edastatavatele isikuandmetele pakutava kaitse taset ei tohi kahjustada selliste andmete täiendav edasisaatmine kolmandasse riiki. Andmete edasisaatmine, mis tähendab Ühendkuningriigi vastutava töötleja või volitatud töötleja seisukohast rahvusvahelist edastamist Ühendkuningriigist, peaks olema lubatud üksnes juhul, kui väljaspool Ühendkuningriiki asuva järgmise saaja enda suhtes kehtivad eeskirjad, millega tagatakse sarnane kaitsetase, nagu on tagatud Ühendkuningriigi õiguskorraga. Sel põhjusel on Ühendkuningriigi isikuandmete kaitse üldmääruses ja 2018. aasta andmekaitseseaduses isikuandmete rahvusvahelise edastamise kohta sätestatud normide kohaldamine oluline tegur jätkuva kaitse tagamiseks käesoleva otsuse alusel isikuandmete Euroopa Liidust Ühendkuningriiki edastamise korral.

⁽⁶⁶⁾ Suuniste kohaselt peavad organisatsioonid suutma selgitada, miks ei ole 1998. aasta andmekaitseseaduse asjaomaste sätete järgimine kooskõlas ajakirjanduse eesmärkidega. Täpsemalt peavad vastutavad töötlejad kaaluma kahjulikku mõju, mida tekitaks sätte järgimine ajakirjandusele, ja kahjulikku mõju, mida tekitaks selle mittejärgimine andmesubjekti õigustele. Kui ajakirjanik suudab mõistlikult saavutada toimetustelised eesmärgid viisil, mis on kooskõlas andmekaitseseaduse standardsätetega, siis peab ta seda tegema. Ühtlasi peavad organisatsioonid põhjendama piirangu kasutamist iga sätte puhul, mida nad ei ole järginud. „Data protection and journalism: a guide for the media“ (Andmekaitse ja ajakirjandus: suunist meediale), kättesaadav aadressil <https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf>.

⁽⁶⁷⁾ Avaliku huvi näited hõlmavad kuriteo väljaselgitamist või avastamist, rahvatervise või avaliku julgeoleku kaitsmist, üksikisikute või organisatsioonide esitatud eksitavate väidete paljastamist või avalikkust mõjutava ebapädevuse avalikustamist. Vt OFCOMi suunist, kättesaadav aadressil https://www.ofcom.org.uk/_data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf, ja BBC toimetamissuunist, kättesaadav aadressil <https://www.bbc.com/editorialguidelines/guidelines/privacy>.

⁽⁶⁸⁾ Vt Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 89 ning 2018. aasta andmekaitseseaduse 2. lisa 6. osa lõike 27 punkt 2 ja lõike 28 punkt 2.

⁽⁶⁹⁾ Selle suhtes kehtib nõue, et isikuandmeid töödeldakse kooskõlas Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 89 lõikega 1, mida täiendab 2018. aasta andmekaitseseaduse paragrahv 19.

⁽⁷⁰⁾ Vt põhjendused 281–287.

- (75) Ühendkuningriigist isikuandmete rahvusvahelise edastamise kord on sätestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklites 44–49, mida täiendab 2018. aasta andmekaitseseadus, ning see vastab sisu poolest määruse (EL) 2016/679 V peatükis sätestatud normidele ⁽⁷¹⁾. Isikuandmeid võib edastada kolmandasse riiki või rahvusvahelisele organisatsioonile üksnes kaitse piisavuse määruse alusel (Ühendkuningriigi vaste määruse (EL) 2016/679 kohasele kaitse piisavuse otsusele) või kaitse piisavuse määruse puudumise korral juhul, kui vastutav töötaja või volitatud töötaja on kehtestanud asjakohased kaitsemeetmed kooskõlas Ühendkuningriigi isikuandmete kaitse üldmääruse artikliga 46. Kaitse piisavuse määruse või asjakohaste kaitsemeetmete puudumise korral võib andmeid edastada üksnes Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandite alusel.
- (76) Ministri antud kaitse piisavuse määruses võib sätestada, et kolmanda riigi (või kolmanda riigi teatava territooriumi või sektori), rahvusvahelise organisatsiooni või sellise riigi, territooriumi, sektori või organisatsiooni täpse kirjelduse ⁽⁷²⁾ puhul on tagatud isikuandmete piisav kaitsetase. Kaitsetaseme piisavuse hindamisel peab minister võtma arvesse täpselt samu elemente kui need, mida peab hindama komisjon määruse (EL) 2016/679 artikli 45 lõike 2 punktide a–c alusel, tõlgendatuna koos määruse (EL) 2016/679 põhjendusega 104 ja jätkuvalt kohaldatava ELi kohtupraktikaga. See tähendab seda, et kolmanda riigi pakutava piisava kaitsetaseme hindamise asjakohane kriteerium on see, kas see kolmas riik tagab kaitsetaseme, mis „sisuliselt vastab“ Ühendkuningriigis tagatud kaitsetasemele.
- (77) Mis puudutab menetlust, siis kaitse piisavuse määruste suhtes kohaldatakse 2018. aasta andmekaitseseaduse paragrahvis 182 sätestatud üldisi menetlusnõudeid. Nimetatud menetluse raames peab minister Ühendkuningriigi kaitse piisavuse määruse vastuvõtmise ettepaneku tegemisel konsulteerima teabevolinikuga ⁽⁷³⁾. Pärast seda, kui minister on kaitse piisavuse määruse vastu võtnud, esitatakse see parlamendile ja kohaldatakse nn negatiivse resolutsiooni menetlust, mille kohaselt võivad parlamendi mõlemad koad määrust kontrollida ja võtta 40 päeva jooksul vastu ettepaneku selle tühistamiseks ⁽⁷⁴⁾.
- (78) 2018. aasta andmekaitseseaduse paragrahvi 17B lõike 1 kohaselt tuleb kaitse piisavuse määrus vähemalt iga nelja aasta tagant läbi vaadata ning minister peab järjepidevalt jälgima kolmandate riikide ja rahvusvaheliste organisatsioonide arengusuundi, mis võivad mõjutada otsuseid kaitse piisavuse määrus teha või seda muuta või see kehtetuks tunnistama. Kui minister saab teada, et konkreetne riik või organisatsioon ei taga enam isikuandmete piisavat kaitsetaset, peab ta määrust vajalikus ulatuses muutma või selle kehtetuks tunnistama ning alustama asjaomase kolmanda riigi või organisatsiooniga konsultatsioone kaitsetaseme ebapiisavuse kõrvaldamiseks. Menetluse need aspektid kajastavad ka määruse (EL) 2016/679 vastavaid nõudeid.

⁽⁷¹⁾ Välja arvatud määruse (EL) 2016/679 artikkel 48, mida Ühendkuningriik otsustas Ühendkuningriigi isikuandmete kaitse üldmäärusesse mitte lisada. Sellega seoses tuleks esiteks meenutada, et kaitse tase, mida loetakse „kaitse piisavaks tasemeks“ on liidu õiguskorras tagatud tasemega sisuliselt samaväärne (mitte identne) kaitse tase, nagu on selgitanud Euroopa Kohus (kohtuotsus Schrems I, punktid 73–74) ja leidnud Euroopa Andmekaitsekoostöökoostöö (kaitse piisavuse viitedokument, lk 3). Seepärast, nagu selgitas Euroopa Andmekaitsekoostöökoostöö kaitse piisavuse viitedokumendis, „ei ole eesmärk kopeerida punkt-punktilt Euroopa õigusakte, vaid teha kindlaks asjaomaste õigusaktide kõige olulisemad nõuded“. See juures on oluline märkida, et kuigi Ühendkuningriigi õiguskorras ei leidu ametlikult sätet, mis oleks identne artikliga 48, on sama õiguslik toime tagatud teiste sätete ja põhimõtete kaudu, näiteks kui kolmanda riigi kohus või haldusamet esitab isikuandmete taotluse, saab isikuandmeid edastada sellese kolmandasse riiki ainult juhul, kui selle riigiga on sõlmitud rahvusvaheline leping, mille alusel tunnustatakse või täidetakse selle riigi kohtuotsuseid või haldusotsuseid Ühendkuningriigis, või kui andmeid edastatakse Ühendkuningriigi isikuandmete kaitse üldmääruse peatükis V sätestatud edastamismehhanismi alusel. Täpsemalt peavad Ühendkuningriigi kohtud suutma välisriigi kohtuotsuse täitmiseks viidata üldisele õigusele või õigusaktile, millega on selle täitmine lubatud. Ent ei üldise õiguse (vt Adams and Others vs. Cape Industries Plc., [1990] 2 W.L.R. 657) ega õigusaktidega ole ette nähtud välisriikide selliste kohtuotsuste täitmist, millega nõutakse andmete edastamist juhul, kui see ei ole sätestatud rahvusvahelises lepingus. Seetõttu ei ole andmete edastamise taotlused Ühendkuningriigi õiguse kohaselt täidetavad, kui puudub selline rahvusvaheline leping. Lisaks sellele kohaldatakse andmete edastamisele kolmandatesse riikidesse – sealhulgas välisriigi kohtu või haldusametuse taotluse korral – Ühendkuningriigi isikuandmete kaitse üldmääruse V peatükis sätestatud piiranguid, mis on identsed määruse (EL) 2016/679 vastavate sätetega ja mille kohaselt peab andmete edastamiseks olema üks V peatükis sätestatud edastamise alus ja kooskõlas konkreetsete tingimustega, mis selle peatüki kohaselt andmete edastamise suhtes kehtivad.

⁽⁷²⁾ Ühendkuningriigi ametiasutused on selgitanud, et riigi või rahvusvahelise organisatsiooni puhul kirjeldatud olukord viitab olukorrale, mille korral on vaja teha konkreetne ja osaline kaitse piisavuse otsus koos suunatud piirangutega (näiteks kaitse piisavuse määrus üksnes teatavat liiki andmete edastamise kohta).

⁽⁷³⁾ Vt digitaal-, kultuuri-, meedia- ja spordivaldkonna ministri ning teabevoliniku vaheline vastastikuse mõistmise memorandum teabevoliniku rolli kohta seoses Ühendkuningriigi uue kaitse piisavuse hindamisega, kättesaadav aadressil <https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments>.

⁽⁷⁴⁾ Kui määrust tühistamise ettepanek vastu võetakse, ei ole määrust lõppkokkuvõttes mingit edasist õigusmõju.

- (79) Kaitse piisavuse määrase puudumise korral võib andmeid rahvusvaheliselt edastada juhul, kui vastutav töötleja või volitatud töötleja on taganud asjakohased kaitsemeetmed kooskõlas Ühendkuningriigi isikuandmete kaitse üldmääruse artikliga 46. Sellised kaitsemeetmed on sarnased määrase (EL) 2016/679 artikli 46 kohaste meetmetega. Nende hulka kuuluvad õiguslikult siduvad ja täitmisele pööratavad dokumendid avaliku sektori asutuste või organite vahel, siduvad kontsernisisised eeskirjad,⁽⁷⁵⁾ standardsed andmekaitseklauslid, heakskiidetud toimimisjuhendid, heakskiidetud sertifitseerimismehhanismid ning teabevoliniku loal vastutavate töötlejate (või volitatud töötlejate) vahelised lepingutingimused või avaliku sektori asutuste vahelised halduskokkulepped. Menetluslikust seisukohast on neid norme aga muudetud, et need toimiksid Ühendkuningriigi kontekstis, eelkõige võib kooskõlas 2018. aasta andmekaitseadusega standardseid andmekaitseklausleid vastu võtta minister (paragrahv 17C) või teabevolinik (paragrahv 119A).
- (80) Kaitse piisavuse otsuse või asjakohaste kaitsemeetmete puudumise korral võib andmeid edastada üksnes Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 49 sätestatud erandite alusel⁽⁷⁶⁾. Võrreldes määrase (EL) 2016/679 vastavate normidega ei ole Ühendkuningriigi isikuandmete kaitse üldmäärusega tehtud nendes erandites sisulisi muudatusi. Sarnaselt määrasele (EL) 2016/679 saab Ühendkuningriigi isikuandmete kaitse üldmääruse alusel tugineda teatavatele eranditele ainult siis, kui edastamine on juhtumipõhine⁽⁷⁷⁾. Peale selle on teabevolinik oma suunistes rahvusvahelise edastamise kohta täpsustanud järgmist: „Neid tuleb kasutada üksnes tõeliste eranditena üldreeglis, mille kohaselt võib piiratud edastamine toimuda ainult siis, kui see on hõlmatud kaitse piisavuse otsusega või kui on kehtestatud asjakohased kaitsemeetmed“⁽⁷⁸⁾. Mis puudutab andmete sellist edastamist, mis on vajalik avalikust huvist tulenevatel kaalukatel põhjustel (artikli 49 lõike 1 punkt d), siis minister võib anda määrase, milles on täpsustatud, millistel asjaoludel ei ole isikuandmete edastamine kolmandale riigile või rahvusvahelisele organisatsioonile vajalik avalikust huvist tulenevatel kaalukatel põhjustel. Peale selle võib minister määrasega piirata teatava isikuandmete liigi kolmandale riigile või rahvusvahelisele organisatsioonile edastamist juhul, kui andmeid ei saa edastada kaitse piisavuse määrase alusel ning minister leiab, et piirang on vajalik avalikust huvist tulenevatel kaalukatel põhjustel. Selliseid määrase ei ole seni vastu võetud.
- (81) Andmete rahvusvahelise edastamise raamistikku hakati kohaldama üleminekuperioodi lõpus⁽⁷⁹⁾. 2018. aasta andmekaitseaduse 21. lisa lõikes 4 (mis kehtestati andmekaitse, eraelu puutumatuse ja elektroonilise side määrasega) on sätestatud, et alates üleminekuperioodi lõpust käsitletakse teatavat isikuandmete edastamist nii, nagu põhineks see kaitse piisavuse määrausel. See kehtib andmete edastamisel EMP riikidesse, Gibraltarit territooriumile, liidu institutsioonile, organile, ametile või asutusele, mis on loodud ELi asutamislepinguga või selle alusel, ning kolmandatesse riikidesse, mille kohta on üleminekuperioodi lõpus olemas ELi otsus kaitse

⁽⁷⁵⁾ Ühendkuningriigi isikuandmete kaitse üldmääruses on säilitatud määrase (EL) 2016/679 artiklis 47 sätestatud normid, muutes neid üksnes siseriiklikku konteksti sobitamise eesmärgil, näiteks asendades viited pädevale järelevalveasutusele viidetega teabevolinikule, kustutades lõikest 1 viite järjepidevuse mehhanismile ning jättes täielikult välja lõike 3.

⁽⁷⁶⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 49 alusel saab andmeid edastada juhul, kui on täidetud üks järgmistest tingimustest: a) andmesubjekt on edastamiseks andnud selgesõnalise nõusoleku pärast seda, kui teda teavitati sellise edastamisega tema jaoks kaasnevatest võimalikest ohtudest, mis tulenevad kaitse piisavuse otsuse ja asjakohaste kaitsemeetmete puudumisest; b) edastamine on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu täitmiseks või andmesubjekti taotluse alusel võetavate lepingueelsete meetmete rakendamiseks; c) edastamine on vajalik, et andmesubjekti huvides sõlmida vastutava töötleja ja muu füüsilise või juriidilise isiku vahel leping või seda lepingut täita; d) edastamine on vajalik avalikust huvist tulenevatel kaalukatel põhjustel; e) edastamine on vajalik õigusnõuete koostamiseks, esitamiseks või kaitsmiseks; f) edastamine on vajalik, et kaitsta andmesubjekti või muude isikute olulisi huve, kui andmesubjekt on füüsiliselt või õiguslikult võimetu nõusolekut andma; g) edastamine tehakse registrist, mis siseriikliku õiguse kohaselt on mõeldud avalikkuse teavitamiseks ja on tutvumiseks avatud kas laiemale avalikkusele või kõigile, kes suudavad tõendada õigustatud huvi, kuid ainult sellisel määral, nagu konkreetsel juhul on täidetud tutvumist käsitlevad tingimused, mis on siseriikliku õigusega ette nähtud. Peale selle võib juhul, kui ükski eespool nimetatud tingimustest ei ole täidetud, edastada kolmandale riigile või rahvusvahelisele organisatsioonile andmeid üksnes juhul, kui edastamine ei ole korduv, puudutab ainult piiratud arvu andmesubjekte, on vajalik, et kaitsta vastutava töötleja õigustatud huve, mille suhtes andmesubjekti huvid, õigused või vabadused ei ole ülekaalus, ning kui vastutav töötleja on hinnanud kõiki andmete edastamisega seotud asjaolusid ja ja kehtestanud selle hinnangu põhjal sobivad kaitsemeetmed isikuandmete kaitseks.

⁽⁷⁷⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse põhjenduses 111 on öeldud, et lepingu või kohtumenetlusega seoses võib andmeid edastada üksnes juhtumipõhiselt.

⁽⁷⁸⁾ Teabevoliniku suunistes andmete rahvusvahelise edastamise kohta, kättesaadavad aadressil <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7>.

⁽⁷⁹⁾ Maksimaalselt kuue kuu pikkuse ajavahemiku jooksul, mis lõpeb kõige hiljem 30. juunil 2021, tuleb selle uue raamistiku kohaldatavust tõlgendada koosmõjus ühelt poolt Euroopa Liidu ja Euroopa Aatomienergiaühenduse ning teiselt poolt Suurbritannia ja Põhja-Iiri Ühendkuningriigi vahelise kaubandus- ja koostöölepingu (edaspidi „ELi-Ühendkuningriigi kaubandus- ja koostööleping“) artikliga 782 (L 444/14, 31.12.2020) (kättesaadav aadressil [https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:22020A1231\(01\)&from=ET](https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:22020A1231(01)&from=ET)

piisavuse kohta. Sellest tulenevalt võib andmete edastamine nendesse riikidesse jätkuda samamoodi kui enne Ühendkuningriigi EList väljaastumist. Pärast üleminekuperioodi lõppu peab minister need kaitse piisavuse kohta tehtud järeldused nelja aasta jooksul, st 2024. aasta detsembri lõpuks läbi vaatama. Ühendkuningriigi ametiasutuste esitatud selgituse kohaselt peab minister järeldused 2024. aasta detsembri lõpuks küll läbi vaatama, kuid üleminekusätteid ei hõlma nn aegumissätet ning asjaomased üleminekusätted ei kaota automaatselt kehtivust, kui läbivaatamine ei ole 2024. aasta detsembri lõpuks lõpule viidud.

- (82) Lõpetuseks, mis puudutab Ühendkuningriigi rahvusvahelise andmeedastuskorra muutumist tulevikus, kui võetakse vastu uusi kaitse piisavuse määrusi, sõlmitakse rahvusvahelisi lepinguid või töötatakse välja muid edastamismehhanisme, siis komisjon jälgib olukorda tähelepanelikult, hindab, kas erinevaid edastamismehhanisme kasutatakse nii, et see tagab kaitse jätkumise, ning võtab vajaduse korral asjakohaseid meetmeid, millega reageerida võimalikele kaitse jätkumist ohustavatele mõjudele (vt põhjendused 278–287). Kuna ELi ja Ühendkuningriigi andmete rahvusvahelise edastamise reeglid on sarnased, võib eeldada, et probleemseid erinevusi saab ära hoida ka koostöö, teabe vahetamise ja kogemuste jagamise abil, muu hulgas teabevoliniku ja Euroopa Andmekaitseinspektsiooni vahel.

2.5.8. Vastutus

- (83) Vastutuse põhimõtte kohaselt peavad andmeid töötlevad üksused kehtestama asjakohased tehnilised ja korralduslikud meetmed, et täita tõhusalt oma andmekaitsekohustusi ja suuta nende täitmist tõendada, eelkõige pädevale järelevalveasutusele.
- (84) Määruses (EL) 2016/679 sätestatud vastutuse põhimõte on Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 5 lõikes 2 ilma sisuliste muudatusteta säilitatud ning sama kehtib artikli 24 („Vastutava töötleja vastutus“), artikli 25 („Lõimitud andmekaitse ja vaikimisi andmekaitse“) ja artikli 30 („Isikuandmete töötlemise toimingute registreerimine“) puhul. Samuti kohaldatakse jätkuvalt artiklit 35 („Andmekaitsealane mõjuhindamine“) ja artiklit 36 („Eelnev konsulteerimine“). Määruse (EL) 2016/679 artiklid 37–39, mis käsitlevad andmekaitseametniku määramist ja tema ülesandeid, on Ühendkuningriigi isikuandmete kaitse üldmääruses ilma sisuliste muudatusteta jätkuvalt kohaldatavad. Lisaks on Ühendkuningriigi isikuandmete kaitse üldmääruses jätkuvalt kohaldatavad määruse (EL) 2016/679 artiklite 40 („Toimimisjuhendid“) ja 42 („Sertifitseerimine“) sätted ⁽⁸⁰⁾.

2.6. Järelevalve ja õigusnormide täitmise tagamine

2.6.1. Sõltumatu järelevalve

- (85) Et tagada andmekaitse piisav tase ka praktikas, peaks olema loodud sõltumatu järelevalveasutus, millele on antud volitused jälgida andmekaitsenormide järgimist ja tagada nende täitmine. See asutus peaks tegutsema oma ülesandeid täites ja volitusi kasutades täiesti sõltumatult ja erapooletult.
- (86) Ühendkuningriigis teeb Ühendkuningriigi isikuandmete kaitse määruse ja 2018. aasta andmekaitseseaduse üle järelevalvet ning tagab nende täitmise teabevolinik. Teabevolinik on n-ö ühest isikust koosnev ühing – eraldi juriidiline isik, mille moodustab üks inimene. Teabevoliniku tööd toetab tema büroo. 31. märtsi 2020. aasta seisuga oli teabevoliniku büroos 768 alalist töötajat ⁽⁸¹⁾. Teabevolinik kuulub digitaal-, kultuuri-, meedia- ja spordivaldkonna ministeeriumi haldusalasse ⁽⁸²⁾.
- (87) Voliniku sõltumatus on sõnaselgelt sätestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 52, millega ei tehta olulisi muudatusi isikuandmete kaitse üldmääruse artikli 52 lõigetes 1–3. Volinik peab talle Ühendkuningriigi isikuandmete kaitse üldmäärusega antud ülesannete täitmisel ja volituste kasutamisel tegutsema täiesti sõltumatult ning olema seoses nende ülesannete ja volitustega vaba nii otsestest kui ka kaudsetest välistest

⁽⁸⁰⁾ Vajaduse korral on viited asendatud viidetega Ühendkuningriigi ametiasutustele. Näiteks võib 2018. aasta andmekaitseseaduse paragrahvi 17 alusel teabevolinik või Ühendkuningriigi riiklik akrediteerimisasutus akrediteerida Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 43 nõuetele vastava isiku tegema sertifitseerimise üle järelevalvet.

⁽⁸¹⁾ Teabevoliniku 2019.–2020. aasta aruanne ja raamatupidamisaruanne, kättesaadav aadressil <https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf>.

⁽⁸²⁾ Nendevaheline suhe on reguleeritud halduslepinguga. Eelkõige on digitaal-, kultuuri-, meedia- ja spordivaldkonna ministeeriumi kui vastutava ministeeriumi põhiülesanded tagada teabevolinikule piisavad rahalised vahendid ja ressursid, esindada teabevoliniku huve parlamendis ja teistes ministeeriumides, tagada usaldusväärse riikliku andmekaitseametniku olemasolu ning pakkuda teabevoliniku büroole suunistes ja toetust sellistes küsimustes nagu kinnisvara, rendilepingud ja hanked (2018.–2021. aasta haldusleping, kättesaadav aadressil <https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf>).

mõjutustest ega tohi mitte kelleltki juhiseid küsida või vastu võtta. Samuti peab volinik hoiduma oma kohustustega kokkusobimatust tegevusest ega tohi oma ametiaja jooksul töötada ühelgi muul sobimatu tasustatud või tasustamata ametikohal.

- (88) Teabevolniku ametisse määramise ja ametist tagandamise tingimused on sätestatud 2018. aasta andmekaitseaduse 12. lisas. Teabevolniku nimetab õiglase ja avatud konkursi tulemusel ametisse Tema Majesteet valitsuse soovitusel põhjal. Kandidaadil peavad olema sobilikud kvalifikatsioonid, oskused ja pädevused. Kooskõlas ametnike ametisse nimetamise halduseeskirjadega ⁽⁸³⁾ koostab nõustav hindamiskogu loetelu kandidaatidest, kelle saaks ametisse nimetada. Enne, kui digitaal-, kultuuri-, meedia- ja spordivaldkonna minister oma lõpliku otsuse teeb, peab parlamendi asjaomane erikomisjon viima läbi ametisse nimetamise eelse kontrolli. Komisjoni seisukoht avalikustatakse ⁽⁸⁴⁾.
- (89) Teabevolniku ametiaeg kestab kuni seitse aastat. Isiku saab nimetada teabevolniku ametikohale ainult ühel korral. Tema Majesteet võib teabevolniku parlamendi mõlema koja pöördumise ⁽⁸⁵⁾ alusel ametist tagandada. Parlamendi kummalegi kojale ei saa esitada teabevolniku ametist tagandamise taotlust, ilma et minister oleks esitanud aruande, milles ta kinnitab oma veendumust, et teabevolnik on pannud toime tõsise üleastumise ja/või et volinik ei vasta enam tema ülesannete täitmiseks nõutavatele tingimustele ⁽⁸⁶⁾.
- (90) Teabevolnikku rahastatakse kolmest allikast: i) vastutavate töötajate makstavad andmekaitsetasud, mis määratakse kindlaks ministri määrusega ⁽⁸⁷⁾ (2018. aasta andmekaitsemäärus (tasud ja teave) (Data Protection (Charges and Information) Regulations 2018)) ja moodustavad 85–90 % büroo aastaelarvest ⁽⁸⁸⁾; ii) valitsuse toetus teabevolnikule; toetust kasutatakse peamiselt teabevolniku nende tegevuskulude rahastamiseks, mis ei ole seotud andmekaitsealaste ülesannetega, ⁽⁸⁹⁾ ja iii) teenustasud ⁽⁹⁰⁾. Seni ei ole selliseid tasusid nõutud.
- (91) Teabevolniku üldised ülesanded seoses nende isikuandmete töötlemisega, mille suhtes Ühendkuningriigi isikuandmete kaitse üldmäärust kohaldatakse, on sätestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 57, mis järgivad üsna täpselt määruse (EL) 2016/679 vastavaid norme. Tema ülesanded hõlmavad Ühendkuningriigi isikuandmete kaitse üldmääruse kohaldamise jälgimist ja täitmise tagamist, üldsuse teadlikkuse suurendamist, andmesubjektide esitatud kaebuste käsitlemist, uurimiste läbiviimist jms. Lisaks on 2018. aasta andmekaitseaduse paragrahvis 115 sätestatud voliniku muud üldised ülesanded, mille hulka kuuluvad kohustus nõustada parlamenti, valitsust ning muid institutsioone ja asutusi seoses seadusandlike ja haldusmeetmetega, mis käsitlevad üksikisikute isikuandmete töötlemisega seotud õigusi ja vabadusi, ning õigus esitada parlamendile,

⁽⁸³⁾ Ametnike ametisse nimetamise halduseeskirjad, kättesaadavad aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

⁽⁸⁴⁾ Alamkoja kultuuri-, meedia- ja spordikomisjoni 2015.–2016. aasta istungjärgu teine aruanne, kättesaadav aadressil <https://publications.parliament.uk/pa/cm201516/cmselect/cmcomeds/990/990.pdf>.

⁽⁸⁵⁾ Pöördumine on parlamendile esitatav ettepanek, mille eesmärk on teavitada monarhi parlamendi arvamusest teatavas küsimuses.

⁽⁸⁶⁾ 2018. aasta andmekaitseaduse 12. lisa lõike 3 punkt 3.

⁽⁸⁷⁾ 2018. aasta andmekaitseaduse paragrahv 137, vt põhjendus 17.

⁽⁸⁸⁾ 2018. aasta andmekaitseaduse paragrahvid 137 ja 138 sisaldavad mitut kaitsemeetet, millega tagatakse, et tasud kehtestatakse sobilikul tasemel. Eelkõige on paragrahv 137 lõikes 4 loetletud küsimused, mida minister peab arvesse võtma, kui koostab määrust, millega nähakse ette summad, mida eri organisatsioonid peavad tasuma; teiseks sisaldavad 2018. aasta andmekaitseaduse paragrahvi 138 lõige 1 ja paragrahv 182 ka õigusnõuet, mille kohaselt peab minister enne määruse andmist konsulteerima teabevolniku ja teiste selliste isikute esindajatega, keda määrus tõenäoliselt mõjutab, et ta saaks nende arvamusi arvesse võtta. Peale selle peab teabevolnik 2018. aasta andmekaitseaduse paragrahvi 138 lõike 2 alusel tasude määruse toimumist pidevalt jälgima ja ta võib esitada ministrile ettepanekuid määruse muutmiseks. Samuti kehtib määruste suhtes kinnitava resolutsiooni menetlus, välja arvatud juhul, kui määrus antakse välja üksnes eesmärgiga võtta arvesse jaehinnaindeksi kasvu (millisel juhul nende suhtes kehtib negatiivne resolutsiooni menetlus), ning neid ei saa välja anda enne, kui parlamendi mõlemad kodad on need resolutsiooniga heaks kiitnud.

⁽⁸⁹⁾ Halduslepingus on selgitatud: „2018. aasta andmekaitseaduse 12. lisa lõike 9 alusel võib minister teha teabevolnikule makseid parlamendi antud rahalistest vahenditest. Pärast teabevolnikuga konsulteerimist maksab digitaal-, kultuuri-, meedia- ja spordivaldkonna minister teabevolnikule asjakohased summad (toetuse) teabevolniku büroo halduskulude ja teabevolniku mitme konkreetse ülesande, sealhulgas teabevabadusega seotud ülesannete täitmise kulude katmiseks“ (2018.–2021. aasta halduslepingu punkt 1.12, vt joonealune märkus nr 82).

⁽⁹⁰⁾ Vt 2018. aasta andmekaitseaduse paragrahv 134.

valitsusele või muudele institutsioonidele ja asutustele, samuti avalikkusele voliniku enda algatusel või taotluse põhjal arvamusi kõikides isikuandmete kaitsega seotud küsimustes. Kohtusüsteemi sõltumatuse säilitamise eesmärgil ei ole teabevinikul õigust täita oma ülesandeid seoses isikuandmete töötlemisega õigust mõistvat funktsiooni täitva isiku või õigust mõistvat funktsiooni täitva kohtu poolt. Järelevalve kohtute üle tagavad aga spetsialiseerunud asutused (vt põhjendused 99–103).

2.6.2. Õigusnormide täitmise tagamine, sealhulgas karistused

- (92) Teabeviniku volitused on sätestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 58, millega ei tehta sisulisi muudatusi määruse (EL) 2016/679 vastavas artiklis. 2018. aasta andmekaitseseadusega on kehtestatud täiendavad normid nende volituste teostamise kohta. Eelkõige on teabevinikul järgmised volitused: a) nõuda vastutavalt töötlejalt ja volitatud töötlejalt (ning teatavatel asjaoludel teistelt isikutelt) vajaliku teabe andmist, esitades teabenõude (edaspidi „teabenõue“); ⁽⁹¹⁾ b) viia läbi uurimisi ja auditeid, esitades hindamisteate, millega võidakse nõuda volitatud töötlejalt või vastutavalt töötlejalt, et nad lubaksid volinikul siseneda märgitud ruumidesse, kontrollida või uurida dokumente või seadmeid, vestelda vastutava töötleja nimel isikuandmeid töötlevate isikutega jne (edaspidi „hindamisteade“); ⁽⁹²⁾ c) saada kooskõlas 2018. aasta andmekaitseseaduse paragrahvi 154 muul viisil juurdepääs vastutavate töötlejate ja volitatud töötlejate dokumentidele jne ning pääseda nende ruumidesse (edaspidi „volitus siseneda ja kontrollida“); d) teostada parandusvolitusi, muu hulgas hoiatusi ja noomitusi tehes, või anda korraldusi täitmisteate näol, millega nõutakse vastutavalt töötlejatelt / volitatud töötlejatelt teatavate meetmete võtmist või võtmata jätmist, sealhulgas anda vastutavale töötlejale / volitatud töötlejale korraldus võtta Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 58 lõike 2 punktides c–g ja j täpsustatud meetmeid (edaspidi „täitmisteade“); ⁽⁹³⁾ ja e) määrata haldustrahve karistuse määramise teate näol (edaspidi „trahviteade“) ⁽⁹⁴⁾. Trahviteateid saab välja anda ka juhul, kui avaliku sektori asutus ei järgi Ühendkuningriigi isikuandmete kaitse üldmääruse sätteid ⁽⁹⁵⁾.
- (93) Teabeviniku büroo regulatiivse tegevuse poliitikas (*Regulatory Action Policy*) on sätestatud asjaolud, mille korral büroo esitab teabenõude või hindamis-, täitmis- või trahviteate ⁽⁹⁶⁾. Vastutava töötleja või volitatud töötleja tegevuses esinevate puuduste tulemusel esitatud täitmisteatega võib määrata üksnes selliseid nõudeid, mida volinik peab vajalikuks puuduse kõrvaldamiseks. Vastutavale töötlejale või volitatud töötlejale võib esitada täitmisteateid ja trahviteateid seoses Ühendkuningriigi isikuandmete kaitse üldmääruse II peatüki (töötlemise põhimõtted), artiklite 12–22 (andmesubjekti õigused), artiklite 25–39 (vastutavate töötlejate ja volitatud töötlejate kohustused) ning artiklite 44–49 (rahvusvaheline edastamine) rikkumisega. Täitmisteate võib esitada ka siis, kui vastutav töötleja ei ole täitnud nõuet maksta 2018. aasta andmekaitseseaduse paragrahvi 137 alusel antud määruse kohast tasu. Peale selle võib esitada täitmisteate artikli 41 kohasele järelevalveasutusele või sertifikaatide väljastajale, kui nad ei täida oma kohustusi Ühendkuningriigi isikuandmete kaitse üldmääruse alusel. Trahviteate võib esitada ka isikule, kes ei ole järginud teabenõuet, hindamisteadet või täitmisteadet.
- (94) Trahviteate saamisel peab isik tasuma teabevinikule teates märgitud summa. Kui teabevinik otsustab, kas esitada isikule trahviteade ja kui suur peaks olema trahvisumma, peab ta võtma arvesse Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 83 lõigetes 1 ja 2 loetletud tingimusi, mis on identsed määruse (EL) 2016/679 vastavate normidega ⁽⁹⁷⁾. Artikli 83 lõigete 4 ja 5 alusel on nendes sätetes nimetatud kohustuste täitmata jätmise korral määratavate haldustrahvide maksimaalsed summad vastavalt 8 700 000 naelsterlingit või 17 500 000 naelsterlingit. Ettevõtja puhul võib teabevinik määrata trahve ka protsendimäärana ülemaailmsest aastakäibest, kui see summa

⁽⁹¹⁾ 2018. aasta andmekaitseseaduse paragrahv 142 (kohaldatakse 2018. aasta andmekaitseseaduse paragrahvis 143 sätestatud piiranguid).

⁽⁹²⁾ 2018. aasta andmekaitseseaduse paragrahv 146 (kohaldatakse 2018. aasta andmekaitseseaduse paragrahvis 147 sätestatud piiranguid).

⁽⁹³⁾ 2018. aasta andmekaitseseaduse paragrahvid 149–151 (kohaldatakse 2018. aasta andmekaitseseaduse paragrahvis 152 sätestatud piiranguid).

⁽⁹⁴⁾ 2018. aasta andmekaitseseaduse paragrahv 155 ja Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 83.

⁽⁹⁵⁾ See tuleneb 2018. aasta andmekaitseseaduse paragrahvi 155 lõikest 1 koostoimes sama seaduse paragrahvi 149 lõigete 2 ja 5 ning sama seaduse paragrahvi 156 lõikest 4, millega piiratakse trahviteadete väljastamist üksnes riigivara volinikele (Crown Estate Commissioners) ja isikutele, kes on kuningakoja vastutavad töötlejad 2018. aasta andmekaitseseaduse paragrahvi 209 lõike 4 järgi.

⁽⁹⁶⁾ Dokument „Regulatory Action Policy“, kättesaadav aadressil <https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf>.

⁽⁹⁷⁾ Sealhulgas rikkumise laad ja raskus (võttes arvesse asjaomase töötlemise laadi, ulatust või eesmärki, samuti mõjutatud andmesubjektide hulka ja neile tekitatud kahju suurust), asjaolu, kas rikkumine pandi toime tahtlikult või hooletusest, vastutava töötleja või volitatud töötleja poolt võetud meetmed andmesubjektide kantud kahju leevendamiseks, vastutava töötleja või volitatud töötleja vastutuse aste (võttes arvesse vastutava töötleja või volitatud töötleja poolt võetud tehnilisi ja korralduslikke meetmeid), vastutava töötleja või volitatud töötleja eelnevad asjakohased rikkumised, volinikuga tehtava koostöö määr, puudusest mõjutatud isikuandmete liigid ning juhtumi asjaolude suhtes kohaldatavad muud raskendavad või kergendavad tegurid, näiteks rikkumisest otseselt või kaudselt saadud finantskasu või välditud kahju.

on suurem. Sarnaselt määruse (EL) 2016/679 samaväärsetele sätetele on artikli 83 lõigetes 4 ja 5 kehtestatud nendeks summadeks vastavalt 2 % ja 4 %. Teabenõude, hindamisteate või täitmisteate järgimata jätmise korral võib trahviteatega määrata trahvi, mille summa on maksimaalselt 17 500 000 naelsterlingit või ettevõtja puhul 4 % ülemaailmsest aastakäibest, olenevalt sellest, kumb summa on suurem.

- (95) Samuti on Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseseadusega tugevdatud teabevolniku muid volitusi. Näiteks võib volinik nüüd viia hindamisteade kaudu läbi kõikide vastutavate töötajate ja volitatud töötajate kohustuslikke auditeid, samas kui varasema õigusakti – 1998. aasta andmekaitseseaduse – alusel olid volinikul volitused üksnes seoses keskvalitsuse ja tervishoiuorganisatsioonidega ning ülejäänud töötajad pidid auditiga nõustuma.
- (96) Alates määruse (EL) 2016/679 kehtestamisest menetleb teabevolinik aastas ligikaudu 40 000 andmesubjektidelt laekunud kaebust ⁽⁹⁸⁾ ja viib lisaks sellele läbi ligikaudu 2 000 uurimist ametiülesande korras ⁽⁹⁹⁾. Enamik kaebusi on seotud andmetega tutvumise õigusega ja õigusega andmete avalikustamisele. Pärast uurimise läbiviimist võtab volinik täitmise tagamise meetmeid mitmesugustes valdkondades. Täpsemalt esitas teabevolinik oma viimase aastaaruande (2019–2020) ⁽¹⁰⁰⁾ kohaselt aruandlusperioodil 54 teabenõuet, 8 hindamisteadet, 7 täitmisteadet, 4 hoiatust ja 8 süüdistust ning määras 15 trahvi ⁽¹⁰¹⁾.
- (97) Nende hulka kuuluvad mitu olulist rahalist karistust, mis määrati määruse (EL) 2016/679 ja 2018. aasta andmekaitseseaduse alusel. Näiteks määras teabevolinik 2020. aasta oktoobris Briti lennuettevõtjale 20 miljoni naelsterlingi suuruse trahvi andmetega seotud rikkumise eest, mis mõjutas rohkem kui 400 000 klienti. 2020. aasta oktoobri lõpus määrati rahvusvahelisele hotelliketile 18,4 miljoni naelsterlingi suurune trahv, kuna ta ei taganud miljonite klientide isikuandmete turvalisust, ning 2020. aasta novembris määrati 1,25 miljoni naelsterlingi suurune trahv ürituste pileteid müüvale Briti teenuseosutajale klientide makseandmete kaitsmata jätmise eest ⁽¹⁰²⁾.
- (98) Lisaks teabevolniku õigusnormide täitmise tagamise volitustele, mida on kirjeldatud põhjenduses 92, on teatavad andmekaitsealaste õigusaktide rikkumised süüteod ja seega võidakse nende korral kohaldada kriminaalkaristusi (vt 2018. aasta andmekaitseseaduse paragrahv 196). See kehtib näiteks juhul, kui teadlikult või hooletuse tõttu hangitakse või avalikustatakse isikuandmeid ilma vastutava töötaja nõusolekuta, korraldatakse isikuandmete avalikustamine teisele isikule ilma vastutava töötaja nõusolekuta, ⁽¹⁰³⁾ muudetakse ilma vastutava töötaja nõusolekuta uuesti identifitseeritavaks teave, mille näol on tegu umbisikustatud isikuandmetega, ⁽¹⁰⁴⁾ takistatakse tahtlikult voliniku õiguse teostamist seoses isikuandmete kontrollimisega kooskõlas rahvusvaheliste kohustustega, ⁽¹⁰⁵⁾ esitatakse vastusena teabenõudele valeväiteid või hävitatakse teavet seoses teabenõute või hindamisteadetega ⁽¹⁰⁶⁾.

⁽⁹⁸⁾ Ühendkuningriigi ametiasutuste esitatud teabe kohaselt tehti teabevolniku aastaaruandes (2019–2020) käsitletud ajavahemiku jooksul ligikaudu 25 % juhtudest järeldus, et rikkumist ei ole toimunud, ligikaudu 29 % juhtudest paluti andmesubjektidel küsimusega esmakordselt teabevolniku poole pöörduda, oodata ära vastutava töötaja vastus või jätkata pooleliolevat dialoogi vastutava töötajaga, ligikaudu 17 % juhtudest ei tehtud kindlaks rikkumist, kuid vastutavale töötajale anti nõu, ligikaudu 25 % juhtudest tegi teabevolinik kindlaks rikkumise ning kas andis vastutavale töötajale nõu või nõudis vastutavalt töötajalt teatavate meetmete võtmist, ligikaudu 3 % juhtudest tehti kindlaks, et kaebus ei kuulu määruse (EL) 2016/679 kohaldamisalasse ning ligikaudu 1 % juhtumeid suunati mõnda teise andmekaitseasutusse Euroopa Andmekaitsekoostöö raamistikus.

⁽⁹⁹⁾ Teabevolinik võib alata selliseid uurimisi teabe põhjal, mis on saadud mitmesugustest allikatest, sealhulgas isikuandmetega seotud rikkumiste teated, Ühendkuningriigi muude avaliku sektori asutuste või välisriikide andmekaitseasutuste poolset suunamist ja üksikisikute või kodanikuühiskonna organisatsioonide kaebused.

⁽¹⁰⁰⁾ Teabevolniku 2019–2020. aasta aruanne ja raamatupidamisaruanne (vt joonealune märkus nr 81).

⁽¹⁰¹⁾ Eelmise aastaaruande kohaselt, milles käsitleti ajavahemikku 2018–2019, esitas teabevolinik aruandlusperioodil 1998. aasta andmekaitseseaduse alusel 22 trahviteadet, kusjuures trahvid moodustasid kokku 3 010 610 naelsterlingit, sealhulgas kaks 500 000 naelsterlingi suurust trahvi (1998. aasta andmekaitseseaduse alusel lubatud maksimumsumma). 2018. aastal uuris teabevolinik pärast Cambridge Analytica puudutavaid paljastusi andmeanalüüsi kasutamist poliitilistel eesmärkidel. Uurimise tulemusel koostati poliitikaaruanne ja kogum soovitusi, määrati Facebookile 500 000 naelsterlingi suurune trahv ning esitati täitmisteade Kanada andmevahendajale Aggregate IQ, millega nõuti äriühingult Ühendkuningriigi kodanike ja elanike isikuandmete kustutamist (vt teabevolniku 2018.–2019. aasta aruanne ja raamatupidamisaruanne, kättesaadav aadressil <https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf>).

⁽¹⁰²⁾ Ülevaade võetud täitemetmetest on esitatud teabevolniku veebisaidil, kättesaadav aadressil <https://ico.org.uk/action-weve-taken/enforcement/>.

⁽¹⁰³⁾ 2018. aasta andmekaitseseaduse paragrahv 170.

⁽¹⁰⁴⁾ 2018. aasta andmekaitseseaduse paragrahv 171.

⁽¹⁰⁵⁾ 2018. aasta andmekaitseseaduse paragrahv 119.

⁽¹⁰⁶⁾ 2018. aasta andmekaitseseaduse paragrahvid 144 ja 148.

2.6.3. Järelevalve kohtute üle

- (99) Järelevalve isikuandmete töötlemise üle kohtute poolt on kahesugune. Kui kohtunik või kohus ei täida õigust mõistvat funktsiooni, siis teeb järelevalvet teabevolnik. Kui vastutav töötleja täidab õigust mõistvat funktsiooni, ei saa teabevolnik oma järelevalveülesandeid täita⁽¹⁰⁷⁾ ja järelevalvet teevad spetsiaalsed asutused. See vastab lähenemisviisile, mida järgitakse määruses (EL) 2016/679 (artikli 55 lõige 3).
- (100) Täpsemalt teeb teise stsenaariumi puhul Inglismaa ja Walesi kohtute ning Inglismaa ja Walesi esimese astme kohtute (First-tier Tribunals) ja kõrgemate kohtute (Upper Tribunals) puhul järelevalvet kohtute andmekaitsekomisjon (Judicial Data Protection Panel)⁽¹⁰⁸⁾. Peale selle on ülemkohtunik (Lord Chief Justice) ja kohtute kõrgeim president (Senior President of Tribunals) andnud välja eraelu puutumatust käsitleva teate,⁽¹⁰⁹⁾ milles on sätestatud isikuandmete töötlemine Inglismaa ja Walesi kohtutes õigust mõistva funktsiooni täitmisel. Sarnase teate on andnud välja Põhja-lirimaa⁽¹¹⁰⁾ ja Šotimaa⁽¹¹¹⁾ kohtud.
- (101) Peale selle on Põhja-lirimaa ülemkohtunik nimetanud Põhja-lirimaal kõrge kohtu kohtuniku andmekaitse üle järelevalvet tegevaks kohtunikuks (Data Supervisory Judge)⁽¹¹²⁾. Samuti on Põhja-lirimaa kohtunikele antud suuniseid selle kohta, mida andmete kaotsimineku või võimaliku kaotsimineku korral teha, ja sellest tulenevate küsimuste lahendamise kohta⁽¹¹³⁾.
- (102) Šotimaal on lordpresident nimetanud andmekaitse üle järelevalvet tegeva kohtuniku, kes uurib kõiki andmekaitsega seotud põhjustel esitatud kaebusi. See on sätestatud kohtunike vastu esitatud kaebusi käsitlevates normides, mis vastavad Inglismaal ja Walesis kehtivatele normidele⁽¹¹⁴⁾.
- (103) Samuti on kõrgeimas kohtus määratud üks kõrgeima kohtu kohtunik andmekaitse üle järelevalvet tegema.

2.6.4. Õiguskaitse

- (104) Piisava kaitse tagamiseks ja eelkõige üksikisiku õiguste maksmapanekuks tuleks andmesubjektile tagada tõhus haldus- ja õiguskaitse, sealhulgas kahju hüvitamine.

⁽¹⁰⁷⁾ 2018. aasta andmekaitseaduse paragrahv 117.

⁽¹⁰⁸⁾ Komisjon vastutab kohtunikele suuniste ja koolituse pakkumise eest. Samuti menetleb ta andmesubjektide kaebusi seoses isikuandmete töötlemisega õigust mõistvat funktsiooni täitvate kohtute ja isikute poolt. Komisjoni eesmärk on pakkuda vahendeid mis tahes kaebuse lahendamiseks. Kui komisjoni vastus kaebuse esitajale ei rahulda ja ta esitab täiendavaid tõendeid, võib komisjon oma otsust uuesti kaaluda. Kuigi komisjon ise rahalisi karistusi ei määra, siis võib ta juhul, kui leiab, et tegemist on 2018. aasta andmekaitseaduse piisavalt tõsise rikkumisega, suunata küsimuse kohtunike käitumist uurivale ametile (Judicial Conduct Investigation Office – JCIO), kes kaebust uurib. Kui kaebus rahuldatakse, siis otsustavad lordkantsler ja ülemkohtunik (või kõrgem kohtunik, kes on delegeritud tema nimel tegutsema), milliseid meetmeid tuleks kohtunikuameti pidaja suhtes võtta. Raskusastme järjekorras hõlmavad need järgmist: ametlik nõuanne, ametlik hoiatus ja noomitus ning viimaks ametist tagandamine. Kui isik ei ole rahul sellega, kuidas JCIO kaebust uuris, võib ta esitada täiendava kaebuse kohtunike ametisse nimetamise ja kohtunike käitumise ombudsmanile (Judicial Appointments and Conduct Ombudsman) (vt <https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman>). Ombudsmanil on õigus nõuda JCIO-lt kaebuse uut uurimist ja kui ta leiab, et kaebuse esitaja on kandnud haldusomavoli tõttu kahju, võib ta teha ettepaneku maksta kaebuse esitajale hüvitist.

⁽¹⁰⁹⁾ Ülemkohtuniku ja kohtute kõrgeima presidendi väljaantud eraelu puutumatust käsitlev teade on kättesaadav aadressil <https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice>.

⁽¹¹⁰⁾ Põhja-lirimaa ülemkohtuniku väljaantud eraelu puutumatust käsitlev teade on kättesaadav aadressil <https://judiciaryni.uk/data-privacy>.

⁽¹¹¹⁾ Šotimaa kohtuid käsitlev eraelu puutumatuse teade on kättesaadav aadressil <https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice>.

⁽¹¹²⁾ Andmekaitse üle järelevalvet tegev kohtunik annab kohtunikele suuniseid ja uurib rikkumisi ja/või kaebusi seoses isikuandmete töötlemisega õigust mõistvat funktsiooni täitvate kohtute või isikute poolt.

⁽¹¹³⁾ Kui leitakse, et kaebus või rikkumine on tõsine, suunatakse see kooskõlas Põhja-lirimaa ülemkohtuniku koostatud tegevusjuhendiga kaebuste kohta täiendavaks uurimiseks edasi kohtunike vastu esitatud kaebusi menetlevale ametnikule. Sellise kaebuse tulemused võivad olla järgmised: täiendavaid meetmeid ei võeta, antakse nõu, pakutakse koolitust või juhendamist, esitatakse mitteametlik hoiatus, esitatakse ametlik hoiatus, esitatakse lõplik hoiatus, piiratakse tegevust või suunatakse küsimus seadusega ettenähtud kohtule. Põhja-lirimaa ülemkohtuniku väljaantud tegevusjuhend kaebuste kohta on kättesaadav aadressil https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20-%202028%20Feb%2013%2028Final%29%20updated%20with%20new%20comp.._1.pdf.

⁽¹¹⁴⁾ Andmekaitse üle järelevalvet tegev kohtunik uurib kõiki põhjendatud kaebusi ja suunab need edasi lordpresidendile, kellel on õigus anda nõu, teha ametlikke hoiatusi või noomitusi, kui ta seda vajalikuks peab (samaväärsed normid on koostatud kohtute liikmete kohta ja on kättesaadavad aadressil https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

- (105) Esiteks on andmesubjektil õigus esitada teabevinikule kaebus, kui ta leiab, et seoses teda puudutavate isikuandmetega on rikutud Ühendkuningriigi isikuandmete kaitse üldmäärust⁽¹¹⁵⁾. Ühendkuningriigi isikuandmete kaitse üldmääruses on ilma sisuliste muudatusteta säilitatud määruse (EL) 2016/679 artiklis 77 selle õiguse kohta sätestatud normid. Sama kehtib artikli 57 lõike 1 punkti f ja lõike 2 puhul, kus on sätestatud voliniku ülesanded seoses kaebuste käsitlemisega. Nagu on kirjeldatud põhjendustes 92–98, on teabevinikul õigus hinnata, kas vastutav töötleja ja volitatud töötleja täidavad Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseaduse nõudeid, nõuda neilt nõuete mittetäitmise korral vajalike meetmete võtmist või meetmete võtmata jätmist ning määrata trahve.
- (106) Teiseks on Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseadusega ette nähtud õigus õiguskaitsevahendile teabeviniku vastu. Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 78 lõike 1 kohaselt on isikul õigus kasutada tõhusat õiguskaitsevahendit voliniku õiguslikult siduva otsuse vastu, mis teda puudutab. Kohtuliku kontrolli raames vaatab kohtunik vaidlustatud otsuse läbi ja kaalub, kas teabevinik tegutses seaduspäraselt. Peale selle saab kaebuse esitaja juhul, kui volinik andmesubjekti esitatud kaebust nõuetekohaselt ei käsitse,⁽¹¹⁶⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 78 lõike 2 kohaselt kasutada õiguskaitsevahendit. Ta võib pöörduda esimese astme kohtusse (First Tier Tribunal), kes võib nõuda volinikult kaebusele vastamiseks nõuetekohaste meetmete võtmist või kaebuse esitaja teavitamist kaebuse menetlemise edenemisest⁽¹¹⁷⁾. Peale selle võib iga isik, kellele volinik esitab mõne eespool nimetatud teate (teabenõue, hindamisteade, täitmisteade või trahviteade), kaevata teate peale esimese astme kohtusse⁽¹¹⁸⁾. Kui kohus leiab, et voliniku otsus ei ole õigusaktidega kooskõlas või et volinik oleks pidanud oma kaalutlusõigust teistmoodi teostama, peab kohus kaebuse rahuldama või asendama teate või otsuse sellise teate või otsusega, mille teabevinik oleks võinud esitada või teha.
- (107) Kolmandaks saavad isikud Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 79 ja 2018. aasta andmekaitseaduse paragrahvi 167 alusel kasutada kohtus õiguskaitsevahendit otse vastutavate töötlejate ja volitatud töötlejate vastu. Kui kohus nõustub andmesubjekti avalduse põhjal, et andmesubjekti andmekaitsealastest õigusaktidest tulenevaid õigusi on rikutud, võib kohus nõuda, et töötlemise eest vastutav töötleja või tema nimel tegutsev volitatud töötleja võtaks või jätaks võtmata kohtumääruses märgitud meetmed.
- (108) Peale selle on iga isikul, kes on kandnud Ühendkuningriigi isikuandmete kaitse üldmääruse rikkumise tulemusel materiaalset või mittemateriaalset kahju, Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 82 ja 2018. aasta andmekaitseaduse paragrahvi 168 kohaselt õigus saada vastutavalt töötlejalt või volitatud töötlejalt hüvitist tekitatud kahju eest. Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 82 lõigetes 1–5 sätestatud normid hüvitise ja vastutuse kohta on identsed määruse (EL) 2016/679 vastavate normidega. 2018. aasta andmekaitseaduse paragrahvi 168 alusel hõlmab mittemateriaalne kahju ka kannatusi. Samuti on andmesubjektil Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 80 alusel õigus volitada esindavat organit või organisatsiooni esitama tema nimel volinikule kaebuse (Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 77 alusel) ja kasutama tema nimel õigusi, mida on nimetatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 78 („Õigus tõhusale õiguskaitsevahendile voliniku vastu“), artiklis 79 („Õigus tõhusale õiguskaitsevahendile vastutava töötleja või volitatud töötleja vastu“) ja artiklis 82 („Õigus hüvitisele ja vastutusele“).
- (109) Neljandaks võib iga isik, kes leiab, et avaliku sektori asutused on rikkunud tema õigusi, sealhulgas õigust eraelu puutumatusele ja andmekaitsele, lisaks nendele õiguskaitsevahendile kasutamise võimalustele taotleda Ühendkuningriigis õiguskaitset ka 1998. aasta inimõiguste seaduse alusel⁽¹¹⁹⁾. Isik, kes väidab, et avaliku sektori asutus käitus (või kavatses käituda) viisil, mis ei ole kooskõlas konventsioonist tuleneva õigusega ja on seetõttu 1998. aasta inimõiguste seaduse paragrahvi 6 lõike 1 alusel ebaseaduslik, võib algatada selle asutuse vastu asjakohases kohtus menetluse või tugineda asjaomastele õigustele mis tahes kohtumenetluses, kui ta on (või oleks) ebaseadusliku tegevuse ohver.
- (110) Kui kohus leiab, et avaliku sektori asutuse tegevus on ebaseaduslik, võib ta määrata oma volituste piires sellise õiguskaitsevahendi või hüvitise või teha sellise korralduse, mida ta peab õiglaseks ja asjakohaseks⁽¹²⁰⁾. Samuti võib kohus sedastada, et esmase õigusakti säte on vastuolus konventsioonist tuleneva õigusega.

⁽¹¹⁵⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikkel 77.

⁽¹¹⁶⁾ 2018. aasta andmekaitseaduse paragrahvis 166 on konkreetselt osutatud järgmistele olukordadele: a) volinik ei võta asjakohaseid meetmeid kaebusele vastamiseks, b) volinik ei esita kaebuse esitajale teavet kaebuse menetlemise edenemise või kaebuse tulemuste kohta kolme kuu jooksul alates sellest, kui volinik sai kaebuse, või c) volinik ei ole selle aja jooksul kaebuse läbivaatamisega lõpule jõudnud ega esita kaebuse esitajale nõutavat teavet ka järgneva kolmekuulise ajavahemiku jooksul.

⁽¹¹⁷⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 78 lõike 2 ja 2018. aasta andmekaitseaduse paragrahv 166.

⁽¹¹⁸⁾ Ühendkuningriigi isikuandmete kaitse üldmääruse artikli 78 lõike 1 ja 2018. aasta andmekaitseaduse paragrahv 162.

⁽¹¹⁹⁾ 1998. aasta inimõiguste seaduse paragrahvi 7 lõike 1. Paragrahvi 7 lõike 7 kohaselt on isik ebaseadusliku tegevuse ohver ainult siis, kui ta oleks ohver Euroopa inimõiguste konventsiooni artikli 34 tähenduses juhul, kui selle tegevuse kohta oleks algatatud menetlus Euroopa Inimõiguste Kohtus.

⁽¹²⁰⁾ 1998. aasta inimõiguste seaduse paragrahvi 8 lõike 1.

- (111) Lisaks võib isik pärast siseriiklike õiguskaitsevahendite ammendumist taotleda Euroopa inimõiguste konventsiooni alusel tagatud õiguste rikkumise korral õiguskaitset Euroopa Inimõiguste Kohtus.

3. JUURDEPÄÄS EUROOPA LIIDUST EDASTATUD ISIKUANDMETELE JA NENDE KASUTAMINE ÜHENDKUNINGRIIGIS ASUVATE AVALIKU SEKTORI ASUTUSTE POOLT

- (112) Komisjon hindas ka Ühendkuningriigi õigusraamistikku, mis reguleerib Ühendkuningriigis asuvatele ettevõtjatele edastatud isikuandmete kogumist ja järgnevat kasutamist Ühendkuningriigi avaliku sektori asutuste poolt avaliku huvi eesmärkidel, eelkõige kriminaalõiguskaitse ja riigi julgeoleku eesmärkidel (edaspidi „valitsuse juurdepääs“). Selle hindamisel, kas tingimused, mille alusel valitsusel on juurdepääs käesoleva otsuse alusel Ühendkuningriiki edastatud andmetele, täidavad määruse (EL) 2016/679 artikli 45 lõikega 1 ette nähtud nn sisulise vastavuse nõude, mida Euroopa Liidu Kohus on tõlgendanud Euroopa Liidu põhiõiguste harta alusel, võttis komisjon arvesse eelkõige järgmisi kriteeriume.
- (113) Esiteks peab isikuandmete kaitse õiguse piirang olema ette nähtud õigusaktidega ning õiguslikus aluses, mis võimaldab sellisesse õigusesse sekkuda, peab olema määratletud, kui ulatuslikult tohib asjaomase õiguse teostamist piirata ⁽¹²¹⁾.
- (114) Teiseks peab proportsionaalsuse nõude täitmiseks, mille kohaselt tohib isikuandmete kaitse suhtes kohaldada erandeid ja piiranguid üksnes sel määral, mil see on demokraatlikus ühiskonnas rangelt vajalik liidus tunnustatud samaväärsete konkreetsete üldist huvi pakkuvate eesmärkide täitmiseks, olema asjaomase kolmanda riigi õigusaktides, millega sekkumist lubatakse, sätestatud selged ja täpsed normid, millega reguleeritakse kõnealuste meetmete kohaldamisala ja kohaldamist ning kehtestatakse minimaalsed kaitsemeetmed, et isikutel, kelle andmeid on edastatud, oleksid piisavad tagatised oma isikuandmete tõhusaks kaitseks kuritarvitamise ohu eest ⁽¹²²⁾. Eelkõige tuleb sellistes õigusaktides osutada, millistel asjaoludel ja tingimustel võib vastu võtta meetme, millega selliste andmete töötlemine ette nähakse, ⁽¹²³⁾ ning kehtestada selliste nõuete täitmise kontrollimiseks sõltumatu järelevalve ⁽¹²⁴⁾.
- (115) Kolmandaks peavad sellised õigusaktid olema siseriikliku õiguse alusel õiguslikult siduvad ning need õigusnõuded ei pea olema mitte üksnes ametiasutuste suhtes siduvad, vaid ka asjaomase kolmanda riigi ametiasutuste vastu kohtus kaitstavad ⁽¹²⁵⁾. Eelkõige peab andmesubjektil olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda teda puudutavate isikuandmetega või lasta neisse parandusi teha või neid kustutada ⁽¹²⁶⁾.

3.1. Üldine õigusraamistik

- (116) Kuna tegemist on avaliku sektori volituste kasutamisega, peab valitsuse juurdepääs Ühendkuningriigis toimuma täielikult õiguspäraselt. Ühendkuningriik on ratifitseerinud Euroopa inimõiguste konventsiooni (vt põhjendus 9) ja kõik avaliku sektori asutused Ühendkuningriigis peavad tegutsema kooskõlas konventsiooniga ⁽¹²⁷⁾. Konventsiooni artikliga 8 on ette nähtud, et mis tahes sekkumine eraelu puutumatuse peab olema kooskõlas seadusega, mõne artikli 8 lõikes 2 sätestatud eesmärgi huvides ja selle eesmärgiga proportsionaalne. Samuti on artikliga 8 nõutud, et sekkumine peab olema ettenähtav, see tähendab, et sellel peab olema õigusaktides selge ja juurdepääsetav alus ning need õigusaktid peavad sisaldama asjakohaseid kaitsemeetmeid kuritarvitamise vältimiseks.
- (117) Peale selle on Euroopa Inimõiguste Kohus oma kohtupraktikas täpsustanud, et eraelu puutumatuse ja andmekaitse õigusesse sekkumise suhtes peab kehtima tõhus, sõltumatu ja erapooletu järelevalvesüsteem, mille on ette näinud kohtunik või mõni muu sõltumatu organ ⁽¹²⁸⁾ (nt haldusasutus või parlamendiorgan).

⁽¹²¹⁾ Vt kohtuotsus Schrems II, punktid 174–175 ja seal nimetatud kohtupraktika. Seoses liikmesriikide avaliku sektori asutuste juurdepääsuga vt ka otsus kohtuasjas C-623/17: Privacy International, ECLI:EU:C:2020:790, punkt 65, ja otsus liidetud kohtuasjades C-511/18, C-512/18 ja C-520/18: La Quadrature du Net ja teised, ECLI:EU:C:2020:791, punkt 175.

⁽¹²²⁾ Vt kohtuotsus Schrems II, punktid 176 ja 181 ja seal nimetatud kohtupraktika. Liikmesriikide avaliku sektori asutuste juurdepääsu kohta vt ka kohtuotsus Privacy International, punkt 68, ja kohtuotsus La Quadrature du Net ja teised, punkt 132.

⁽¹²³⁾ Vt kohtuotsus Schrems II, punkt 176. Liikmesriikide avaliku sektori asutuste juurdepääsu kohta vt ka kohtuotsus Privacy International, punkt 68, ja kohtuotsus La Quadrature du Net ja teised, punkt 132.

⁽¹²⁴⁾ Vt kohtuotsus Schrems II, punkt 179.

⁽¹²⁵⁾ Vt kohtuotsus Schrems II, punktid 181–182.

⁽¹²⁶⁾ Vt kohtuotsus Schrems I, punkt 95, ja kohtuotsus Schrems II, punkt 194. Sellega seoses on Euroopa Liidu Kohus eelkõige rõhutanud Euroopa Liidu põhiõiguste harta artiklit 47 (millega tagatakse õigus tõhusale õiguskaitsevahendile sõltumatus ja erapooletus kohtus), „millel on oma osa liidus nõutava kaitse taseme kujundamisel [ja] mille järgimise peab komisjon olema tuvastanud enne, kui ta saab vastu võtta otsuse“ määruse (EL) 2016/679 artikli 45 lõike 1 alusel (kohtuotsus Schrems II, punkt 186).

⁽¹²⁷⁾ 1998. aasta inimõiguste seaduse paragrahv 6.

⁽¹²⁸⁾ Euroopa Inimõiguste Kohtu otsus kohtuasjas Klass ja teised vs. Saksamaa, kaebus nr 5029/71, punktid 17–51.

- (118) Lisaks tuleb üksikisikutele pakkuda tõhusat õiguskaitsevahendit ning Euroopa Inimõiguste Kohus on selgitanud, et sellist õiguskaitsevahendit peab pakkuma sõltumatu ja erapooletu organ, mis on vastu võtnud oma kodukorra ja koosneb liikmetest, kes töötavad või on töötanud kõrges kohtunikuametis või on kogenud juristid, ning sellele organile taotluse esitamise tingimuseks ei tohi olla tõendamiskohustuse täitmine. Üksikisikute kaebuste läbivaatamisel peab sõltumatul ja erapooletul organil olema juurdepääs kogu asjakohasele teabele, sealhulgas suletud toimikutele. Samuti peavad tal olema volitused nõuete täitmata jätmise heastada ⁽¹²⁹⁾.
- (119) Ühendkuningriik on ratifitseerinud ka Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (konventsioon nr 108) ja allkirjastas 2018. aastal protokolli, millega muudetakse isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (mida tuntakse ka konventsioonina nr 108+) ⁽¹³⁰⁾. Konventsiooni nr 108 artiklis 9 on sätestatud, et erandid andmekaitsepõhimõtetest (artikkel 5 „Andmekvaliteet“), andmete eriliike reguleerivatest normidest (artikkel 6 „Andmete eriliigid“) ja andmesubjekti õigustest (artikkel 8 „Lisatagatise andmesubjektile“) on lubatud üksnes juhul, kui selline erand on ette nähtud osalisriigi õigusega ning osutub demokraatlikus ühiskonnas vajalikuks, et kaitsta riigi julgeolekut, avalikku korda, riigi rahalisi huve või võidelda kuritegevuse vastu või kaitsta andmesubjekti või muu isiku õigusi ja vabadusi ⁽¹³¹⁾.
- (120) Kuna Ühendkuningriik on Euroopa Nõukogu liige, kehtib tema suhtes Euroopa inimõiguste konventsiooni järgimise ja Euroopa Inimõiguste Kohtu pädevusse kuulumise tagajärjel seega mitu rahvusvahelises õiguses sätestatud kohustust, mis loovad raamistiku valitsuse juurdepääsu süsteemile, lähtudes sarnastest põhimõtetest, kaitsemeetmetest ja üksikisiku õigustest kui need, mis on tagatud ELi õiguse alusel ja kohaldatavad liikmesriikides. Nagu on rõhutatud põhjenduses 19, on selliste õigusaktide jätkuv järgimine seega käesoleva otsuse aluseks oleva hindamise eriti oluline element.
- (121) Lisaks on 2018. aasta andmekaitseseadusega tagatud konkreetsed andmekaitsega seotud kaitsemeetmed ja õigused juhul, kui andmeid töötlevad avaliku sektori asutused, sealhulgas õiguskaitseasutused ja riiklikud julgeolekuasutused.
- (122) Isikuandmete töötlemise kord kriminaalõiguskaitse kontekstis on sätestatud eeskätt 2018. aasta andmekaitseseaduse 3. osas, mis kehtestati direktiivi (EL) 2016/680 ülevõtmiseks. 2018. aasta andmekaitseseaduse 3. osa kohaldatakse isikuandmete töötlemise suhtes pädevate asutuste poolt süütegude ennetamiseks, uurimiseks, avastamiseks või nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks ⁽¹³²⁾.
- (123) Pädev asutus on määratletud andmekaitseseaduse paragrahvis 30 kui 2018. aasta andmekaitseseaduse 7. lisas loetletud isik ja muu isik, kellel on seadusjärgsed ülesanded õiguskaitse tagamise eesmärgil ⁽¹³³⁾. Nagu on järgnevalt selgitatud (vt põhjendus 139), võivad teatavad pädevad asutused (näiteks riiklik kuritegevusevastase võitluse amet) teataval tingimustel kasutada 2016. aasta uurimisvolituste seaduses sätestatud volitusi. Sellisel juhul kohaldatakse lisaks 2018. aasta andmekaitse seaduse 3. osas sätestatud kaitsemeetmetele ka 2016. aasta uurimisvolituste seaduses sätestatud kaitsemeetmeid. Luureteenistused (salaluureteenistus, julgeolekuteenistus ja valitsusside peakorter) ei ole 2018. aasta andmekaitseseaduse 3. osa kohaldamisalasse kuuluvad pädevad asutused ⁽¹³⁴⁾ ja seetõttu ei kohaldata nende tegevuse suhtes 2018. aasta andmekaitseseaduse 3. osas sätestatud norme. 2018. aasta andmekaitseseaduse 4. osa reguleerib isikuandmete töötlemist luureteenistuste poolt (vt põhjendus 125).

⁽¹²⁹⁾ Euroopa Inimõiguste Kohtu otsus kohtuasjas Kennedy vs. Ühendkuningriik, kaebuse nr 26839/05, (edaspidi „kohtuotsus Kennedy“), punktid 167 ja 190.

⁽¹³⁰⁾ Lisateavet Euroopa inimõiguste konventsiooni ja selle Ühendkuningriigi õigusesse kaasamise kohta 1998. aasta inimõiguste seaduse kaudu ning konventsiooni nr 108 kohta on esitatud põhjenduses 9.

⁽¹³¹⁾ Samamoodi on konventsiooni nr 108+ artikli 11 kohaselt teatavate konventsioonist tulenevate õiguste ja kohustuste piirangud riigi julgeoleku või süütegude ennetamise, uurimise ja nende eest vastutusele võtmise ning kriminaalkaristuste täideviimise eesmärgil lubatud üksnes siis, kui sellised piirangud on ette nähtud õigusaktidega, nendega austatakse põhiõiguste ja -vabaduste olemust ning nende näol on tegemist demokraatlikus ühiskonnas vajaliku ja proportsionaalse meetmega. Ka riigi julgeoleku ja riigikaitse eesmärgil tehtavate töötlemistoimingute suhtes peab konventsiooni asjaomase osalisriigi siseriikliku õiguse alusel kehtima sõltumatu ja tõhus läbivaatamine ja järelevalve.

⁽¹³²⁾ 2018. aasta andmekaitseseaduse paragrahv 31.

⁽¹³³⁾ 7. lisas loetletud pädevate asutuste hulka ei kuulu üksnes politseijõud, vaid ka kõik Ühendkuningriigi ministriumid ja teised uurimisülesannetega asutused (nt Ühendkuningriigi maksu- ja tolliameti volinik (Commissioner for Her Majesty's Revenue and Customs), riiklik kuritegevusevastase võitluse amet (National Crime Agency), Walesi maksu- ja tolliamet (Welsh Revenue Authority), konkurents- ja turuamet (Competition and Markets Authority) ja Ühendkuningriigi kinnistusregister (Her Majesty's Land Registry)), prokuratuuri organid, muud kriminaalõiguse asutused ja muud uurimisülesannetega isikud ja õiguskaitsega tegelevad organisatsioonid (nende seas on 2018. aasta andmekaitseseaduse 7. lisas nimetatud prokuratuuri direktorid, Põhja-Iirimaa prokuratuuri direktor ja teabevolinik).

⁽¹³⁴⁾ 2018. aasta andmekaitseseaduse paragrahvi 30 lõige 2.

(124) Sarnaselt direktiivile (EL) 2016/680 on 2018. aasta andmekaitseaduse 3. osas sätestatud seaduslikkuse ja õigluse, ⁽¹³⁵⁾ eesmärgi piirangu, ⁽¹³⁶⁾ võimalikult väheste andmete kogumise, ⁽¹³⁷⁾ õigsuse, ⁽¹³⁸⁾ säilitamise piirangu ⁽¹³⁹⁾ ja turvalisuse ⁽¹⁴⁰⁾ põhimõtted. Kehtestatud on konkreetsed läbipaistvuskohustused ⁽¹⁴¹⁾ ning üksikisikutele antud õigus andmetega tutvuda, ⁽¹⁴²⁾ neid parandada ja kustutada ⁽¹⁴³⁾ ja õigus, et nende kohta ei võeta vastu automatiseeritud otsust ⁽¹⁴⁴⁾. Samuti peavad pädevad asutused rakendama lõimitud andmekaitset ja vaikimisi andmekaitset, töötlemistoimingud dokumenteerima ning hindama teatavate töötlemistoimingute puhul andmekaitsealast mõju ja eelnevalt teabevolnikuga konsulteerima ⁽¹⁴⁵⁾. 2018. aasta andmekaitseaduse paragrahvi 56 kohaselt peavad nad tõendama, et täidavad nimetatud seaduse nõudeid. Lisaks peavad nad kehtestama asjakohased meetmed, et tagada isikuandmete töötlemise turvalisus, ⁽¹⁴⁶⁾ ning nende suhtes kehtivad konkreetsed kohustused andmetega seotud rikkumiste korral, mille hulka kuulub kohustus teavitada rikkumisest teabevolnikku ja andmesubjekti ⁽¹⁴⁷⁾. Nagu ka direktiivi (EL) 2016/680 puhul, peab vastutav töötleja (välja arvatud juhul, kui tegemist on kohtu või muu õigust mõistvat funktsiooni täitva õigusasutusega) määrama andmekaitseametniku, ⁽¹⁴⁸⁾ kes abistab vastutavat töötlejat nii tema kohustuste täitmisel kui ka nende täitmise üle järelevalve tegemisel ⁽¹⁴⁹⁾. Peale selle on 2018. aasta andmekaitseadusega kehtestatud erinõuded õiguskaitse eesmärkidel isikuandmete rahvusvahelise edastamise kohta kolmandatesse riikidesse või rahvusvahelistele organisatsioonidele, et tagada kaitse jätkumine ⁽¹⁵⁰⁾. Käesoleva otsusega samal kuupäeval võttis komisjon direktiivi (EL) 2016/680 artikli 36 lõike 3 alusel vastu kaitse piisavuse otsuse, milles järeldati, et Ühendkuningriigis kriminaalõiguskaitseasutustele kohaldatava andmekaitse korraga on tagatud kaitsetase, mis sisuliselt vastab direktiiviga (EL) 2016/680 tagatud kaitsetasemele.

(125) 2018. aasta andmekaitseaduse 4. osa kohaldatakse kogu andmete töötlemise suhtes, mida teevad luureteenistused või mida tehakse nende nimel. Eelkõige on selles sätestatud peamised andmekaitsepõhimõtted (seaduslikkus, õiglus ja läbipaistvus, ⁽¹⁵¹⁾ eesmärgi piirang, ⁽¹⁵²⁾ võimalikult väheste andmete kogumine, ⁽¹⁵³⁾ õigsus, ⁽¹⁵⁴⁾ säilitamise piirang ⁽¹⁵⁵⁾ ja turvalisus ⁽¹⁵⁶⁾), kehtestatud andmete eriliikide töötlemise tingimused ⁽¹⁵⁷⁾ ja andmesubjektide õigused, ⁽¹⁵⁸⁾ nõutud

⁽¹³⁵⁾ 2018. aasta andmekaitseaduse paragrahv 35.

⁽¹³⁶⁾ 2018. aasta andmekaitseaduse paragrahv 36.

⁽¹³⁷⁾ 2018. aasta andmekaitseaduse paragrahv 37.

⁽¹³⁸⁾ 2018. aasta andmekaitseaduse paragrahv 38.

⁽¹³⁹⁾ 2018. aasta andmekaitseaduse paragrahv 39.

⁽¹⁴⁰⁾ 2018. aasta andmekaitseaduse paragrahv 40.

⁽¹⁴¹⁾ 2018. aasta andmekaitseaduse paragrahv 44.

⁽¹⁴²⁾ 2018. aasta andmekaitseaduse paragrahv 45.

⁽¹⁴³⁾ 2018. aasta andmekaitseaduse paragrahvid 46 ja 47.

⁽¹⁴⁴⁾ 2018. aasta andmekaitseaduse paragrahvid 49 ja 50.

⁽¹⁴⁵⁾ 2018. aasta andmekaitseaduse paragrahvid 56–65.

⁽¹⁴⁶⁾ 2018. aasta andmekaitseaduse paragrahv 66.

⁽¹⁴⁷⁾ 2018. aasta andmekaitseaduse paragrahvid 67–68.

⁽¹⁴⁸⁾ 2018. aasta andmekaitseaduse paragrahvid 69–71.

⁽¹⁴⁹⁾ 2018. aasta andmekaitseaduse paragrahvid 67–68.

⁽¹⁵⁰⁾ 2018. aasta andmekaitseaduse 3. osa 5. peatükk.

⁽¹⁵¹⁾ 2018. aasta andmekaitseaduse paragrahvi 86 lõike 6 alusel tuleb töötlemise õigluse ja läbipaistvuse kindlakstegemiseks võtta arvesse andmete saamise meetodit. Sellega seoses on õigluse ja läbipaistvuse nõue täidetud, kui andmed saadakse isikult, kellel on seadusjärgselt luba või kohustus neid esitada.

⁽¹⁵²⁾ 2018. aasta andmekaitseaduse paragrahvi 87 alusel peab töötlemise eesmärk olema täpsustatud, sõnaselge ja seaduslik. Andmeid ei tohi töödelda viisil, mis ei ole kooskõlas nende kogumise eesmärkidega. 2018. aasta andmekaitseaduse paragrahvi 87 lõike 3 alusel võib isikuandmete täiendav eesmärgile vastav töötlemine olla lubatud üksnes juhul, kui vastutaval töötlejal on seadusjärgne luba andmeid sellel eesmärgil töödelda ning töötlemine on sellel eesmärgil vajalik ja proportsionaalne. Töötlemist tuleb käsitada eesmärgile vastavana siis, kui see hõlmab töötlemist avalikes huvides arhiveerimise eesmärgil, teadus- või ajaloouringute eesmärgil või statistilisel eesmärgil ning selle suhtes kehtivad asjakohased kaitsemeetmed (2018. aasta andmekaitseaduse paragrahvi 87 lõike 4).

⁽¹⁵³⁾ Isikuandmed peavad olema asjakohased ja olulised ega tohi olla ülemääraseks (2018. aasta andmekaitseaduse paragrahv 88).

⁽¹⁵⁴⁾ Isikuandmed peavad olema õiged ja ajakohased (2018. aasta andmekaitseaduse paragrahv 89).

⁽¹⁵⁵⁾ Isikuandmeid ei tohi säilitada kauem, kui on vajalik (2018. aasta andmekaitseaduse paragrahv 90).

⁽¹⁵⁶⁾ Kuuenda andmekaitsepõhimõtte kohaselt tuleb isikuandmeid töödelda viisil, mis hõlmab asjakohaste turvameetmete võtmist seoses isikuandmete töötlemisest tulenevate ohtudega. Need ohud hõlmavad isikuandmete juhuslikku või loata juurdepääsu või nende hävitamist, kaotamist, kasutamist, muutmist või avalikustamist (kuid ei piirdu sellega) (2018. aasta andmekaitseaduse paragrahv 91). Samuti on paragrahviga 107 ette nähtud, et 1) iga vastutav töötleja peab rakendama turvameetmeid, mis on isikuandmetele töötlemisega kaasnevate ohtude seisukohast asjakohased, ja 2) automatiseeritud töötlemise korral peab iga vastutav töötleja ja iga volitatud töötleja rakendama ohtude hindamisel põhinevaid ennetus- või leevendusmeetmeid.

⁽¹⁵⁷⁾ 2018. aasta andmekaitseaduse paragrahvi 86 lõike 2 punkt b ja 10. lisa.

⁽¹⁵⁸⁾ 2018. aasta andmekaitseaduse 4. osa 3. peatükk, eelkõige õigus andmetega tutvuda, neid parandada ja kustutada, õigus töötlemine vaidlustada ja õigus, et andmesubjekti kohta ei võeta vastu automatiseeritud otsust, õigus sekkuda automatiseeritud otsuste tegemisse ning õigus olla otsuste tegemisest teavitatud. Lisaks peab vastutav töötleja andma andmesubjektile teavet tema isikuandmete töötlemise kohta. Nagu on selgitatud teabevolniku suunistes isikuandmete töötlemise kohta luureteenistuste poolt, saavad üksikisikud teostada kõiki oma õigusi (sealhulgas taotleda andmete parandamist), kui esitavad kaebuse teabevolnikule või pöörduvad kohtusse (vt teabevolniku suunistes luureteenistuste andmetöötlemise kohta, kättesaadavad aadressil <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/>).

lõimitud andmekaitset ⁽¹⁵⁹⁾ ja reguleeritud isikuandmete rahvusvaheline edastamine ⁽¹⁶⁰⁾. Teabevolnik andis hiljuti välja põhjalikud suunised isikuandmete töötlemise kohta luureteenistuste poolt 2018. aasta andmekaitseaduse 4. osa kohaselt ⁽¹⁶¹⁾.

- (126) Samal ajal on 2018. aasta andmekaitseaduse paragrahviga 110 nähtud ette erand 2018. aasta andmekaitseaduse 4. osa sätetest, ⁽¹⁶²⁾ kui selline erand on vajalik riigi julgeoleku kaitsmiseks. Sellele erandile tuginemiseks tuleb iga juhtumit eraldi analüüsida ⁽¹⁶³⁾. Nagu Ühendkuningriigi ametiasutused selgitasid ja nagu kinnitab kohtupraktika, „tuleb vastutaval töötlejal kaaluda tegelikke tagajärgi riigi julgeolekule või riigikaitsele juhul, kui ta peab konkreetset andmekaitseäset järgima, ning seda, kas ta saaks mõistlikult järgida tavapäraseid norme, ilma et see mõjutaks riigi julgeolekut või riigikaitset“ ⁽¹⁶⁴⁾. Selle üle, kas erandit kasutati nõuetekohaselt, teeb järelevalvet teabevolnik ⁽¹⁶⁵⁾.
- (127) Mis puudutab võimalust piirata „riigi julgeoleku“ kaitsmise eesmärgil nimetatud sätete kohaldamist, siis võib vastutav töötleja 2018. aasta andmekaitseaduse paragrahvi 111 järgi taotleda kabinetiministri või peaprokuröri (Attorney General) allkirjastatud sertifikaati, mis kinnitab, et selliste õiguste piiramine on riigi julgeoleku kaitsmiseks vajalik ja proportsionaalne meede ⁽¹⁶⁶⁾.
- (128) Ühendkuningriigi valitsus on andnud välja suunised, et aidata vastutavaid töötlejaid selle kaalumisel, kas kohaldada 2018. aasta andmekaitseaduse alusel riigi julgeoleku sertifikaati; suunistes on eelkõige rõhutatud, et andmesubjektide õiguste piiramine riigi julgeoleku kaitsmise eesmärgil peab olema proportsionaalne ja vajalik ⁽¹⁶⁷⁾. Kõik riigi julgeoleku sertifikaadid tuleb avaldada teabevolniku veebisaidil ⁽¹⁶⁸⁾.

⁽¹⁵⁹⁾ 2018. aasta andmekaitseaduse paragrahv 103.

⁽¹⁶⁰⁾ 2018. aasta andmekaitseaduse paragrahv 109. Isikuandmete edastamine rahvusvahelistele organisatsioonidele või väljaspool Ühendkuningriiki asuvatele riikidele on võimalik juhul, kui edastamine on vajalik ja proportsionaalne meede, mis võetakse vastutava töötleja seadusjärgsete ülesannete täitmiseks või muul 1989. aasta julgeolekuteenistuse seaduse ja 1994. aasta luureteenistuste seaduse konkreetsetes paragrahvides sätestatud eesmärgil.

⁽¹⁶¹⁾ Teabevolniku suunised, vt joonealune märkus nr 158.
2018. aasta andmekaitseaduse paragrahv 30 ja 7. lisa.

⁽¹⁶²⁾ 2018. aasta andmekaitseaduse paragrahvis 110 lõikes 2 on loetletud sätted, millest võib erandi teha. Nende hulka kuuluvad andmekaitsepõhimõtted (välja arvatud seaduslikkuse põhimõte), andmesubjekti õigused, kohustus teavitada teabevolnikku andmetega seotud rikkumisest, teabevolniku kontrollivõimused kooskõlas rahvusvaheliste kohustustega, teabevolniku teatavad õigusnormide täitmise tagamise volitused, sätted, mille kohaselt on teatavad andmekaitsega seotud rikkumised süüteod, ning sätted, mis käsitlevad andmete töötlemise eesesmärke, nagu ajakirjanduslikud, akadeemilised või kunstilised eesmärgid.

⁽¹⁶³⁾ Vt kohtuotsus Baker vs. Secretary of State, vt joonealune märkus nr 61.

⁽¹⁶⁴⁾ „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu H: „National Security Data Protection and Investigatory Powers Framework“ (Riigi julgeolekuga seotud andmekaitse ja uurimisvolituste raamistik), lk 15–16 (vt joonealune märkus nr 31). Vt ka kohtuotsus Baker vs. Secretary of State (vt joonealune märkus nr 61), milles kohus tühistas siseministri väljastatud riigi julgeoleku sertifikaadi ja kinnitas riigi julgeolekuga seotud erandi kohaldamist, kuna puudus põhjus kehtestada üldine erand kohustusest vastata juurdepääsutaotlustele ning sellise erandi lubamine kõikidel asjaoludel ilma iga juhtumit eraldi analüüsivata ületas seda, mis on riigi julgeoleku kaitsmiseks vajalik ja proportsionaalne.

⁽¹⁶⁵⁾ Vt teabevolniku ja Ühendkuningriigi luureühenduse vaheline vastastikuse mõistmise memorandum, kus on öeldud: „Kui teabevolnik saab andmesubjektilt kaebuse, soovib ta kontrollida, kas küsimust on käsitletud õigesti, ja vajaduse korral seda, kas erandit on kohaldatud nõuetekohaselt.“ Teabevolniku büroo ja Ühendkuningriigi luureasutuste vaheline vastastikuse mõistmise memorandum, punkt 16, kättesaadav aadressil <https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf>.

⁽¹⁶⁶⁾ 2018. aasta andmekaitseadusega on kaotatud võimalus anda välja sertifikaate 1998. aasta andmekaitseaduse paragrahvi 28 lõike 2 alusel. Ent võimalus anda välja nn vanu sertifikaate kehtib edasi juhul, kui õiguste piiramine vaidlustatakse 1998. aasta seaduse kohaselt (vt 2018. aasta andmekaitseaduse 20. lisa 5. osa paragrahv 17). Seda võimalust saab aga kasutada väga harva ja seda kohaldatakse vähestel juhtudel, näiteks siis, kui andmesubjekt vaidlustab riigi julgeoleku erandi kasutamise avaliku sektori asutuse poolse andmetöötlemise suhtes, kui avaliku sektori asutus töötleb andmeid 1998. aasta seaduse alusel. Tuleb märkida, et sellistel juhtudel kohaldatakse 1998. aasta andmekaitseaduse paragrahvi 28 tervikuna, kaasa arvatud andmesubjekti õigust sertifikaati kohtus vaidlustada.

⁽¹⁶⁷⁾ „UK Government Guidance on National Security Certificates under the Data Protection Act 2018“ (Ühendkuningriigi valitsuse suunised 2018. aasta andmekaitseaduse kohaste riigi julgeoleku sertifikaatide kohta), kättesaadavad aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. Ühendkuningriigi ametiasutuste esitatud selgituse kohaselt on sertifikaat küll veenev tõend selle kohta, et erand on sertifikaadil kirjeldatud andmete või töötlemise suhtes kohaldatav, kuid see ei kõrvalda nõuet, et vastutav töötleja peab kaaluma erandi kohaldamise vajadust iga juhtumi puhul eraldi.

⁽¹⁶⁸⁾ Teabevolnik võib 2018. aasta andmekaitseaduse paragrahvi 130 kohaselt otsustada sertifikaadi teksti või osa sertifikaadi tekstist mitte avaldada, kui see oleks vastuolus riigi julgeoleku huvidega või avaliku huviga või võib seada ohtu inimeste turvalisuse. Sellisel juhul peab teabevolnik aga avaldama teate selle kohta, et sertifikaat on välja antud.

- (129) Sertifikaadil peaks olema kindlaksmääratud kehtivusaeg, mis ei ületa viit aastat, seega peab täitevvõim selle regulaarselt läbi vaatama⁽¹⁶⁹⁾. Sertifikaadile märgitakse nii isikuandmed või isikuandmete kategooriad kui ka 2018. aasta andmekaitseaduse sätteid, mille suhtes erandit kohaldatakse⁽¹⁷⁰⁾.
- (130) On oluline mainida, et riigi julgeoleku sertifikaat ei kujuta endast lisaalust andmekaitseõiguste piiramiseks riigi julgeolekuga seotud põhjustel. Teiste sõnadega võib vastutav töötleja või volitatud töötleja sertifikaadile tugineda üksnes siis, kui ta on teinud järelduse, et riigi julgeoleku erandi kasutamine on vajalik, mida tuleb teha iga juhtumi puhul eraldi, nagu eespool selgitatud⁽¹⁷¹⁾. Isegi kui asjaomase küsimuse suhtes kohaldatakse riigi julgeoleku sertifikaati, võib teabevinik uurida, kas riigi julgeoleku erandile tuginemine oli konkreetsel juhul põhjendatud⁽¹⁷²⁾.
- (131) Iga isik, keda sertifikaadi väljastamine otseselt mõjutab, võib kõrgemale kohtule (Upper Tribunal)⁽¹⁷³⁾ sertifikaadi suhtes kaebuse esitada⁽¹⁷⁴⁾ või juhul, kui sertifikaadil on andmed kindlaks tehtud üldise kirjeldusena, siis vaidlustada sertifikaadi kohaldamise konkreetsete andmete suhtes⁽¹⁷⁵⁾. Kohus vaatab sertifikaadi väljastamise otsuse läbi ja otsustab, kas sertifikaat väljastati mõistlikel alustel⁽¹⁷⁶⁾. Kohus võib kaaluda mitmesuguseid küsimusi, sealhulgas vajalikkust, proportsionaalsust ja seaduslikkust, võttes arvesse mõju andmesubjektide õigustele ja viies selle tasakaalu vajadusega kaitsta riigi julgeolekut. Selle tulemusel võib kohus otsustada, et sertifikaati ei kohaldata konkreetsete isikuandmete suhtes, mille kohta kaebus esitati⁽¹⁷⁷⁾.
- (132) Erinevat kogumit võimalikke piiranguid kohaldatakse 2018. aasta andmekaitseaduse 11. lisa alusel 2018. aasta andmekaitseaduse 4. osa teatavate sätete suhtes,⁽¹⁷⁸⁾ et kaitsta muid üldist avalikku huvi pakkuvaid olulisi eesmärke või kaitstud huve, nagu parlamentaarne puutumatus, kutsesaladus, kohtumenetluste läbiviimine või relvajõudude lahinguvõime⁽¹⁷⁹⁾. Nende sätete kohaldamise puhul on tehtud erand kas teatavate teabeliikide suhtes (nn kategooriapõhine) või sel määral, mil nende sätete kohaldamine tõenäoliselt kahjustaks kaitstud huvi (nn kahjupõhine)⁽¹⁸⁰⁾. Kahjupõhistele eranditele saab tugineda üksnes sel määral, mil loetletud andmekaitse sätte

⁽¹⁶⁹⁾ „UK Government Guidance on National Security Certificates“ (Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta), punkt 15, vt joonealune märkus nr 167.

⁽¹⁷⁰⁾ „UK Government Guidance on National Security Certificates“ (Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta), punkt 5, vt joonealune märkus nr 167.

⁽¹⁷¹⁾ Vt joonealune märkus nr 164.

⁽¹⁷²⁾ 2018. aasta andmekaitseaduse paragrahvi 102 kohaselt peab vastutav töötleja suutma tõendada, et ta täitis 2018. aasta andmekaitseaduse nõudeid. See tähendab seda, et luureteenistus peab teabevinikule tõendama, et ta on erandile tuginemise korral kaalunud juhtumi konkreetseid asjaolusid. Samuti avaldab teabevinik riigi julgeoleku sertifikaatide andmed, mis on kättesaadavad aadressil <https://ico.org.uk/about-the-ico/our-information/national-security-certificates/>.

⁽¹⁷³⁾ Kõrgem kohus on pädev ära kuulama madalama astme halduskohtute otsuste peale esitatud kaebusi ja tal on eripädevus seoses teatavate valitsusasutuste otsuste peale esitatud otsekaebustega.

⁽¹⁷⁴⁾ 2018. aasta andmekaitseaduse paragrahvi 111 lõige 3.

⁽¹⁷⁵⁾ 2018. aasta andmekaitseaduse paragrahvi 111 lõige 5.

⁽¹⁷⁶⁾ Kohtuotsuses Baker vs. Secretary of State (vt joonealune märkus nr 61) tühistas teabeküsimuste kohus siseministri väljastatud riigi julgeoleku sertifikaadi, kuna puudus põhjus näha ette üldine erand kohustusest vastata juurdepääsutaotlustele ning sellise erandi lubamine kõikidel asjaoludel ilma iga juhtumit eraldi analüüsivata ületas seda, mis on riigi julgeoleku kaitsmiseks vajalik ja proportsionaalne.

⁽¹⁷⁷⁾ „UK Government Guidance on National Security Certificates“ (Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta), punkt 25, vt joonealune märkus nr 167.

⁽¹⁷⁸⁾ Nende hulka kuuluvad: i) 4. osas sisalduvad andmekaitsepõhimõtted, välja arvatud esimese põhimõtte kohane andmete töötlemise seaduslikkuse nõue ja asjaolu, et töötlemine peab vastama ühele 9. ja 10. lisa sätestatud asjaomasele tingimusele, ii) andmesubjektide õigused ja iii) kohustused seoses teabevinikule rikkumistest teatamisega.

⁽¹⁷⁹⁾ 2018. aasta andmekaitseaduse 4. osas on sätestatud õiguslik raamistik, mida kohaldatakse kõigi luureteenistuste tehtavate andmetöötlustoimingute suhtes (mitte ainult selliste toimingute suhtes, mida nad teevad riigi julgeolekuga seotud ülesannete raames). Seetõttu kohaldatakse 4. osa ka siis, kui luureteenistused töötlevad isikuandmeid näiteks personalihalduse valdkonnas, seoses kohtumenetluse või riigihangetega, 11. lisa loetletud piirangud on mõeldud peamiselt selleks, et neid kohaldataks sellistes olukordades. Näiteks, kui tegu on kohtuvaidlusega töötaja vastu, võidakse tugineda piirangule seoses „kohtumenetlusega“, ja kui tegu on riigihanakemenetlusega, võidakse tugineda piirangule seoses „lääbiraäkimisega“, jne. Seda on mainitud ka teabeviniku suunistes isikuandmete töötlemise kohta luureteenistuste poolt, kus 11. lisa piirangute kohaldamise näitena on nimetatud läbiraäkimisi luureasutuse ja selle endise töötaja vahel, kes on esitanud tööõiguse alase nõude (vt joonealune märkus nr 161). Samuti tuleks märkida, et 2018. aasta andmekaitseaduse 2. osa 2. lisa järgi saavad samu piiranguid kasutada teised avaliku sektori asutused.

⁽¹⁸⁰⁾ Ühendkuningriigi selgitava raamistiku kohaselt on nn kategooriapõhised erandid järgmised: i) teave riiklike teenetemärkide ja aunimetuste andmise kohta, ii) kutsesaladus, iii) konfidentsiaalsed töö-, koolitus- ja haridusalased soovituskirjad ja iv) eksamitööd ja -hinded. Nn kahjupõhised erandid on seotud järgmistega küsimustega: i) kuriteo ennetamine või avastamine, õigusrikkujate kinnipidamine ja vastutusele võtmine, ii) parlamentaarne puutumatus, iii) kohtumenetlused, iv) riigi relvajõudude lahinguvõime, v) Ühendkuningriigi majanduslik heaolu, vi) läbiraäkimised andmesubjektiga, vii) teadus- või ajaloouringutega seotud või statistilised eesmärgid, viii) avalikes huvides toimuv arhiveerimine. „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu H: „National Security“ (Riigi julgeolek), lk 13, vt joonealune märkus nr 31.

kohaldamine tõenäoliselt kahjustaks kõnealust konkreetset huvi. Seepärast peab erandi kasutamist alati põhjendama, osutades asjaomasele kahjule, mis konkreetse juhtumi puhul tõenäoliselt esineks. Kategooriapõhistele eranditele saab tugineda üksnes seoses konkreetse kitsalt määratletud teabeliigiga, mille suhtes erandit võimaldatakse. Oma eesmärgilt ja mõjult on need sarnased Ühendkuningriigi isikuandmete kaitse üldmääruse mitme erandiga (2018. aasta andmekaitseseaduse 2. lisa alusel), mis omakorda vastavad isikuandmete kaitse üldmääruse artikliga 23 ette nähtud eranditele.

- (133) Eespool kirjeldatust ilmneb, et Ühendkuningriigi kohaldatavate õigusnormide alusel on kehtestatud piirangud ja tingimused, mida on tõlgendanud ka kohtud ja teabevolnik ja millega tagatakse, et kõnealused erandid ja piirangud jäävad selle piiresse, mis on riigi julgeoleku kaitse seisukohast vajalik ja proportsionaalne.

3.2. Juurdepääs andmetele ja andmete kasutamine Ühendkuningriigi avaliku sektori asutuste poolt kriminaalõiguskaitse eesmärkidel

- (134) Ühendkuningriigi õigusega on kehtestatud mitu piirangut seoses isikuandmetega tutvumise ja nende kasutamisega kriminaalõiguskaitse eesmärkidel ning nähtud selles valdkonnas ette järelevalve- ja õiguskaitsemehhanismid, mis on kooskõlas käesoleva otsuse põhjendustes 113–115 osutatud nõuetega. Tingimusi, mille korral andmetega võib tutvuda, ning kõnealuste volituste kasutamise suhtes kohaldatavaid kaitsemeetmeid on üksikasjalikult hinnatud järgnevatel punktides.

3.2.1. Õiguslikud alused ja kohaldatavad piirangud/kaitsemeetmed

- (135) 2018. aasta andmekaitseseaduse paragrahvi 35 alusel tagatud seaduslikkuse põhimõtte kohaselt on isikuandmete töötlemine õiguskaitsega seotud eesmärgil seaduslik üksnes siis, kui see põhineb õigusaktil ning andmesubjekt on andnud nõusoleku andmete sel eesmärgil töötlemiseks ⁽¹⁸¹⁾ või on töötlemine vajalik seoses ülesandega, mida pädev asutus sel eesmärgil täidab.

3.2.1.1. Läbiotsimismäärused ja andmeesitamismäärused

- (136) Ühendkuningriigi õigusraamistikus on ettevõtjalt, sealhulgas kehtiva kaitse piisavuse otsuse alusel EList edastatud andmeid töötlevatelt ettevõtjalt lubatud kriminaalõiguskaitse eesmärkidel isikuandmeid koguda läbiotsimismääruste ⁽¹⁸²⁾ ja andmeesitamismääruste alusel ⁽¹⁸³⁾.
- (137) Läbiotsimismäärusi annavad välja kohtud uurija taotlusel. Need võimaldavad uurijal ruumidesse siseneda, et otsida oma uurimise jaoks asjakohaseid materjale või isikuid ning võtta hoiule kõik, mida läbiotsimisluba hõlmab, sealhulgas asjakohased isikuandmeid sisaldavad dokumendid ja materjalid ⁽¹⁸⁴⁾. Andmeesitamismääruse kohaselt, mille peab samuti välja andma kohus, peab määruses märgitud isik esitama tema

⁽¹⁸¹⁾ Kaitse piisavuse kontekstis ei tundu nõusolek olevat asjakohane, sest andmete edastamise korral ei ole Ühendkuningriigi õiguskaitseasutus kogunud andmeid otse ELi andmesubjektilt tema nõusoleku põhjal.

⁽¹⁸²⁾ Asjakohase õigusliku aluse kohta vt 1984. aasta politsei- ja kriminaaltõendite seaduse (Police and Criminal Evidence Act 1984) paragrahv 8 jj (Inglismaa ja Walesi puhul), 1989. aasta politsei- ja kriminaaltõendite määruse (Põhja-Iirimaa) paragrahv 10 jj ning Šotimaa puhul tuleneb õiguslik alus üldisest õigusest (vt 2016. aasta kriminaalõiguse seaduse (Šotimaa) (Criminal Justice (Scotland) Act 2016) paragrahv 46 ja konsolideeritud kriminaalseaduse (Šotimaa) paragrahv 23B). Kui läbiotsimismäärus on tehtud pärast vahistamist, on õiguslik alus 1984. aasta politsei- ja kriminaaltõendite seaduse paragrahv 18 (Inglismaa ja Walesi puhul), 1989. aasta politsei- ja kriminaaltõendite määruse (Põhja-Iirimaa) paragrahv 20 jj ning Šotimaa puhul tuleneb õiguslik alus üldisest õigusest (vt 2016. aasta kriminaalõiguse seaduse (Šotimaa) paragrahv 46). Ühendkuningriigi ametiasutused selgitasid, et läbiotsimismäärusi annavad välja kohtud uurija taotlusel. Need võimaldavad uurijal ruumidesse siseneda, et otsida oma uurimise jaoks asjakohaseid materjale või isikuid, ja määruse täitmisele on sageli vaja politseikonstaabli abi.

⁽¹⁸³⁾ Kui uurimine puudutab rahapesu (sealhulgas konfiskeerimismenetlusi ja tsiviilkohtumenetlusega väljanõudmisi), on andmeesitamismääruse kohaldamise asjakohased õiguslikud alused 2002. aasta kriminaaltulu seaduse (Proceeds of Crime Act 2002) paragrahv 345 jj Inglismaa, Walesi ja Põhja-Iirimaa puhul ning paragrahv 380 jj Šotimaa puhul. Kui uurimine käsitleb muid valdkondi kui rahapesu, võib andmeesitamismäärust taotleda 1984. aasta politsei- ja kriminaaltõendite seaduse paragrahvi 9 ja 1. lisa alusel Inglismaa ja Walesi puhul ning 1989. aasta politsei- ja kriminaaltõendite määruse (Põhja-Iirimaa) paragrahvi 10 jj alusel Põhja-Iirimaa puhul. Šotimaa puhul saadakse määrus üldise õiguse alusel (vt 2016. aasta kriminaalõiguse seaduse (Šotimaa) paragrahv 46) ja konsolideeritud kriminaalseaduse (Šotimaa) paragrahvi 23B alusel. Ühendkuningriigi ametiasutused selgitasid, et andmeesitamismääruse kohaselt peab määruses märgitud isik esitama tema valduses või kontrolli all oleva materjali või võimaldama sellele juurdepääsu (vt 1984. aasta politsei- ja kriminaaltõendite seaduse 1. lisa lõige 4).

⁽¹⁸⁴⁾ Näiteks hõlmavad 1984. aasta politsei- ja kriminaaltõendite seaduse paragrahvid 8 ja 18 volitusi arestida ja võtta hoiule kõik, mida läbiotsimisluba hõlmab.

valduses või kontrolli all oleva materjali või võimaldama sellele juurdepääsu. Taotleja peab kohtule põhjendama nii seda, miks määrus on vajalik, kui ka seda, miks see on avalikes huvides. Läbiotsimismääruste ja andmeesitamismääruste väljaandmine on lubatud mitmete seadusjärgsete volituste alusel. Iga sätte puhul kehtib kogum seadusjärgseid tingimusi, mis peavad läbiotsimismääruse⁽¹⁸⁵⁾ või andmeesitamismääruse⁽¹⁸⁶⁾ väljaandmiseks täidetud olema.

- (138) Andmeesitamismäärusi ja läbiotsimismäärusi saab kohtuliku kontrolli teel vaidlustada⁽¹⁸⁷⁾. Mis puudutab kaitsemeetmeid, siis võivad kõik 2018. aasta andmekaitseseaduse 3. osa kohaldamisalasasse kuuluvad kriminaalõiguskaitseasutused isikuandmetega tutvuda (mis on üks töötlemise vorm) üksnes kooskõlas 2018. aasta andmekaitseseaduses sätestatud põhimõtete ja nõuetega (vt põhjendused 122–124). Seepärast

⁽¹⁸⁵⁾ Näiteks on politsei- ja kriminaalteenuste seaduse paragrahviga 8 ja 18 reguleeritud vastavalt kohtuniku volitused läbiotsimismääruse lubamiseks ja politseiametniku volitused omand läbi otsida. Esimesel juhul (paragrahv 8) peab kohtunik enne läbiotsimismääruse väljaandmist kõigepealt veenduma, et on mõistlik alus arvata, et i) toime on pandud kuritegu, ii) ruumides on materjali, millel tõenäoliselt on süüte uurimise seisukohast oluline väärtus (kas omaette või koos muude materjalidega), iii) selle materjali puhul on tõenäoliselt tegemist asjakohase tõendiga, iv) see ei sisalda ega hõlma esemeid, mille suhtes kehtib kutsesaladus, välja jäetud materjale ega erimenetluse materjale ja v) ilma läbiotsimismääruse taotlemisest pääseda. Teisel juhul on politseiametnikul paragrahvi 18 järgi lubatud otsida kuriteo eest vahistatud isiku ruumidest materjale, mille suhtes ei kehti kutsesaladus, kui tal on mõistlik alus kahtlustada, et ruumides on tõendeid kõnealuse kuriteo või mõne muu sarnase või seotud kuriteo kohta. Selline läbiotsimine peab piirduma kõnealuse materjali otsimisega ja selleks peab olema vähemalt inspektori ametikohal töötava politseiametniku kirjalik luba, välja arvatud juhul, kui see on vajalik kuriteo uurimiseks. Sellisel juhul tuleb vähemalt inspektori ametikohal töötavat politseiametnikku pärast läbiotsimise tegemist niipea kui võimalik teavitada. Läbiotsimise alused ja otsitavate tõendite laad tuleb dokumenteerida. Peale selle on 1984. aasta politsei- ja kriminaalteenuste seaduse paragrahvidega 15 ja 16 ette nähtud seadusjärgsed kaitsemeetmed, mida tuleb läbiotsimismääruse taotlemisel järgida. Paragrahvis 15 on täpsustatud läbiotsimismääruse saamisel kohaldatavad tingimused (sealhulgas konstaabli esitatava taotluse sisu ja asjaolu, et määruks tuleb muu hulgas nimetada seadus, mille alusel see välja antakse, ja teha võimalikult ulatuslikult kindlaks otsitavad esemed ja isikud ning läbiotsitavad ruumid). Paragrahviga 16 on reguleeritud see, kuidas tuleb määruks kohane läbiotsimine läbi viia (näiteks on paragrahvi 16 lõikega 5 ette nähtud, et määrust täitev ametnik esitab ruumide kasutajale määruks koopia, paragrahvi 16 lõikes 11 on sätestatud, et pärast täitmist tuleb määrust 12 kuu pikkuse ajavahemiku jooksul säilitada, paragrahvi 16 lõikega 12 on ruumide kasutajale antud õigus määruks selle ajavahemiku jooksul soovi korral tutvuda). Need paragrahvid aitavad tagada vastavuse Euroopa inimõiguste konventsiooni artiklile 8 (vt nt kohtuotsus *Kent Pharmaceuticals vs. Director of the Serious Fraud Office*, [2002], EWHC 3023 (QB), [30], Lord Woolf CJ). Nende kaitsemeetmete järgimata jätmise tulemusel võidakse läbiotsimine kuulutada ebaseaduslikuks (selle näited on muu hulgas kohtuotsus *R (Brook) vs. Preston Crown Court*, [2018], EWHC 2024 (Admin), [2018], ACD 95; kohtuotsus *R (Superior Import / Export Ltd) vs. Revenue and Customs Commissioners*, [2017], EWHC, 3172 (Admin), [2018], Lloyd's Rep FC 115, ja kohtuotsus *R (F) vs. Blackfriars Crown Court*, [2014], EWHC 1541 (Admin)). 1984. aasta politsei- ja kriminaalteenuste seaduse paragrahve 15 ja 16 täiendab politsei- ja kriminaalteenuste seaduse juhend B – tegevusjuhend, millega on reguleeritud politseivolituste teostamine ruumide läbiotsimisel.

⁽¹⁸⁶⁾ Näiteks kui andmeesitamismäärus antakse välja 2002. aasta kriminaaltulu seaduse alusel, peab lisaks mõistlikule alusele arvata, et täidetud on kriminaaltulu seaduse punkti 346 alapunktis 2 sätestatud tingimused, olema ka mõistlik alus arvata, et kõnealune materjal on isiku valduses või kontrolli all ning et sellel materjalil on tõenäoliselt oluline väärtus. Veel üks andmeesitamismääruse väljaandmise tingimus on see, et peab olema mõistlik alus arvata, et materjali esitamine või sellele juurdepääsu saamine on avalikes huvides, võttes arvesse a) tõenäolist kasu uurimise jaoks materjali saamise korral ja b) asjaolusid, millel taotluses märgitud isik, kelle valduses või kontrolli all asjaomane materjal tundub olevat, seda teavet omab. Samamoodi peab kohus, kes kaalub 1984. aasta politsei- ja kriminaaltulu seaduse 1. lisa kohase andmeesitamismääruse taotlust, olema veendunud, et täidetud on konkreetsed tingimused. Eelkõige on politsei- ja kriminaaltulu seaduse 1. lisa sätestatud kaks eraldi alternatiivset tingimuste kogumit, millest üks peab olema täidetud, enne kui kohtunik saab andmeesitamismääruse välja anda. Esimese tingimuste kogumiga nõutakse, et kohtunikul on mõistlik alus arvata, et i) sooritatud on kuritegu, ii) ruumides otsitav materjal sisaldab või hõlmab erimenetluse materjale, kuid mitte välja jäetud materjale, iii) sellel on uurimise seisukohast tõenäoliselt oluline väärtus kas omaette või koos muude materjalidega iv) ja selle puhul on tõenäoliselt tegemist asjakohase tõendiga, v) materjali on püütud saada muul viisil või ei ole seda püütud, sest see ei oleks tulemuslik, ja vi) võttes arvesse kasu uurimise jaoks ja asjaolusid, mille tõttu materjal isiku valduses on, on materjali esitamine või sellele juurdepääsu saamine avalikes huvides. Teise tingimuste kogumiga nõutakse järgmist: i) ruumides on materjal, mis koosneb erimenetluse materjalidest või välja jäetud materjalidest, ii) kui enne politsei- ja kriminaaltulu seadust vastu võetud õigusaktide põhjal toimuvad erimenetluste materjalide, välja jäetud materjalide ja kutsesaladusega hõlmatud materjalidega seotud läbiotsimised ei oleks keelatud, siis oleks saanud selle materjali kohta läbiotsimismääruse välja anda ja iii) see oleks olnud asjakohane.

⁽¹⁸⁷⁾ Kohtulik kontroll on kohtumenetlus, mille raames saab avaliku sektori asutuse otsuse kõrges kohtus (High Court) vaidlustada. Kohtud kontrollivad vaidlustatud otsust ja otsustavad, kas avaliku õiguse mõisteid/põhimõtteid arvesse võttes saab väita, et otsus on õiguslikult ebakorrektn. Kohtuliku kontrolli peamised alused on eelkõige ebaseaduslikkus, ebaratsionaalsus, menetlusnormide rikkumine, õiguspärased ootused ja inimõigused. Pärast edukat kohtulikku kontrolli saab kohus kasutada mitmesuguseid õiguskaitsevahendeid, millest kõige levinum on tühistamiskorraldus (millega jäetakse algne otsus, st läbiotsimismääruse väljaandmise otsus kõrvale või see tühistatakse), mis võib teataval asjaoludel hõlmata ka rahalise hüvitise määramist. Täiendavad üksikasjad kohtuliku kontrolli kohta Ühendkuningriigis on esitatud valitsuse õigusosakonna väljaandes „Judge Over Your Shoulder – a guide to good decision-making“ (Kohtunik sinu kõrval – heade otsuste tegemise juhend), kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

peab õiguskaitseasutuse taotlus vastama põhimõttele, mille kohaselt peavad töötlemise eesmärgid olema täpsustatud, sõnaselged ja seaduslikud⁽¹⁸⁸⁾ ning isikuandmed, mida pädev asutus töötleb, peavad olema selle eesmärgi jaoks asjakohased ega tohi olla ülemääraseks⁽¹⁸⁹⁾.

3.2.1.2. Õiguskaitse eesmärkidega seotud uurimisvolitused

- (139) Üksnes raskete kuritegude ennetamise või avastamise eesmärgil⁽¹⁹⁰⁾ võivad mõned õiguskaitseasutused, näiteks riiklik kuritegevusevastase võitluse amet ja politsei ameti juht,⁽¹⁹¹⁾ kasutada 2016. aasta uurimisvolituste seaduse alusel suunatud uurimisvolitusi. Sellisel juhul kohaldatakse lisaks 2018. aasta andmekaitse seaduse 3. osas sätestatud kaitsemeetmetele ka 2016. aasta uurimisvolituste seaduses sätestatud kaitsemeetmeid. Need õiguskaitseasutused võivad kasutada järgmisi uurimisvolitusi: suunatud pealtkuulamine (2016. aasta uurimisvolituste seaduse 2. osa), sideandmete hankimine (2016. aasta uurimisvolituste seaduse 3. osa), sideandmete säilitamine (2016. aasta uurimisvolituste seaduse 4. osa) ja suunatud sekkumine seadmete töösse (2016. aasta uurimisvolituste seaduse 5. osa). Pealtkuulamine hõlmab side sisu hankimist,⁽¹⁹²⁾ samal ajal kui sideandmete hankimise ja säilitamise eesmärk ei ole saada side sisu, vaid vastus sellele, kes, millal, kus ja kuidas suhtles. See hõlmab näiteks side aega ja kestust, side algataja ja adressaadi telefoninumbrit või e-posti aadressi ning mõnikord kasutatud sidevahendite asukohta, telefoniteenuse abonenti või üksikasjalikku arvet⁽¹⁹³⁾. Seadmete töösse sekkumise (*equipment interference*) näol on tegemist tehnikate kogumiga, mida kasutatakse mitmesuguste andmete saamiseks muu hulgas sellistest seadmetest nagu arvutid, tahvelarvutid ja nutitelefoniid, aga ka kaablid, juhtmed ja salvestusseadmed⁽¹⁹⁴⁾.
- (140) Suunatud pealtkuulamisvolitusi võib kasutada ka siis, kui see on „vajalik vastastikust abi käsitleva ELi õigusakti või vastastikust abi käsitleva rahvusvahelise lepingu sätete täitmiseks“ (nn vastastikuse abiga seotud luba⁽¹⁹⁵⁾). Vastastikuse abiga seotud lube antakse ainult pealtkuulamiseks, mitte sideandmete hankimiseks ega seadmete töösse sekkumiseks. Need suunatud volitused on reguleeritud 2016. aasta uurimisvolituste seadusega,⁽¹⁹⁶⁾ mis moodustab koos Inglismaa, Walesi ja Põhja-Iirimaa puhul 2000. aasta uurimisvolituste reguleerimise seadusega ja Šotimaa puhul 2000. aasta uurimisvolituste reguleerimise seadusega (Šotimaa) õigusliku aluse ning milles on sätestatud selliste volituste kasutamise suhtes kohaldatavad piirangud ja kaitsemeetmed. Samuti on 2016. aasta uurimisvolituste seadusega ette nähtud massiliste uurimisvolituste kasutamine, kuigi neid ei saa kasutada õiguskaitseasutused, vaid ainult luureasutused⁽¹⁹⁷⁾.

⁽¹⁸⁸⁾ Ühendkuningriigi 2018. aasta andmekaitse seaduse paragrahvi 36 lõige 1.

⁽¹⁸⁹⁾ Ühendkuningriigi 2018. aasta andmekaitse seaduse paragrahv 37.

⁽¹⁹⁰⁾ 2016. aasta andmekaitse seaduse paragrahvi 263 lõikes 1 on sätestatud, et „raske kuritegu“ tähendab süütegu, mille puhul võib mõistlikult eeldada, et täiskasvanule, keda ei ole varem süüdi mõistetud, võib selle eest määrata vähemalt kolme aasta pikkuse vangistuse, või mille toimepanekul kasutatakse vägivalda, mille tulemusel saadakse olulist rahalist tulu või mille paneb toime suur arv inimesi. Seoses sideandmete hankimisega 2016. aasta uurimisvolituste seaduse 4. osa alusel on paragrahvi 87 lõikes 10B lisaks sätestatud, et „raske kuritegu“ tähendab kuritegu, mille eest võib määrata vähemalt 12 kuu pikkuse vangistuse, või süütegu, mille on toime pannud isik, kes ei ole üksikisik, või mille lahutamatu osa on side edastamine või isiku eraelu puutumatuse rikkumine.

⁽¹⁹¹⁾ Suunatud pealtkuulamise määrust võivad taotleda eelkõige järgmised õiguskaitseasutused: riikliku kuritegevusevastase võitluse ameti peadirektor (Director General of the National Crime Agency), Londoni politsei ameti juht (Commissioner of Police of the Metropolis), Põhja-Iirimaa politseiteenistuse peakonstaabel (Chief Constable of the Police Service of Northern Ireland), Šotimaa politseiteenistuse peakonstaabel (Chief Constable of the Police Service of Scotland), Ühendkuningriigi maksu- ja tollivolinik (Commissioner for Her Majesty's Revenue and Customs), kaitseluure ülem (Chief of Defence Intelligence) ja isik, kes on väljaspool Ühendkuningriiki asuva riigi või territooriumi pädev asutus vastastikust abi käsitleva ELi õigusakti või vastastikust abi käsitleva rahvusvahelise lepingu tähenduses (2016. aasta uurimisvolituste seaduse paragrahvi 18 lõige 1).

⁽¹⁹²⁾ Vt 2016. aasta uurimisvolituste seaduse paragrahv 4.

⁽¹⁹³⁾ Vt 2016. aasta uurimisvolituste seaduse paragrahvi 261 lõige 5 ja „Code of Practice on Bulk Acquisition of Communications Data“ (Sideandmete massilise hankimise tegevusjuhend), kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, punkt 2.9.

⁽¹⁹⁴⁾ „Code of Practice on Equipment Interference“ (seadmete töösse sekkumise tegevusjuhend), kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punkt 2.2.

⁽¹⁹⁵⁾ Vastastikuse abiga seotud loa lubatakse Ühendkuningriigi ametiasutusel abistada väljaspool Ühendkuningriigi territooriumi asuvat ametiasutust seoses pealtkuulamisega ja pealtkuulamise teel saadud materjali edastamisega sellisele ametiasutusele kooskõlas vastastikust abi käsitleva rahvusvahelise õigusaktiga (2016. aasta uurimisvolituste seaduse paragrahvi 15 lõige 4).

⁽¹⁹⁶⁾ 2016. aasta uurimisvolituste seadusega (Investigatory Powers Act – IPA 2016) (vt <https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted>) asendati eri seadused, mis käsitlesid side pealtkuulamist, seadmete töösse sekkumist ja sideandmete hankimist, eelkõige 2000. aasta uurimisvolituste reguleerimise seaduse I osa, mis moodustas õiguskaitseasutuste ja riiklike julgeolekuasutuste uurimisvolituste kasutamise varasema üldise õigusliku aluse.

⁽¹⁹⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 138 lõige 1, paragrahvi 158 lõige 1, paragrahvi 178 lõige 1 ja paragrahvi 199 lõige 1.

- (141) Nende volituste teostamiseks peavad ametiasutused saama määruse, ⁽¹⁹⁸⁾ mille annab välja pädev asutus ⁽¹⁹⁹⁾ ning kiidab heaks sõltumatu kohtuvolinik (Judicial Commissioner) ⁽²⁰⁰⁾ (nn topeltkinnituse menetlus). Määruse välja andmisel hinnatakse vajalikkust ja proportsionaalsust ⁽²⁰¹⁾. Kuna need 2016. aasta uurimisvolituste seadusega ette nähtud suunatud uurimisvolitused on samad kui riiklike julgeolekuasutuste käsutuses olevad uurimisvolitused, on selliste volituste suhtes kohaldatavaid piiranguid ja kaitsemeetmeid üksikasjalikult käsitletud jaos „Isikuandmete juurdepääs ja isikuandmete kasutamine Ühendkuningriigi avaliku sektori asutuste poolt riigi julgeoleku eesmärgil“ (vt põhjendus 177 jj).

3.2.2. Kogutud teabe edasine kasutamine

- (142) Kui õiguskaitseasutus jagab teise asutusega andmeid muul eesmärgil kui see, milleks need algselt koguti, (andmete edasisaatmine) siis kehtivad selle suhtes teatavad tingimused.
- (143) Sarnaselt direktiivi (EL) 2016/680 artikli 4 lõikes 2 sätestatule on 2018. aasta andmekaitseaduse paragrahvi 36 lõikega 3 lubatud pädeva asutuse poolt õiguskaitse eesmärgil kogutud isikuandmete edasine töötlemine (algse vastutava töötleja või muu vastutava töötleja poolt) muul õiguskaitse eesmärgil, tingimusel et vastutav töötleja on kooskõlas õigusaktidega volitatud andmeid kõnealusel muul eesmärgil töötlemise ning et töötlemine on selle eesmärgi seisukohast vajalik ja proportsionaalne ⁽²⁰²⁾. Sel juhul kohaldatakse andmeid saava ametiasutuse läbiviidava töötlemise suhtes kõiki 2018. aasta andmekaitseaduse 3. osas sätestatud kaitsemeetmeid, millele on osutatud põhjendustes 122 ja 124.
- (144) Ühendkuningriigi õiguskorras on andmete selline edasisaatmine eri õigusaktidega sõnaselgelt lubatud. Eelkõige on need õigusaktid i) 2017. aasta digimajanduse seadus, millega lubatakse jagada andmeid avaliku sektori asutuste vahel mitmel eesmärgil, näiteks avaliku sektori vastu toimepandud pettuse korral, millega kaasneb avaliku sektori asutuste jaoks kahju või oht kanda kahju, ⁽²⁰³⁾ või avaliku sektori asutuse või riigi ees võlgu olemise korral, ⁽²⁰⁴⁾ ii) 2013. aasta kuritegevuse vastu võitlemise ja kohtute seadus, mille järgi on lubatud jagada teavet riikliku kuritegevusevastase võitluse ametiga (National Crime Agency) ⁽²⁰⁵⁾ raske ja organiseeritud kuritegevusega võitlemiseks, selle uurimiseks ja selle eest vastutusele võtmiseks, ning iii) 2007. aasta raskeid kuritegusid käsitlev seadus, millega lubatakse avaliku sektori asutustel avalikustada teavet pettusevastase võitlusega tegelevatele organisatsioonidele pettuse ennetamise eesmärgil ⁽²⁰⁶⁾.
- (145) Nende seadustega on sõnaselgelt ette nähtud, et teabe jagamine peab olema kooskõlas 2018. aasta andmekaitseaduses sätestatud põhimõtetega. Lisaks on politseikolledž teabe jagamise kohta andnud välja kinnitatud tegevussuunised, ⁽²⁰⁷⁾ et aidata politseil täita oma andmekaitsekohustusi Ühendkuningriigi isikuandmete kaitse

⁽¹⁹⁸⁾ 2016. aasta uurimisvolituste seaduse 2. osa 2. peatükis on sätestatud mõned olukorrad, kus pealtkuulamine võib toimuda ilma määruseta. Need on järgmised: pealtkuulamine saatja või vastuvõtja nõusolekul, pealtkuulamine halduslikel või nõuete täitmise tagamisega seotud eesmärkidel, pealtkuulamine teatavates asutustes (vanglad, psühhiaatriahaglad ja rändajate ennhipidamiskeskused) ning pealtkuulamine kooskõlas asjakohase rahvusvahelise lepinguga.

⁽¹⁹⁹⁾ Enamikul juhtudel annab 2016. aasta uurimisvolituste seaduse alusel määruse välja valitsuskabineti minister, samal ajal kui Šotimaa ministritel on õigus anda välja suunatud pealtkuulamise määruseid, vastastikuse abiga seotud lubasid ja määruseid suunatud sekkumiseks seadmete tööde juhul, kui pealtkuulata isik või ruumid ja seadmed, mille tööde sekkutakse, asuvad Šotimaal (vt 2016. aasta uurimisvolituste seaduse paragrahvid 22 ja 103). Suunatud sekkumise korral seadmete tööde võib 2016. aasta uurimisvolituste seaduse paragrahvis 106 nimetatud tingimustel anda määruse õiguskaitseasutuse ülem (nagu on kirjeldatud 2016. aasta uurimisvolituste seaduse 6. lisa 1. ja 2. osas).

⁽²⁰⁰⁾ Kohtuvolinikud abistavad uurimisvolituste volinikku (Investigatory Powers Commissioner), sõltumatut organit, kelle ülesanne on teha järelevalvet luureasutuste uurimisvolituste kasutamise üle (täpsemad üksikasjad on esitatud põhjenduses 162 jj).

⁽²⁰¹⁾ Vt eelkõige 2016. aasta uurimisvolituste seaduse paragrahvid 19 ja 23.

⁽²⁰²⁾ 2018. aasta andmekaitseaduse paragrahvi 36 lõige 3.

⁽²⁰³⁾ 2017. aasta digimajanduse seaduse (Digital Economy Act 2017) paragrahv 56, kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/2017/30/section/56>.

⁽²⁰⁴⁾ 2017. aasta digimajanduse seaduse paragrahv 48.

⁽²⁰⁵⁾ 2013. aasta kuritegevuse vastu võitlemise ja kohtute seaduse (Crime and Courts Act 2013) paragrahv 7, kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/2013/22/section/7>.

⁽²⁰⁶⁾ 2007. aasta raskeid kuritegusid käsitleva seaduse (Serious Crime Act 2007) paragrahv 68, kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/2007/27/contents>.

⁽²⁰⁷⁾ „Authorised Professional Practice on Information Sharing“ kättesaadav aadressil <https://www.app.college.police.uk/app-content/information-management/sharing-police-information>.

üldmääruse, andmekaitseaduse ja 1998. aasta inimõiguste seaduse alusel. Selle üle, kas andmete jagamine vastab kohaldatavale andmekaitsealasele õigusraamistikule, tehakse kohtulikku kontrolli ⁽²⁰⁸⁾.

- (146) Peale selle on 2018. aasta andmekaitseadusega sarnaselt direktiivi (EL) 2016/680 artiklis 9 sätestatud ette nähtud, et õiguskaitse eesmärgil kogutud isikuandmeid võib töödelda muul kui õiguskaitse eesmärgil, kui selline töötlemine on õigusaktiga lubatud ⁽²⁰⁹⁾.
- (147) Seda liiki jagamine hõlmab kahte stsenaariumi: 1) kui kriminaalõiguskaitseasutus jagab andmeid muu kui kriminaalõiguse valdkonna õiguskaitseasutusega, mis ei ole luureasutus (näiteks finants- või maksuasutusega, pädeva asutusega, noorsooametiga jne), 2) kui kriminaalõiguskaitseasutus jagab andmeid luureasutusega. Esimese stsenaariumi korral jääb isikuandmete töötlemine nii Ühendkuningriigi isikuandmete kaitse üldmääruse kui ka 2018. aasta andmekaitseaduse 2. osa kohaldamisalasse. Komisjon hindas Ühendkuningriigi isikuandmete kaitse üldmääruses ja 2018. aasta andmekaitsemääruse 2. osas sätestatud kaitsemeetmeid põhjendustes 12–111 ja järeldas, et Ühendkuningriik tagab määruse (EL) 2016/679 kohaldamisalas Euroopa Liidust Ühendkuningriiki edastatavatele isikuandmetele piisava kaitsetaseme.
- (148) Teise stsenaariumi puhul, mis käsitleb kriminaalõiguskaitseasutuse kogutud andmete jagamist luureasutusega riigi julgeoleku eesmärgil, on sellist jagamist võimaldav õiguslik alus 2008. aasta terrorismivastase seaduse paragrahv 19 ⁽²¹⁰⁾. Nimetatud seaduse alusel võib iga isik esitada luureteenistusele teavet asjaomase asutuse ülesannete täitmise, sealhulgas riigi julgeoleku tagamise eesmärgil.
- (149) Seoses riigi julgeoleku eesmärgil andmete jagamise tingimustega on luureteenistuste seaduse ⁽²¹¹⁾ ja julgeoleku-teenistuse seadusega ⁽²¹²⁾ piiratud luureteenistuste võimalusi hankida oma seadusjärgsete ülesannete täitmiseks vajalikku teavet. Õiguskaitseasutused, kes soovivad jagada andmeid luureteenistustega, peavad lisaks asutuste seadusjärgsetele ülesannetele, mis on sätestatud luureteenistuste seaduses ja julgeolekuteenistuse seaduses, ⁽²¹³⁾ kaaluma mitut tegurit/piirangut. 2008. aasta terrorismivastase seaduse paragrahvis 20 on selgitatud, et igasugune andmete jagamine paragrahvi 19 alusel peab siiski vastama andmekaitsealastele õigusaktidele, mis tähendab seda, et kohaldatakse kõiki 2018. aasta andmekaitseaduse 3. osas sätestatud piiranguid ja nõudeid. Kuna pädevad asutused on 1998. aasta inimõiguste seaduse tähenduses avaliku sektori asutused, peavad nad peale selle tagama, et nad järgivad Euroopa inimõiguste konventsioonist tulenevaid õigusi, sealhulgas konventsiooni artiklit 8. Nende piirangutega tagatakse, et igasugune õiguskaitseasutuste ja luureteenistuste vaheline andmete jagamine on kooskõlas andmekaitsealaste õigusaktide ja Euroopa inimõiguste konventsiooniga.

⁽²⁰⁸⁾ Vt nt otsus kohtuasjas M, R vs. the Chief Constable of Sussex Police, [2019], EWHC 975 (Admin), milles kõrgel kohtul paluti arutada andmete jagamist politsei ja organisatsiooni Business Crime Reduction Partnership (BCRP) vahel, kes on volitatud haldama sisenemise keelamise teadete süsteemi, millega keelatakse isikutel siseneda tema liikmete äripindadele. Kohus vaatas läbi andmete jagamise, mis toimus lepingu alusel, mille eesmärk oli kaitsta avalikkust ja ennetada kuritegusid, ning järeldas kokkuvõttes, et suurem osa andmete jagamise aspekte olid seaduslikud, välja arvatud teatava tundliku teabe puhul, mida politsei ja BCRP vahel vahetati. Veel üks näide on otsus kohtuasjas Cooper vs. NCA, [2019], EWCA Civ 16, milles apellatsioonikohus toetas andmete jagamist politsei ja raske organiseeritud kuritegevuse vastase võitluse ameti (Serious Organised Crime Agency – SOCA) vahel (SOCA on õiguskaitseasutus, mis praegu moodustab osa riikliku kuritegevusevastase võitluse ametist).

⁽²⁰⁹⁾ 2018. aasta andmekaitseaduse paragrahvi 36 lõige 4.

⁽²¹⁰⁾ 2008. aasta terrorismivastane seadus (Counter Terrorism Act – CTA 2008), kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/2008/28/section/19>.

⁽²¹¹⁾ 1994. aasta luureteenistuste seadus (Intelligence Services Act 1994), kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/1994/13/contents>.

⁽²¹²⁾ 1989. aasta julgeolekuteenistuste seadus (Security Service Act 1989), kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/1989/5/contents>.

⁽²¹³⁾ 1994. aasta luureteenistuste seaduse paragrahvi 2 lõikes 2 on sätestatud: „Luureteenistuse ülem vastutab teenistuse tõhususe eest ning tema ülesanne on tagada, et a) kehtestatud on korraldus selle tagamiseks, et luureteenistus ei hangi mingit muud teavet peale selle, mis on vajalik tema ülesannete nõuetekohaseks täitmiseks, ning et ta ei avalikusta mingit teavet, välja arvatud sel määral, mil see on vajalik i) sel eesmärgil, ii) riigi julgeoleku huvides, iii) raske kuriteo ennetamise või avastamise eesmärgil või iv) mis tahes kriminaalkohtumenetluse eesmärgil, ja b) luureteenistus ei võta mingeid meetmeid Ühendkuningriigi ühegi partei huvide edendamiseks“, samal ajal kui 1989. aasta julgeolekuteenistuste seaduse paragrahvi 2 lõikes 2 on sätestatud: „Peadirektor vastutab teenistuse tõhususe eest ning tema ülesanne on tagada, et a) kehtestatud on korraldus selle tagamiseks, et teenistus ei hangi mingit muud teavet peale selle, mis on vajalik tema ülesannete nõuetekohaseks täitmiseks, ega avalikusta teavet, välja arvatud sel määral, mil see on vajalik sel eesmärgil või raske kuriteo ennetamise või avastamise eesmärgil või mis tahes kriminaalkohtumenetluse eesmärgil, ja b) teenistus ei võta mingeid meetmeid ühegi partei huvide edendamiseks ning c) on olemas riikliku kuritegevusevastase võitluse ameti peadirektoriga kokku lepitud korraldus, et koordineerida kooskõlas käesoleva seaduse paragrahvi 1 lõikega 4 teenistuse tegevust politsei, riikliku kuritegevuse vastase võitluse ameti ja teiste õiguskaitseasutuste tegevusega“.

- (150) Kui pädev asutus kavatseb jagada 2018. aasta andmekaitseaduse 3. osa alusel töödeldud isikuandmeid kolmanda riigi õiguskaitseasutustega, kohaldatakse erinõudeid ⁽²¹⁴⁾. Eelkõige võib selliseid andmeid edastada juhul, kui see põhineb ministri antud kaitse piisavuse määruel, või sellise määruel puudumise korral juhul, kui on tagatud asjakohased kaitsemeetmed. 2018. aasta andmekaitseaduse paragrahvis 75 on sätestatud, et asjakohased kaitsemeetmed on olemas juhul, kui need on kehtestatud andmete kavandatud saaja jaoks siduva õigusaktiga või kui vastutav töötleja teeb pärast seda liiki andmete kolmandasse riiki või rahvusvahelisele organisatsioonile edastamise kõikide asjaolude hindamist järeltule, et andmete kaitsmiseks on olemas asjakohased kaitsemeetmed.
- (151) Kui edastamine ei põhine kaitse piisavuse määruel ega asjakohastel kaitsemeetmetel, võib see toimuda üksnes teataval täpsustatud asjaoludel, mida nimetatakse eritingimusteks ⁽²¹⁵⁾. See kehtib juhul, kui edastamine on vajalik a) andmesubjekti või teise isiku eluliste huvide kaitsmiseks, b) andmesubjekti õigustatud huvide kaitsmiseks, c) liikmesriigi või kolmanda riigi avalikku julgeolekut ähvardava vahetu ja tõsise ohu ennetamiseks, d) üksikjuhtudel õiguskaitsega seotud eesmärgil või e) üksikjuhtudel õiguslikel eesmärkidel (näiteks seoses kohtumenetlusega või õigusnõustamise saamiseks). Võib täheldada, et punkte d ja e ei kohaldata juhul, kui edastamisel kaaluvad andmesubjekti õigused ja vabadused üles avaliku huvi. Need asjaolud vastavad direktiivi (EL) 2016/680 artikli 38 kohastele eriolukordadele ja tingimustele, mis liigitatakse eranditeks.
- (152) Peale selle on 2016. aasta uurimisvolituste seaduses kehtestatud täiendavad kaitsemeetmed juhiks, kui kolmandale riigile antakse üle materjalid, mille õiguskaitseasutused on saanud pealtkuulamist või seadmesse sekkumist võimaldava määruel alusel. Eelkõige on andmete selline avalikustamine, mida nimetatakse „avalikustamiseks välisriigile“, lubatud üksnes siis, kui väljaandev asutus leiab, et kehtestatud on konkreetne asjakohane kord, millega piiratakse nende isikute arvu, kellele andmeid avalikustatakse, materjalide avalikustamise või kättesaadavaks tegemise ulatust ning materjalidest koopiaid tegemise ulatust ja tehtud koopiaid arvu. Samuti võib väljaandev asutus leida, et asjakohane kord on vajalik selle tagamiseks, et kõik materjali mis tahes osast tehtud koopiaid hävitatakse niipea, kui nende säilitamiseks ei ole enam mingeid asjakohaseid põhjuseid (kui neid ei hävitata varem) ⁽²¹⁶⁾.
- (153) Andmete Ühendkuningriigist Ameerika Ühendriikidesse edasisaatmise konkreetsed viisid võivad edaspidi hakata tuginema Suurbritannia ja Põhja-Iiri Ühendkuningriigi ja Ameerika Ühendriikide valitsuse vahel 2019. aasta oktoobris sõlmitud lepingule, mis käsitleb juurdepääsu elektroonilistele andmetele raskete kuritegude vastu võitlemise eesmärgil (edaspidi „Ühendkuningriigi ja USA vaheline leping“ või „leping“) ⁽²¹⁷⁾ ⁽²¹⁸⁾. Kuigi Ühendkuningriigi ja USA vaheline leping ei ole käesoleva otsuse vastuvõtmise ajal veel jõustunud, võib selle prognoositav jõustumine mõjutada algul otsuse alusel Ühendkuningriigile edastatud andmete edasisaatmist USAsse. Täpsemalt võiks EList Ühendkuningriigis asuvatele teenuseosutajatele edastatavate andmete suhtes kohaldada korraldusi esitada elektroonilisi tõendeid, mille on väljastanud USA pädevad õiguskaitseasutused ja mida kohaldatakse Ühendkuningriigis käesoleva lepingu alusel, kui see on jõustunud. Nendel põhjustel on käesoleva otsuse seisukohast oluline hinnata tingimusi ja kaitsemeetmeid, mille alusel selliseid korraldusi võib välja anda ja täita.

⁽²¹⁴⁾ Vt 2018. aasta andmekaitseaduse 3. osa 5. peatükk.

⁽²¹⁵⁾ 2018. aasta andmekaitseaduse paragrahv 76.

⁽²¹⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 54 ja 130. Väljaandvad asutused peavad kaaluma vajadust kehtestada välisriikide ametiasutustele üle antud materjali suhtes konkreetsed kaitsemeetmed selle tagamiseks, et andmete säilitamise, hävitamise ja avaldamise suhtes kehtivad sarnased kaitsemeetmed kui need, mis on sätestatud 2016. aasta uurimisvolituste seaduse paragrahvides 53 ja 129.

⁽²¹⁷⁾ Suurbritannia ja Põhja-Iiri Ühendkuningriigi valitsuse ning Ameerika Ühendriikide valitsuse vaheline leping, mis käsitleb juurdepääsu elektroonilistele andmetele raskete kuritegude vastu võitlemise eesmärgil, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

⁽²¹⁸⁾ See on esimene leping, mis on sõlmitud USA andmete õiguspärasest välismaist kasutust selgitava seaduse (CLOUD (Clarifying Lawful Overseas Use of Data) Act) alusel. CLOUD Act on USA föderaalseadus, mis võeti vastu 23. märtsil 2018 ja milles on selgitatud 1986. aasta salvestatud sideandmete seaduse muudatuse kaudu, et USA teenuseosutajad on kohustatud täitma USA korraldusi avaldada sisulisi ja mittesisulisi andmeid, olenemata sellest, kus selliseid andmeid säilitatakse. Samuti võimaldab CLOUD Act sõlmida välisriikide valitsustega täitelepingsid, mille alusel USA teenuseosutajad saavad edastada sisuandmeid otse välisriikide valitsustele (CLOUD Act'i tekst on kättesaadav aadressil <https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf>).

- (154) Sellega seoses tuleks märkida, et esiteks kohaldatakse lepingut üksnes kuritegude suhtes, mille eest määratava karistuse maksimummäär on vähemalt kolmeaastane vangistus (määratletud „raske kuriteona“),⁽²¹⁹⁾ mis hõlmab ka terroriakte. Teiseks võib teises jurisdiktsioonis töödeldavaid andmeid kõnealuse lepingu alusel saada üksnes pärast seda, kui „kohus, kohtunik, magistraat või muu sõltumatu asutus on [...] korralduse enne selle täitmisele pööramist või selle täitmisele pööramise menetluse käigus korralduse andnud lepinguosalise siseriikliku õiguse kohaselt läbi vaadanud või seda kontrollinud“⁽²²⁰⁾. Kolmandaks peab korraldus „põhinema selgetel ja usaldusväärsetel faktidel, uuritava tegevuse eripäral, seaduslikkusel ja tõsisel põhineva mõistliku põhjenduse nõudel“⁽²²¹⁾ ning „peab olema suunatud konkreetsetele kontodele ning tuvastama konkreetse isiku, konto, aadressi, isikliku seadme või mis tahes muu konkreetse tunnuse“⁽²²²⁾. Neljandaks tagatakse lepingu alusel saadud andmetele samaväärne kaitse kui konkreetsetele kaitsemeetmetele, mis on sätestatud ELi ja USA vahelises raamlepingus,⁽²²³⁾ st 2016. aasta detsembris ELi ja USA vahel sõlmitud laiaulatuslikus andmekaitselepingus, milles sätestatakse õiguskaitsealase koostöö valdkonnas andmete edastamise suhtes kohaldatavad kaitsemeetmed ja õigused, mis kõik on *mutatis mutandis* inkorporeeritud kõnealusesse lepingusse, et võtta eelkõige arvesse andmete edastamise eripära (st andmete edastamine pigem eraõiguslikelt ettevõtjalt õiguskaitseasutustele kui õiguskaitseasutuste vahel)⁽²²⁴⁾. Ühendkuningriigi ja USA lepingus on konkreetsetl sätestatud, et ELi ja USA raamlepingus sätestatuga võrdväärset kaitset kohaldatakse „kõigi isikuandmete suhtes, mis on saadud lepingu alusel antud korralduste täitmise käigus, et tagada samaväärne kaitse“⁽²²⁵⁾.
- (155) Seega peaksid Ühendkuningriigi ja USA vahelise lepingu alusel USA ametiasutustele edastatud andmed olema kaitstud ELi õigusaktiga, milles on tehtud vajalikud kohandused, et kajastada kõnealuste edastamiste laadi. Lisaks on Ühendkuningriigi ametiasutused kinnitanud, et raamlepingu kaitset kohaldatakse kõigi lepingu alusel saadud või säilitatud isikuandmete suhtes, olenemata taotluse esitanud asutuse laadist või liigist (nt nii USA föderalsed kui ka osariikide õiguskaitseasutused), nii et kõikidel juhtudel tuleb tagada samaväärne kaitse. Ühendkuningriigi ametiasutused on siiski ka selgitanud, et andmekaitsemeetmete konkreetse rakendamise üksikasju arutatakse endiselt Ühendkuningriigi ja USA vahel. Käesolevat otsust käsitlevatel kõnelustel Euroopa Komisjoni talitustega kinnitasid Ühendkuningriigi ametiasutused, et võimaldavad lepingul jõustuda alles siis, kui on veendunud, et lepingu rakendamine on kooskõlas lepingus sätestatud õiguslike kohustustega, sealhulgas selgusega andmekaitse-õuete järgimise osas kõigi lepingu alusel nõutavate andmete puhul. Kuna lepingu võimalik jõustumine võib mõjutada käesolevas otsuses hinnatud kaitsetaset, peaks Ühendkuningriik edastama Euroopa Komisjonile mis tahes teabe ja tulevased selgitused selle kohta, kuidas hakkab USA täitma lepingust tulenevaid kohustusi, niipea kui need on kättesaadavad ja igal juhul enne lepingu jõustumist, et tagada käesoleva otsuse nõuetekohane järelevalve kooskõlas määruse (EL) 2016/679 artikli 45 lõikega 4. Erilist tähelepanu pööratakse raamlepinguga ette nähtud kaitsemeetmete kohaldamisele ja kohandamisele Ühendkuningriigi ja USA vahelise lepinguga hõlmatud konkreetset liiki andmeedastuse suhtes.
- (156) Üldisemalt võetakse käesoleva otsuse üle pideva järelevalve teostamisel nõuetekohaselt arvesse kõiki lepingu jõustumise ja kohaldamisega seotud olulisi arengusuundi, sealhulgas seoses vajalike meetmetega, mida tuleb võtta juhul, kui ilmneb, et sisuliselt vastav kaitsetase ei ole enam tagatud.

3.2.3. Järelevalve

- (157) Sõltuvalt volitustest, mida pädevad asutused kasutavad isikuandmete töötlemisel õiguskaitse eesmärgil (kas 2018. aasta andmekaitseseaduse või 2016. aasta uurimisvolituste seaduse alusel), tagavad eri asutused järelevalve nende õiguste kasutamise üle. Täpsemalt: teabevolinik teostab järelevalvet isikuandmete töötlemise üle, kui see

⁽²¹⁹⁾ Lepingu artikli 1 lõige 14.

⁽²²⁰⁾ Lepingu artikli 5 lõige 2.

⁽²²¹⁾ Lepingu artikli 5 lõige 1.

⁽²²²⁾ Lepingu artikli 4 lõige 5. Reaalajas toimuva pealtkuulamise suhtes kohaldatakse täiendavat ja rangemat nõuet: korraldused peavad olema piiratud kestusega, mis ei tohi olla pikem, kui on põhjendatult vajalik korralduse eesmärkide saavutamiseks, ning need antakse välja ainult juhul, kui sama teavet ei ole mõistlikult võimalik saada mõnel vähem sekkuval viisil (lepingu artikli 5 lõige 3).

⁽²²³⁾ Ameerika Ühendriikide ja Euroopa Liidu vaheline süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmisega seotud isikuandmete kaitse kokkulepe, ELT L 336, 10.12.2016, lk 3–13, kättesaadav aadressil [https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:22016A1210\(01\)&from=EN](https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN).

⁽²²⁴⁾ Lepingu artikli 9 lõige 1.

⁽²²⁵⁾ Lepingu artikli 9 lõige 1.

kuulub 2018. aasta andmekaitseaduse 3. osa kohaldamisalasse⁽²²⁶⁾. Sõltumatu ja kohtuliku järelevalve uurimisvõimuste kasutamise üle 2016. aasta uurimisvõimuste seaduse alusel tagab uurimisvõimuste voliniku büroo⁽²²⁷⁾ (seda osa käsitletakse põhjendustes 250–255). Lisaks tagavad täiendava järelevalve nii parlament kui ka teised organid.

3.2.3.1. Järelevalve 2018. aasta andmekaitseaduse 3. osa üle

- (158) Teabeviniku – kelle sõltumatust ja töökorraldust on selgitatud põhjenduses 87 – üldised ülesanded seoses 2018. aasta andmekaitseaduse 3. osa kohaldamisalasse kuuluvate isikuandmete töötlemisega on sätestatud 2018. aasta andmekaitseaduse 13. lisas. Teabeviniku peamine ülesanne on jälgida ja tagada 2018. aasta andmekaitseaduse 3. osa täitmist ning suurendada üldsuse teadlikkust, nõustada parlamenti, valitsust ning muid institutsioone ja organeid. Kohtute sõltumatuse säilitamiseks ei ole teabevinikul õigust täita oma ülesandeid seoses isikuandmete töötlemisega õigustmõistvat funktsiooni täitva isiku või kohtu poolt. Sellisel juhul täidavad järelevalveülesandeid teised organid, nagu on selgitatud põhjendustes 99–103.
- (159) Seoses 3. osa kohaldamisalasse kuuluvate isikuandmete töötlemisega on volinikul üldised uurimis-, parandus-, loaandmis- ja nõuandevõimused. Eelkõige on volinikul õigus teavitada vastutavat või volitatud töötlejat 2018. aasta andmekaitseaduse 3. osa väidetavast rikkumisest, anda välja hoiatusi või noomitusi vastutavale või volitatud töötlejale, kes on rikkunud seaduse 3. osa sätteid, ning esitada omal algatusel või taotluse alusel parlamendile, valitsusele või muudele institutsioonidele ja asutustele ning üldsusele arvamusi isikuandmete kaitsega seotud mis tahes küsimustes⁽²²⁸⁾.
- (160) Lisaks on volinikul õigus väljastada teabenõudeid⁽²²⁹⁾ ning hindamis-⁽²³⁰⁾ ja täitmisteateid⁽²³¹⁾ ning samuti on tal õigus tutvuda vastutavate ja volitatud töötlejate dokumentidega, siseneda nende ruumidesse⁽²³²⁾ ja määrata haldustrahve trahviteadete kujul⁽²³³⁾. Teabeviniku büroo regulatiivse tegevuse poliitikas on sätestatud asjaolud, mille korral büroo esitab teabenõude ning hindamis-, täitmis- ja trahviteateid⁽²³⁴⁾ (vt ka põhjendus 93 ja direktiivi (EL) 2016/680 kohase kaitse piisavuse otsuse, põhjendused 101 ja 102).
- (161) Viimaste aastaaruannete (2018–2019,⁽²³⁵⁾ 2019–2020⁽²³⁶⁾) kohaselt on teabevinik teostanud mitu uurimist ja võtnud täitemeeteid seoses andmete töötlemisega õiguskaitseasutustes. Näiteks viis volinik läbi uurimise ja avaldas 2019. aasta oktoobris arvamuse selle kohta, kuidas õiguskaitseasutused kasutavad avalikes kohtades näotuvastustehnoloogiat. Uurimisel keskenduti eelkõige sellele, kuidas kasutavad näotuvastusvõimekust Lõuna-Walesi politsei ja Londoni politseiamet (Metropolitan Police Service – MPS). Teabevinik uuris ka MPSi nn jõukude maatriksit⁽²³⁷⁾ ja leidis hulga tõsisemaid andmekaitseõiguse rikkumisi, mis tõenäoliselt õnnestavad üldsuse usaldust maatriksi ja selle andmete kasutamise vastu. 2018. aasta novembris andis teabevinik välja täitmisteate ja seejärel astus MPS vajalikud sammud turvalisuse ja

⁽²²⁶⁾ 2018. aasta andmekaitseaduse paragrahv 116.

⁽²²⁷⁾ Vt 2016. aasta uurimisvõimuste seadus, eelkõige selle 8. osa 1. peatükk.

⁽²²⁸⁾ 2018. aasta andmekaitseaduse 13. lisa lõige 2.

⁽²²⁹⁾ Nõuda vastutavalt ja volitatud töötlejalt (ja teatavatel asjaoludel muult isikult) vajaliku teabe esitamist (2018. aasta andmekaitseaduse paragrahv 142).

⁽²³⁰⁾ Võimaldada viia läbi uurimisi ja auditeid, mille käigus võidakse vastutavalt või volitatud töötlejalt nõuda, et ta lubaks volinikul siseneda kindlaksmääratud ruumidesse, tutvuda dokumentide või seadmetega või neid kontrollida ja küsitleda vastutava töötleja nimel isikuandmeid töötlevaid isikuid (2018. aasta andmekaitseaduse paragrahv 146).

⁽²³¹⁾ Lubada kasutada parandusvõimusi, millega nõutakse vastutavalt või volitatud töötlejatelt konkreetsete meetmete võtmist või võtmata jätmist (2018. aasta andmekaitseaduse paragrahv 149).

⁽²³²⁾ 2018. aasta andmekaitseaduse paragrahv 154.

⁽²³³⁾ 2018. aasta andmekaitseaduse paragrahv 155.

⁽²³⁴⁾ Dokument „Regulatory Action Policy“, vt joonealune märkus nr 96.

⁽²³⁵⁾ Teabeviniku 2018.–2019. aasta aruanne ja finantsaruanded, vt joonealune märkus nr 101.

⁽²³⁶⁾ Teabeviniku 2019.–2020. aasta aruanne ja finantsaruanded, vt joonealune märkus nr 82.

⁽²³⁷⁾ Andmebaas, mis sisaldab andmeid väidetavate jõuguliikmete ja jõukudega seotud kuritegude ohvrite kohta.

vastutuse suurendamiseks ning andmete proportsionaalse kasutamise tagamiseks. Teine näide täitemeetmest selles valdkonnas on 325 000 naelsterlingi suurune trahv, mille volinik määras 2018. aasta mais riigiprokuratuurile (Crown Prosecution Service) politseiküsitluste salvestisi sisaldavate krüptimata DVDde kaotamise eest. Teabevinik viis läbi uurimisi ka laiematel teemadel, näiteks 2020. aasta esimeses pooles uuriti mobiiltelefoni kõneeristuse väljavõtte kasutamist politseitöö eesmärgil ja ohvrite andmete töötlemist politseis. Lisaks uurib volinik praegu juhtumit, mis puudutab õiguskaitseasutuste juurdepääsu erasektori üksuse Clearview AI Inc. valduses olevatele andmetele ⁽²³⁸⁾.

- (162) Lisaks teabeviniku õigusnormide täitmise tagamise volitustele, mida on nimetatud põhjendustes 160 ja 161, kujutavad andmekaitsealaste õigusaktide teatavad rikkumised endast õigusrikkumisi ja seetõttu võidakse nende suhtes kohaldada kriminaalkaristusi (2018. aasta andmekaitseseaduse paragrahv 196). Sellised rikkumised on näiteks isikuandmete kogumine, avalikustamine või säilitamine ilma vastutava töötleja nõusolekuta ning isikuandmete avalikustamine teisele isikule ilma vastutava töötleja nõusolekuta ⁽²³⁹⁾; umbisikustatud isikuandmetega seotud teabe põhjal andmesubjektide taastuvastamine ilma isikuandmete umbisikustamise eest vastutava töötleja nõusolekuta ⁽²⁴⁰⁾; voliniku tahtlik takistamine, kui ta teostab oma volitusi seoses isikuandmete kontrollimisega vastavalt rahvusvahelistele kohustustele, ⁽²⁴¹⁾ valeandmete esitamine vastuseks teabenõudele või teabenõude ja hindamisteadetega seotud teabe hävitamine ⁽²⁴²⁾.

3.2.3.2. Muud järelevalveasutused kriminaalõiguskaitse valdkonnas

- (163) Lisaks teabevinikule on kriminaalõiguskaitse valdkonnas mitu järelevalveorganit, kellel on andmekaitseksimustega seoses konkreetset volitused. Sellised organid on näiteks biomeetriliste andmete säilitamise ja kasutamise volinik (edaspidi „biomeetriavolinik“) ⁽²⁴³⁾ ja valvekaamerate volinik ⁽²⁴⁴⁾.

3.2.3.3. Parlamentaarne järelevalve kriminaalõiguskaitse valdkonnas

- (164) Siseasjade erikomisjon (Home Affairs Select Committee – HASC) tagab parlamentaarse järelevalve õiguskaitse valdkonnas. Komisjon koosneb 11 parlamendiliikmest, kes on valitud kolmest suurimast parteist. Komisjoni ülesanne on uurida siseministeeriumi ja sellega seotud avalik-õiguslike asutuste, st politsei ja riikliku kuritegevusevastase võitluse ameti (National Crime Agency – NCA) kulusid, juhtimist ja poliitikat; NCA tööd saab komisjon konkreetselt kontrollida ⁽²⁴⁵⁾.

⁽²³⁸⁾ Vt teabeviniku avaldus, kättesaadav aadressil <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/>.

⁽²³⁹⁾ 2018. aasta andmekaitseseaduse paragrahv 170.

⁽²⁴⁰⁾ 2018. aasta andmekaitseseaduse paragrahv 171.

⁽²⁴¹⁾ 2018. aasta andmekaitseseaduse paragrahvi 119 lõige 6.

⁽²⁴²⁾ Majandusaasta jooksul, mis hõlmab ajavahemikku 1. aprillist 2019 kuni 31. märtsini 2020, on teabeviniku uurimiste tulemusena esitatud neli hoiatust ja kaheksa süüdistust. Nende juhtumite eest esitati süüdistus 1998. aasta andmekaitseseaduse paragrahvi 55, 2000. aasta teabevabaduse seaduse paragrahvi 77 ja 2018. aasta andmekaitseseaduse paragrahvi 170 alusel. Kostjad võtsid 75 %-l juhtudest süü omaks, mistõttu õnnestus vältida pikale veninud kohtuprotsesse ja nendega seotud kulusid. (Teabeviniku 2019.–2020. aasta aruanne ja finantsaruanded, vt joonealune märkus nr 87, lk 40).

⁽²⁴³⁾ Biomeetriavoliniku institutsioon loodi 2012. aasta vabaduste kaitse seadusega (vt <https://www.legislation.gov.uk/ukpga/2012/9/contents>). Peale muude ülesannete täitmise otsustab biomeetriliste andmete volinik, kas politsei tohib säilitada selliste isikute DNA-profiilide andmeid ja sõrmejälgi, kes on vahistatud, kuid kellele ei ole esitatud süüdistust kuriteos (*qualifying offence*) (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahv 63G). Biomeetriavolinikul on ka üldine kohustus jälgida DNA ja sõrmejälgede säilitamist ja kasutamist ning säilitamist riikliku julgeoleku kaalutlustel (2012. aasta vabaduste kaitse seaduse paragrahvi 20 lõige 2). Biomeetriavolinik nimetatakse ametisse ametnike ametisse nimetamise eeskirjade järgi (eeskirjad on kättesaadavad aadressil <https://www.gov.uk/government/publications/governance-code-for-public-appointments>) ja ametist tagandada saab teda ainult siseminister kitsalt piiritletud olukordades, mille hulka kuuluvad kohustuste täitmata jätmise kolme kuu jooksul, kuriteos süüdi mõistmine ja ametisse nimetamise tingimuste rikkumine.

⁽²⁴⁴⁾ Valvekaamerate voliniku institutsioon loodi 2012. aasta vabaduste kaitse seadusega ja tema ülesanne on toetada valvekaamerate tegevusjuhendi järgimist, vaadata läbi tegevusjuhendi toimimine ja nõustada ministreid seoses sellega, kas tegevusjuhendit on vaja muuta. Valvekaamerate volinik nimetatakse ametisse samade eeskirjade järgi nagu biomeetriavolinik ning tal on samasugused volitused, vahendid ja kaitse ametist tagandamise eest.

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

- (165) Komisjon võib oma pädevuse piires valida ise oma uurimisobjekti, sealhulgas erijuhtumid, v.a juhul, kui küsimus on kohtuliku uurimise all (*sub judice*). Komisjon võib küsida ka kirjalikke ja suulisi tõendeid mitmesugustelt isikute rühmadelt ja üksikisikutelt. Ta koostab oma järelduste kohta aruandeid ja annab valitsusele soovitusi ⁽²⁴⁶⁾. Valitsus peab vastama kõigile aruandes esitatud soovitudele 60 päeva jooksul ⁽²⁴⁷⁾.
- (166) Jälgimisvaldkonnas koostas komisjon ka aruande 2000. aasta uurimisvolituste reguleerimise seaduse (Regulation of Investigatory Powers Act – RIPA 2000) kohta, ⁽²⁴⁸⁾ milles leiti, et seadus ei vasta oma eesmärkidele. Aruannet võeti arvesse 2000. aasta uurimisvolituste reguleerimise seaduse oluliste osade asendamisel 2016. aasta uurimisvolituste seadusega. Uurimiste täielik loetelu on avaldatud erikomisjoni veebisaidil ⁽²⁴⁹⁾.
- (167) Siseasjade erikomisjoni ülesandeid täidab Šotimaal politseitöö õigusküsimuste allkomisjon ja Põhja-Iirimaaal õiguskomisjon ⁽²⁵⁰⁾.

3.2.4. Õiguskaitse

- (168) Seoses andmete töötlemisega õiguskaitseasutuste poolt on 2018. aasta andmekaitseseaduse 3. osaga ja 2016. aasta uurimisvolituste seadusega, samuti 1998. aasta inimõiguste seadusega ette nähtud õiguskaitsemehhanismid.
- (169) Need mehhanismid annavad andmesubjektidele tõhusad halduslikud ja kohtulikud õiguskaitsevahendid, mis võimaldavad neil eelkõige teostada oma õigusi, sealhulgas õigust tutvuda oma isikuandmetega või taotleda nende parandamist või kustutamist.
- (170) Esiteks on 2018. aasta andmekaitseseaduse paragrahvi 165 kohaselt andmesubjektil õigus esitada teabevolnikule kaebus, kui andmesubjekt leiab, et seoses teda puudutavate isikuandmetega on rikutud 2018. aasta andmekaitseseaduse 3. osa ⁽²⁵¹⁾. Teabevolnikul on õigus hinnata, kas vastutav ja volitatud töötleja täidavad 2018. aasta andmekaitseseaduse nõudeid, nõuda neilt mittevastavuse korral vajalike meetmete võtmist ja määrata trahve.

⁽²⁴⁶⁾ Erikomisjonide, sealhulgas siseasjade erikomisjoni suhtes kohaldatakse alamkoja alalisi korraldusi. Alalised korraldused on alamkojas kokku lepitud eeskirjad, millega reguleeritakse parlamendi kodukorda. Erikomisjonide pädevus on lai: alalise korralduse 152 punktis 1 on sätestatud: „Erikomisjonid uurivad selle korralduse punktis 2 nimetatud peamiste valitsusasutuste ja nendega seotud avalik-õiguslike asutuste kulusid, juhtimist ja poliitikat“. See võimaldab siseasjade erikomisjonil uurida siseministeeriumi haldusalas olevat mis tahes poliitikat, sealhulgas uurimisvolitusi käsitlevat poliitikat (ja nendega seotud õigusakte). Lisaks on alalise korralduse 152 punktis 4 märgitud, et komisjonidel on mitmesugused volitused, sealhulgas õigus nõuda isikutelt teatavas küsimuses tõendite või dokumentide esitamist ja õigus koostada aruandeid. Teave komisjoni käimasolevate ja lõpetatud uurimiste kohta on kättesaadav aadressil <https://committees.parliament.uk/committee/83/home-affairs-committee/>.

⁽²⁴⁷⁾ Inglismaa ja Walesi siseasjade erikomisjoni volitused on sätestatud alamkoja alalistes korraldustes, mis on kättesaadavad aadressil <https://www.parliament.uk/business/publications/commons/standing-orders-public11/>.

⁽²⁴⁸⁾ Kättesaadav aadressil <https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm>.

⁽²⁴⁹⁾ Kättesaadav aadressil <https://committees.parliament.uk/committee/83/home-affairs-committee>.

⁽²⁵⁰⁾ Šotimaa politseitöö õigusküsimuste allkomisjoni eeskirjad on esitatud aadressil <https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx> ja Põhja-Iirimaa õiguskomisjoni eeskirjad on esitatud aadressil <http://www.niassembly.gov.uk/assembly-business/standing-orders/>.

⁽²⁵¹⁾ Teabevolniku viimases aastaaruandes on esitatud saadud ja lahendatud kaebuste jaotus. Politseitöö ja karistusandmete kohta laekunud kaebuste arv moodustab 6 % laekunud kaebuste koguarvust (see on 1 % rohkem kui eelmisel majandusaastal). Aastaaruandest nähtub ka, et kõige rohkem on andmesubjektide juurdepääsutaotlusi käsitlevaid kaebusi (46 % kaebuste koguarvust, mis on eelmise majandusaastaga võrreldes 8 % rohkem) (teabevolniku 2019.–2020. aasta aruanne, lk 55; vt joonealune märkus nr 88).

- (171) Teiseks on 2018. aasta andmekaitseseaduses sätestatud õigus õiguskaitsevahendile teabeviniku vastu, kui ta ei käsitle andmesubjekti kaebust nõuetekohaselt. Täpsemalt: kui volinik ei saada andmesubjekti kaebust edasi, ⁽²⁵²⁾ on kaebuse esitajal võimalik kasutada õiguskaitsevahendit – ta võib pöörduda esimese astme kohtusse, ⁽²⁵³⁾ et kohustada volinikku võtma asjakohaseid meetmeid kaebusele vastamiseks või teavitama kaebuse esitajat kaebuse menetlemise edenemisest ⁽²⁵⁴⁾. Lisaks võib iga isik, kellele volinik on saatnud mõne teate (teabenõude, hindamis-, täitmis- või trahviteate), pöörduda esimese astme kohtusse. Kui kohus leiab, et voliniku otsus ei ole seadusega kooskõlas või et teabevinik oleks pidanud kasutama oma kaalutlusõigust teisiti, peab kohus kaebuse rahuldama või asendama teate mõne muu teate või otsusega, mille teabevinik oleks võinud saata või teha ⁽²⁵⁵⁾.
- (172) Kolmandaks võivad üksikisikud vastutavate ja volitatud töötajate vastu pöörduda otse kohtusse. Eelkõige võib andmesubjekt 2018. aasta andmekaitseseaduse paragrahvi 167 kohaselt esitada kohtule hagi oma andmekaitsealastest õigusaktidest tuleneva õiguse rikkumise kohta ning kohus võib määrusega nõuda, et vastutav töötaja võtaks (või hoiduks võtmast) seoses isikuandmete töötlemisega mis tahes meetmeid, et täita 2018. aasta andmekaitseseaduse nõudeid. Lisaks on 2018. aasta andmekaitseseaduse paragrahvi 169 kohaselt igal isikul, kes on kandnud kahju andmekaitsealaste õigusaktide (sh 2018. aasta andmekaitseseaduse 3. osa), välja arvatud Ühendkuningriigi isikuandmete kaitse üldmääruse nõuete rikkumise tõttu, õigus saada selle kahju eest vastutavalt või volitatud töötajalt hüvitist, välja arvatud juhul, kui vastutav või volitatud töötaja tõendab, et vastutav või volitatud töötaja ei ole mingil viisil vastutav kahju põhjustanud sündmuse eest. Kahju hõlmab nii rahalist kahju kui ka kannatusi, millega ei kaasne rahalist kahju.
- (173) Peale selle võib iga isik, kes leiab, et avaliku sektori asutus on rikkunud tema õigusi, sealhulgas õigust eraelu puutumatusele ja andmekaitsele, taotleda õiguskaitset Ühendkuningriigi kohtutes 1998. aasta inimõiguste seaduse alusel ⁽²⁵⁶⁾ ning kui riigisisised õiguskaitsevahendid on ammendunud, võib isik, valitsusväline organisatsioon või üksikisikute rühm taotleda Euroopa inimõiguste konventsiooniga ⁽²⁵⁷⁾ tagatud õiguste rikkumise eest õiguskaitset Euroopa Inimõiguste Kohtus (vt põhjendus 111).

3.2.4.1. 2016. aasta uurimisvolituste seadusega ette nähtud õiguskaitsemehhanismid

- (174) Üksikisikud võivad saada 2016. aasta uurimisvolituste seaduse rikkumiste eest õiguskaitset uurimisvolituste kohtus. 2016. aasta uurimisvolituste seaduses sätestatud õiguskaitsevahendeid on kirjeldatud põhjendustes 263–269.

⁽²⁵²⁾ 2018. aasta andmekaitseseaduse paragrahvis 166 on konkreetselt osutatud järgmistele olukordadele: a) volinik ei võta asjakohaseid meetmeid kaebusele vastamiseks, b) volinik ei esita kaebuse esitajale teavet kaebuse menetlemise edenemise või kaebuse tulemuste kohta kolme kuu jooksul alates sellest, kui volinik sai kaebuse, või c) volinik ei ole selle aja jooksul kaebuse läbivaatamisega lõpule jõudnud ega esita kaebuse esitajale nõutavat teavet ka järgneva kolme kuulise ajavahemiku jooksul.

⁽²⁵³⁾ Esimese astme kohus on kohus, kes on pädev menetlema kaebusi, mis on esitatud riiklike reguleerivate asutuste otsuste peale. Teabeviniku otsuse puhul on pädev koda üldine regulatiivkolleegium, mis on pädev kogu Ühendkuningriigis.

⁽²⁵⁴⁾ 2018. aasta andmekaitseseaduse paragrahv 166. Näited edukatest hagidest teabeviniku vastu esimese astme kohtus on juhtum, kus teabevinik kinnitas andmesubjektilt kaebuse saamist, kuid ei märkinud, kuidas ta kavatseb kaebust menetleda, ning seetõttu kohustati teda 21 kalendripäeva jooksul kinnitama, kas ta kavatseb kaebust uurida, ja kui kavatseb, siis teavitama kaebuse esitajat uurimise käigust vähemalt iga 21 kalendripäeva järel (kohtuotsust ei ole veel avaldatud), ning juhtum, mille puhul esimese astme kohus leidis, et jääb selgusetuks, kas teabeviniku vastus kaebusele kujutab endast nõuetekohast tulemust (vt otsus Susan Milne vs. The Information Commissioner, [2020], kättesaadav aadressil <https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf>).

⁽²⁵⁵⁾ 2018. aasta andmekaitseseaduse paragrahvid 162 ja 163.

⁽²⁵⁶⁾ Vt näiteks otsus Brown vs. Commissioner of Police of the Metropolis & Anor, [2019], EWCA, Civ 1724, kus 1998. aasta andmekaitseseaduse ja 1998. aasta inimõiguste seaduse alusel mõisteti isikuteabe ebaseadusliku hankimise ja väärkasutamise eest välja 9 000 naelsterlingit kahjutasu, ning R (on the application of Bridges) vs. Chief Constable of South Wales, [2020], EWCA, Civ 1058, kus apellatsioonikohus kinnitas, et Walesi politsei on kasutanud näotuvastussüsteemi ebaseaduslikult, kuna on rikutud Euroopa inimõiguste konventsiooni artiklit 8 ja vastutava töötaja tehtud andmekaitse mõjuhinnang ei vastanud 2018. aasta andmekaitseseadusele.

⁽²⁵⁷⁾ Euroopa inimõiguste konventsiooni artiklis 34 on sätestatud: „Kohus võib vastu võtta avaldusi igalt üksikisikult, vabaihenduselt ja isikurühmalt, kes väidavad, et nad on konventsioonis ja selle protokollides sätestatud õiguste konventsiooniosalise poolt toimepandud rikkumise ohvriks. Konventsiooniosaliseid ei või mitte mingil viisil takistada selle õiguse tõhusat kasutamist.“

3.3. Juurdepääs andmetele ja nende kasutamine Ühendkuningriigi ametiasutuste poolt riikliku julgeoleku eesmärgil

- (175) Ühendkuningriigi õiguskorras on luureteenistused, kes on volitatud riigi julgeoleku kaalutlustel koguma vastutavate või volitatud töötajate valduses olevat elektroonilist teavet piisava kaitse stsenaariumi seisukohast olulistes olukordades: julgeolekuteenistus ⁽²⁵⁸⁾ (Security Service, MI5), salaluureteenistus ⁽²⁵⁹⁾ (Secret Intelligence Service – SIS) ja valitsusside peakorter ⁽²⁶⁰⁾ (Government Communications Headquarters – GCHQ) ⁽²⁶¹⁾.

3.3.1. Õiguslikud alused, piirangud ja kaitsemeetmed

- (176) Ühendkuningriigis on luureasutuste volitused kehtestatud 2016. aasta uurimisvolituste seaduse ja 2000. aasta uurimisvolituste reguleerimise seadusega, milles on koos 2018. aasta andmekaitse seadusega sätestatud nende volituste sisuline ja isikuline kohaldamisala ning nende kasutamise piirangud ja kaitsemeetmed. Neid volitusi ning nende suhtes kohaldatavaid piiranguid ja kaitsemeetmeid on üksikasjalikult hinnatud järgmistes punktides.

3.3.1.1. Riikliku julgeolekuga seotud uurimisvolitused

- (177) 2016. aasta uurimisvolituste seadusega on ette nähtud õigusraamistik uurimisvolituste kasutamiseks, st volitused pealtkuulamiseks, sideandmetele juurdepääsuks ja seadmete töösse sekkumiseks. 2016. aasta uurimisvolituste seadusega on üldiselt keelatud ja kriminaliseeritud selliste meetodite kasutamine, mis võimaldavad juurdepääsu side sisule või sideandmetele või seadmete töösse sekkumist ilma seadusliku loata ⁽²⁶²⁾. Sellest annab tunnistust asjaolu, et kõnealuste uurimisvolituste kasutamine on seaduslik ainult juhul, kui see toimub määruse alusel ⁽²⁶³⁾.
- (178) 2016. aasta uurimisvolituste seadusega on ette nähtud üksikasjalikud normid, mis reguleerivad iga uurimisvolituse kohaldamisala ja kohaldamist ning nendega seotud piiranguid ja kaitsemeetmeid. Sõltuvalt uurimisvolituse liigist (side pealtkuulamine, sideandmete kogumine ja säilitamine ja seadmete töösse

⁽²⁵⁸⁾ MI5 on siseministri alluvuses. 1989. aasta julgeolekuteenistuse seaduses on sätestatud MI5 ülesanded: riigi julgeoleku kaitsmine (sealhulgas kaitse spionaaži, terrorismi ja sabotaaži eest, välisjõudude agentide tegevuse eest ning tegevuse eest, mille eesmärk on parlamentaarse demokraatia kukutamine või õhnestamine poliitiliste, tööstuslike või vägivaldsete vahenditega), Ühendkuningriigi majandusliku heaolu kaitsmine väliste ohtude eest ning politseijõudude ja muude õiguskaitseasutuste toetamine raskete kuritegude ennetamisel ja avastamisel.

⁽²⁵⁹⁾ SIS on välisministri alluvuses ja selle ülesanded on sätestatud 1994. aasta luureteenistuste seaduses. Selle ülesanne on saada ja anda teavet väljaspool Briti saari asuvate isikute tegevuse või kavatsuste kohta ning täita muid selliste isikute tegevuse või kavatsustega seotud ülesandeid. Neid ülesandeid saab täita üksnes riigi julgeoleku huvides, Ühendkuningriigi majandusliku heaolu huvides või raskete kuritegude ennetamise või avastamise toetamiseks.

⁽²⁶⁰⁾ Valitsusside peakorter on välisministri alluvuses ja selle ülesanded on sätestatud 1994. aasta luureteenistuste seaduses. Nendeks on a) jälgida või kasutada elektromagnetkiirguse või muu sarnase kiirguse abil edastatavaid andmeid ja sellist kiirgust tekitavaid seadmeid ning nendesse sekkuda; hankida ja esitada sellise kiirguse või selliste seadmete või krüpteeritud materjali kaudu edastatavat või nendega seotud teavet; b) anda nõu ja abi keelte, sealhulgas tehniliste ja krüptograafiaga seotud terminite kohta, ning muudes teabe kaitsmisega seotud küsimustes relvajõududele, valitsusele või muudele asjakohaseks peetud organisatsioonidele või isikutele. Neid ülesandeid saab täita üksnes riigi julgeoleku huvides, Ühendkuningriigi majandusliku heaolu huvides seoses väljaspool Briti saari asuvate isikute tegevuse või kavatsustega või raskete kuritegude ennetamise või avastamise toetamiseks.

⁽²⁶¹⁾ Muud riikliku julgeolekuga seotud ülesandeid täitvad avalik-õiguslikud asutused on kaitseluure (Defence Intelligence – DI), riiklik julgeolekunõukogu ja sekretariaat (National Security Council and Secretariat), ühine luureorganisatsioon (Joint Intelligence Organisation) ja ühine luurekomitee (Joint Intelligence Committee). Siiski ei saa ei ühine luurekomitee ega ühine luureorganisatsioon kasutada 2016. aasta uurimisvolituste seaduse alusel uurimisvolitusi, samas kui kaitseluurel on piiratud võimalused oma volitusi kasutada.

⁽²⁶²⁾ Keeld kehtib nii era- kui ka avalik-õiguslike sidevõrkude suhtes, samuti avaliku postiteenuse suhtes, kui pealtkuulamine toimub Ühendkuningriigis. Keeldu ei kohaldata eravõrgu vastutava töötaja suhtes, kui vastutav töötaja on andnud otsese või kaudse nõusoleku pealtkuulamiseks (2016. aasta uurimisvolituste seaduse paragrahv 3).

⁽²⁶³⁾ Teatavatel piiratud juhtudel on seaduslik pealtkuulamine ilma määruseta võimalik, st kui pealtkuulamine toimub saatja või vastuvõtja nõusolekul (2016. aasta uurimisvolituste seaduse paragrahv 44), piiratud haldus- või õiguskaitse-eesmärkide korral (uurimisvolituste seaduse paragrahvid 45–48), teatavates eriinstitutsioonides (uurimisvolituste seaduse paragrahvid 49–51) ja kooskõlas välisriikide taotlustega (uurimisvolituste seaduse paragrahv 52).

sekkumine) ⁽²⁶⁴⁾ ning sellest, kas volitust kasutatakse suunatult või laialdaselt, kohaldatakse eri norme. Järgnevas osas kirjeldatakse iga 2016. aasta uurimisvolituste seaduses sätestatud volituse kohaldamisala, kaitsemeetmeid ja piiranguid.

- (179) Lisaks täiendavad 2016. aasta uurimisvolituste seadust mitmed ministri väljaantud kohustuslikud tegevusjuhendid, mille on heaks kiitnud parlamendi mõlemad koad ⁽²⁶⁵⁾ ja mida kohaldatakse kogu riigis ning milles antakse lisajuhiseid nende volituste kasutamiseks ⁽²⁶⁶⁾. Andmesubjektid saavad oma õiguste teostamiseks tugineda vahetult 2016. aasta uurimisvolituste seaduse sätetele ning seaduse 7. lisa lõikes 5 on märgitud, et tegevusjuhendid on tsiviil- ja kriminaalmenetluses tõenditena lubatavad ning kohus või järelevalveasutus võib kohtumenetluses asjakohase küsimuse otsustamisel võtta arvesse tegevusjuhendite rikkumist ⁽²⁶⁷⁾. Kui Euroopa Inimõiguste Kohtu suurkoda hindas Ühendkuningriigi varasema jälgimist reguleeriva õigusakti, 2000. aasta uurimisvolituste reguleerimise seaduse kvaliteeti, tunnustas kohus sõnaselgelt Ühendkuningriigi tegevusjuhendite asjakohasust ja nõustus, et nende sätteid võib jälgimist reguleeriva õigusakti ootuspärasuse hindamisel arvesse võtta ⁽²⁶⁸⁾.
- (180) Samuti tuleks märkida, et suunatud volitused (suunatud pealtkuulamine, ⁽²⁶⁹⁾ sideandmete kogumine ⁽²⁷⁰⁾ ja säilitamine ⁽²⁷¹⁾ ning suunatud sekkumine seadmete töösse ⁽²⁷²⁾) on kättesaadavad riiklikele julgeolekuasutustele ja teatavatele õiguskaitseasutustele, ⁽²⁷³⁾ samal ajal kui üksnes luureteenistused võivad kasutada laialdasi volitusi (st laialdane pealtkuulamine, ⁽²⁷⁴⁾ laialdane sideandmete kogumine, ⁽²⁷⁵⁾ laialdane seadmete töösse sekkumine ⁽²⁷⁶⁾ ja suured isikuandmete kogumid ⁽²⁷⁷⁾).
- (181) Otsustades, millist uurimisvolitust tuleks kasutada, peab luureasutus järgima 2016. aasta uurimisvolituste seaduse paragrahvi 2 lõike 2 punktis a loetletud „üldisi eraelu puutumatuse kaitsega seotud kohustusi“, mis hõlmavad vajalikkuse ja proportsionaalsuse kontrolli. Täpsemalt peab avaliku sektori asutus, kes kavatseb kasutada uurimisvolitusi, selle sätte kohaselt kaaluma i) kas määruse, loa või teatisega taotletavat eesmärki on mõistlikult

⁽²⁶⁴⁾ Mis puudutab näiteks selliste meetmete kohaldamisala, siis 3. ja 4. osa (sideandmete säilitamine ja kogumine) kohaselt on meetme kohaldamisala rangelt seotud „telekommunikatsioonioperaatori“ määratlusega ja meedet kohaldatakse telekommunikatsioonioperaatorite kasutajate andmete suhtes. Teise näite saab tuua laialdaste volituste kasutamise kohta. Nende volituste kohaldamisala piirneb „selliste sõnumitega, mille on saatnud või vastu võtnud väljaspool Briti saari viibivad isikud“.

⁽²⁶⁵⁾ 2016. aasta uurimisvolituste seaduse 7. lisas on määratud kindlaks tegevusjuhendite kohaldamisala, nende väljaandmise menetlus, nende läbivaatamise reeglid ja tegevusjuhendite mõju.

⁽²⁶⁶⁾ 2016. aasta uurimisvolituste seaduse kohased tegevusjuhendid on kättesaadavad aadressil <https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice>.

⁽²⁶⁷⁾ Kohtud kasutavad tegevusjuhendeid ametiasutuste tegevuse õiguspärasuse hindamisel. Vt näiteks: *Dias vs. Cleveland Police*, [2017], UKIPTrib15_586-CH, kus uurimisvolituste kohus viitas sideandmete tegevusjuhendi konkreetsetele lõikudele, et mõista sideandmete kogumisel kasutatava „kuritegevuse ennetamise või avastamise või korrarikkumiste ennetamise“ aluse määratlust. Tegevusjuhendit mainiti põhjendustes, millega selgitati, kas seda alust on kasutatud vääriti. Seejärel järeldas kohus, et vaidlustatud tegevus oli õigusvastane. Kohtud on hinnanud ka tegevusjuhendites sisalduvate kaitsemeetmete taset, vt näiteks *Just for Law Kids vs. Secretary of State for the Home Department*, [2019], EWHC 1772 (Admin), kus kõrgema astme kohus leidis, et esmased ja teised õigusaktid koos sisesuunistega pakuvad piisavaid kaitsemeetmeid, või *R (National Council for Civil Liberties) vs. Secretary of State for the Home Department & Others*, [2019], EWHC 2057 (Admin), kus leiti, et nii 2016. aasta uurimisvolituste seadus kui ka seadmete töösse sekkumise tegevusjuhend sisaldasid piisavalt sätteid selle kohta, kas konkreetsed määrused on vajalikud.

⁽²⁶⁸⁾ Kohtuasjas *Big Brother Watch* märkis Euroopa Inimõiguste Kohtu suurkoda, et „side pealtkuulamise tegevusjuhend on avalik dokument, mille kiidavad heaks mõlemad parlamendikoad, mille valitsus avaldab internetis ja trükitväljaandena ning mida peavad arvesse võtma nii pealtkuulamisülesanded täitvad isikud kui ka kohtud (vt punktid 93–94). Seetõttu nõustub kohus sellega, et tegevusjuhendi sätteid võib 2000. aasta uurimisvolituste reguleerimise seaduse ootuspärasuse hindamisel arvesse võtta (vt eespool viidatud *Kennedy* kohtuotsus, punkt 157). Sellest tulenevalt nõustub kohus sellega, et siseriiklik õigus on piisavalt „juurdepääsetav“.“ (Vt Euroopa Inimõiguste Kohtu (suurkoda) 25. mai 2021. aasta otsus asjas *Big Brother Watch* ja teised vs. Ühendkuningriik, kaebused nr 58170/13, 62322/14 ja 24960/15, punkt 366).

⁽²⁶⁹⁾ 2016. aasta uurimisvolituste seaduse 2. osa.

⁽²⁷⁰⁾ 2016. aasta uurimisvolituste seaduse 3. osa.

⁽²⁷¹⁾ 2016. aasta uurimisvolituste seaduse 4. osa.

⁽²⁷²⁾ 2016. aasta uurimisvolituste seaduse 5. osa.

⁽²⁷³⁾ Loetelu asjaomastest õiguskaitseasutustest, kes võivad kasutada 2016. aasta uurimisvolituste seaduse alusel suunatud uurimisvolitusi, vt joonealune märkus nr (139).

⁽²⁷⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahv 136.

⁽²⁷⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahv 158.

⁽²⁷⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahv 176.

⁽²⁷⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahv 199.

võimalik saavutada muude, vähem sekkuvate vahenditega; ii) kas määruse, loa või teatise alusel teabe hankimise suhtes kohaldatav kaitsetase on selle teabe erilise tundlikkuse tõttu kõrgem; iii) telekommunikatsioonisüsteemide ja postiteenuste usaldusväärsuse ja turvalisuse vastu valitsevat avalikku huvi ning iv) kõiki muid eraelu puutumatus kaitse suhtes valitseva avaliku huvi aspekte⁽²⁷⁸⁾.

- (182) Seda, kuidas neid kriteeriume tuleks kohaldada, ja viisi, kuidas nende täitmist hinnatakse selliste volituste kasutamise lubamise raames ministri ja sõltumatute kohtuvolinike poolt, on täpsemalt kirjeldatud asjaomastes tegevusjuhendites. Eelkõige peab iga sellise uurimisvolituse kasutamine alati olema „proportsionaalne eesmärgiga, mida soovitakse saavutada, [mis] hõlmab eraelu puutumatuse sekkumise tõsiduse (ja muude paragrahvi 2 lõikes 2 esitatud kaalutluste) tasakaalustamist vajadusega juurdluse, tegevuse või suutlikkuse seisukohast olulise tegevuse järele“. See tähendab eelkõige, et see „peaks pakkuma realistlikku väljavaadet saavutada oodatud kasu ja ei tohiks olla ebaproportsionaalne ega meelevaldne“ ning „eraelu puutumatuse riivet ei tohiks pidada proportsionaalseks, kui taotletavat teavet oleks mõistlikult võimalik saada muude, vähem sekkuvate vahenditega“⁽²⁷⁹⁾. Täpsemalt tuleb proportsionaalsuse põhimõtte järgimist hinnata järgmiste kriteeriumide alusel: „i) kavandatava eraelu puutumatuse riive ulatus võrreldes soovitava eesmärgiga; ii) kuidas ja miks kasutatavad meetodid asjaomast isikut ja teisi võimalikult vähe häirivad; iii) kas kavandatav tegevus kujutab endast seaduse asjakohast ja mõistlikku kohaldamisviisi soovitava eesmärgi saavutamiseks, võttes arvesse kõiki mõistlikke alternatiive; iv) milliseid muid meetodeid kas ei ole rakendatud või on kasutatud, kuid peetakse tegevuseesmärkide täitmiseks ebapiisavaks ilma kavandatud uurimisvolitusi kasutamata.“⁽²⁸⁰⁾

- (183) Nagu Ühendkuningriigi ametiasutused on selgitanud, tagab see praktikas selle, et luureasutus kehtestab esiteks tegevuseesmärgi (piiritledes seega andmete kogumise nt rahvusvahelise terrorismivastase võitluse eesmärgiga konkreetses geograafilises piirkonnas) ja peab teiseks selle tegevuseesmärgi alusel kaaluma, milline tehniline lahendus (nt suunatud või laialdane pealtkuulamine, seadmete töösse sekkumine, sideandmete kogumine) on kõige proportsionaalsem (st riivab kõige vähem eraelu puutumatust, vt uurimisvolituste seaduse paragrahvi 2 lõige 2) taotletava eesmärgiga ning mida võib seega mõnest seaduslikust alusest tulenevalt lubada.

- (184) Tasub märkida, et sellist tuginemist vajalikkuse ja proportsionaalsuse nõuetele on märkinud ja tervitanud ka eraelu puutumatuse õigusega tegelev ÜRO eriraportöör Joseph Cannataci, kes märkis 2016. aasta uurimisvolituste seaduse alusel loodud süsteemi kohta, et „nii luureteenistustes kui ka õiguskaitseasutustes kasutusel olevate menetluste alusel näib süstemaatiliselt olevat nõutud jälgimismeetme või -operatsiooni vajalikkuse ja proportsionaalsuse kaalumise enne, kui seda soovitatakse loa saamiseks, ning selle läbivaatamine samadel alustel“⁽²⁸¹⁾. Samuti märkis ta, et kohtumisel õiguskaitseasutuste ja riiklike julgeolekuasutuste esindajatega „ilmnes üksmeelne seisukoht, et õigus eraelu puutumatusele peab olema iga jälgimismeetmeid käsitleva otsuse puhul esmatahtis. Kõik nad mõistsid ja hindasid vajadust ja proportsionaalsust kui keskseid põhimõtteid, mida tuleb arvesse võtta“.

⁽²⁷⁸⁾ Side pealtkuulamise tegevusjuhendis on täpsustatud, et proportsionaalsuse kontrolli muud elemendid on järgmised: „i) kavandatava eraelu puutumatuse riive ulatus võrreldes soovitava eesmärgiga; ii) kuidas ja miks kasutatavad meetodid asjaomast isikut ja teisi võimalikult vähe häirivad; iii) kas kavandatav tegevus kujutab endast seaduse asjakohast ja mõistlikku kohaldamisviisi soovitava eesmärgi saavutamiseks, võttes arvesse kõiki mõistlikke alternatiive; iv) milliseid muid meetodeid kas ei ole rakendatud või on kasutatud, kuid peetakse tegevuseesmärkide täitmiseks ebapiisavaks ilma kavandatud uurimisvolitusi kasutamata.“ Side pealtkuulamise tegevusjuhendi punkt 4.16, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

⁽²⁷⁹⁾ Side pealtkuulamise tegevusjuhendi punktid 4.12 ja 4.15, kättesaadavad aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

⁽²⁸⁰⁾ Vt side pealtkuulamise tegevusjuhendi punkt 4.16.

⁽²⁸¹⁾ Eraelu puutumatuse õigusega tegeleva eriraportööri Suurbritannia ja Põhja-Iiri Ühendkuningriigi missiooni lõpu aruanne, kättesaadav aadressil <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E>, punkti 1 alapunkt a.

- (185) Eri määruste ja lubade väljaandmise konkreetseid kriteeriume ning 2016. aasta uurimisvolituste seadusega igale uurimisvolitusele kehtestatud piiranguid ja kaitsemeetmeid on üksikasjalikult kirjeldatud põhjendustes 186–243.

3.3.1.1.1. Suunatud pealtkuulamine ja läbivaatamine

- (186) Suunatud pealtkuulamise määrusi on kolme liiki: suunatud pealtkuulamise määrus, ⁽²⁸²⁾ suunatud läbivaatamise määrus ja vastastikuse abistamise määrus ⁽²⁸³⁾. Nende saamise tingimused ja asjakohased kaitsemeetmed on sätestatud 2016. aasta uurimisvolituste seaduse 2. osa 1. peatükis.
- (187) Suunatud pealtkuulamise määruusega lubatakse määruuses kirjeldatud side pealtkuulamist selle edastamise käigus ja muude sellise side jaoks oluliste andmete, ⁽²⁸⁴⁾ sealhulgas teisest andmete ⁽²⁸⁵⁾ kogumist. Suunatud läbivaatamise määrus annab isikule õiguse teha valik laialdase pealtkuulamise määruuse alusel saadud pealtkuulatava sisu läbivaatamiseks ⁽²⁸⁶⁾.
- (188) Kõiki 2016. aasta uurimisvolituste seaduse 2. osa kohaseid määruuseid võib välja anda minister ⁽²⁸⁷⁾ ja selle võib heaks kiita kohtuvolinik ⁽²⁸⁸⁾. Suunatud toimingute määruuse kehtivusaeg piirdub igal juhul kuue kuuga ⁽²⁸⁹⁾ ning selle muutmise ⁽²⁹⁰⁾ ja uuendamise ⁽²⁹¹⁾ suhtes kohaldatakse erinorme.
- (189) Enne määruuse välja andmist peab minister hindama vajalikkust ja proportsionaalsust ⁽²⁹²⁾. Täpsemalt peaks minister suunatud pealtkuulamise ja läbivaatamise määruuse puhul kontrollima, kas meede on vajalik ühel järgmistest põhjustest: riikliku julgeoleku huvid; raske kuriteo ennetamine või avastamine või Ühendkuningriigi majandusliku heaolu huvid, ⁽²⁹³⁾ kui need huvid on olulised ka riigi julgeoleku jaoks ⁽²⁹⁴⁾. Teisalt saab vastastikuse abistamise määruuse (vt põhjendus 139) välja anda ainult juhul, kui minister leiab, et olukord on samaväärne olukorraga, milles ta annaks välja määruuse raskete kuritegude ennetamiseks ja või avastamiseks ⁽²⁹⁵⁾.
- (190) Lisaks peaks minister hindama, kas meede on proportsionaalne eesmärgiga, mida soovitakse saavutada ⁽²⁹⁶⁾. Taotletavate meetmete proportsionaalsuse hindamisel tuleb arvesse võtta üldisi kohustusi seoses eraelu puutumatusega, mis on sätestatud 2016. aasta uurimisvolituste seaduse paragrahvi 2 lõikes 2, eelkõige vajadust

⁽²⁸²⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 15 lõige 2.

⁽²⁸³⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 15 lõige 4.

⁽²⁸⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 15 lõige 2.

⁽²⁸⁵⁾ Teisesed andmed on andmed, mis on lisatud side kaudu edastatud pealtkuulatud teabele või on sellega loogiliselt seotud, mida saab sellest loogiliselt eraldada ja millest eraldatult ei ilmneks midagi sellist, mida võiks mõistliku järeldusena pidada side kaudu edastatud sõnumi tähenduseks (kui see on olemas). Teisesed andmed on näiteks ruuteri konfiguratsioonid või tulemüürid või ajavahemik, mille jooksul ruuter on võrgus olnud aktiivne, kui see on ühendatud või loogiliselt seotud pealtkuulatud sõnumiga. Üksikasjalikum määratlus on esitatud 2016. aasta uurimisvolituste seaduse paragrahvis 16 ja side pealtkuulamise tegevusjuhendi punktis 2.19, vt joonealune märkus nr 278.

⁽²⁸⁶⁾ Kõnealune läbivaatamine on erand 2016. aasta uurimisvolituste seaduse paragrahvi 152 lõikest 4, millega on keelatud püüda tuvastada Briti saartel viibivate isikute sõnumeid. Vt põhjendus 229.

⁽²⁸⁷⁾ Šotimaa minister teeb määruuse, kui see on seotud raske kuritegevusega Šotimaal (vt 2016. aasta uurimisvolituste seaduse paragrahvid 21 ja 22), samal ajal kui minister võib määrata kõrgema ametniku, kes annab välja vastastikuse abiga seotud loa, kui ilmneb, et pealtkuulamine puudutab väljaspool Ühendkuningriiki asuvat isikut või hooneid (2016. aasta uurimisvolituste seaduse paragrahv 40).

⁽²⁸⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 19 ja 23.

⁽²⁸⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 32.

⁽²⁹⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahv 39. Määratud isikud võivad vahistamismäärusi 2016. aasta uurimisvolituste seaduses sätestatud tingimustel piiratud ulatuses muuta. Vahistamismääruse väljaandnud isik võib selle igal ajal tühistada. Ta peab seda tegema, kui määrus ei ole enam vajalik asjakohastel põhjustel või kui määruusega lubatud tegevus ei ole enam proportsionaalne sellega, mida soovitakse saavutada.

⁽²⁹¹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 33. Määruuse uuendamise otsuse peab heaks kiitma kohtuvolinik.

⁽²⁹²⁾ 2016. aasta uurimisvolituste seaduse paragrahv 19.

⁽²⁹³⁾ Mõiste „Ühendkuningriigi majandusliku heaolu huvid, kui need huvid on olulised ka riikliku julgeoleku jaoks“ kohta leidis Euroopa Inimõiguste Kohtu suurkoda asjas Big Brother Watch ja teised vs. Ühendkuningriik (vt joonealune märkus nr 268) tehtud otsuses (punkt 371), et see mõiste oli piisavalt seotud riigi julgeolekuga. Kuigi kohtu järeldus selles asjas puudutas selle mõiste kasutamist 2000. aasta uurimisvolituste reguleerimise seaduses, kasutatakse sama mõistet 2016. aasta uurimisvolituste seaduses.

⁽²⁹⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 20 lõige 2.

⁽²⁹⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 20 lõige 3.

⁽²⁹⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 19 lõike 1 punkt b, lõike 2 punkt b ja lõike 3 punkt b.

hinnata, kas määruse, loa või teatega taotletavat eesmärki on mõistlikult võimalik saavutada muude, vähem sekkuvate vahenditega ning kas määruse alusel teabe saamise suhtes kohaldatav kaitsetase on selle teabe erilise tundlikkuse tõttu kõrgem (vt põhjendus 181).

(191) Selleks peab minister võtma arvesse kõiki soovi esitanud asutuse taotluse elemente, eelkõige neid, mis on seotud pealtkuulatavate isikutega ja meetme asjakohasusega uurimise seisukohast. Sellised elemendid on sätestatud side pealtkuulamise tegevusjuhendis ja neid tuleb kirjeldada teataval konkreetsuse tasemel ⁽²⁹⁷⁾. Lisaks on 2016. aasta uurimisvolituste seaduse paragrahvis 17 nõutud, et igas selle 2. peatüki alusel välja antud määrukses tuleb nimetada või kirjeldada konkreetset isikut või isikute rühma, organisatsiooni või ruume, mille suhtes pealtkuulamist kohaldatakse (edaspidi „sihtmärk“). Suunatud pealtkuulamise või läbivaatamise määrust võidakse kohaldada ka isikute rühma, rohkem kui ühe isiku või organisatsiooni või rohkem kui ühe ruumi suhtes (ka nn temaatilise loa puhul) ⁽²⁹⁸⁾. Sellistel juhtudel tuleks määrukses kirjeldada isikute rühma ühist eesmärki või tegevust või operatsiooni/uurimisi ja nimetada või kirjeldada niivõrd paljusid kõnealuseid isikuid/organisatsioone või ruume, kui on mõistlikult teostatav ⁽²⁹⁹⁾. Samuti peavad kõik 2016. aasta uurimisvolituste seaduse 2. osa alusel välja antud määruksed sisaldama sõnumite identifitseerimiseks kasutatavaid aadresse, numbreid, seadmeid, tegureid või tegurite kombinatsioone ⁽³⁰⁰⁾. Selle kohta on side pealtkuulamise tegevusjuhendis öeldud, et suunatud pealtkuulamise määruuse ja läbivaatamise määruuse puhul „tuleb määrukses täpsustada (või kirjeldada) tegureid või tegurite kombinatsiooni, mida kasutatakse sõnumite tuvastamiseks. Kui sõnumeid tuvastatakse (näiteks) telefoninumbri järgi, tuleb number esitada tervikuna. Ent kui sõnumite tuvastamiseks on vaja kasutada väga keerukaid või pidevalt muutuvaid internetitunnuseid, tuleks neid kirjeldada nii põhjalikult kui võimalik.“ ⁽³⁰¹⁾

(192) Selles kontekstis on oluline kaitsemeede, et ministri hinnangu määruuse väljaandmise kohta peab heaks kiitma sõltumatu kohtuvolinik, ⁽³⁰²⁾ kes kontrollib eelkõige, kas määruuse väljaandmise otsus on kooskõlas vajalikkuse ja proportsionaalsuse põhimõtetega ⁽³⁰³⁾ (kohtuvolinike staatuse ja rolli kohta vt põhjendused 251–256). 2016. aasta uurimisvolituste seaduses on lisaks selgitatud, et sellise kontrolli tegemisel peab kohtuvolinik kohaldama samu põhimõtteid, mida kohaldaks kohus kohtuliku kontrolli taotluse suhtes ⁽³⁰⁴⁾. Sellega tagatakse, et igal konkreetsel juhul ja enne andmete juurdepääsu andmist kontrollib sõltumatu asutus süstemaatiliselt vajalikkuse ja proportsionaalsuse põhimõtte järgimist.

(193) 2016. aasta uurimisvolituste seaduses on sätestatud konkreetsed ja piiritletud erandid suunatud pealtkuulamiseks ilma määruseta. Need vähesed juhtumid on loetletud seaduses ⁽³⁰⁵⁾ ja (välja arvatud juhtum, mis põhineb saatja/vastuvõtja nõusolekul) on mõeldud isikutele (era- või avaliku sektori asutustele), kes ei ole riiklikud julgeolekuasutused. Peale selle toimub seda liiki pealtkuulamine muudel eesmärkidel kui luureteabe kogumine ⁽³⁰⁶⁾ ja mõningatel juhtudel on väga ebatõenäoline, et seda sorti andmekogumine saab toimuda andmete edastamise kontekstis (näiteks pealtkuulamine psühhiaatriaiglas või vanglas). Võttes arvesse, mis sorti asutuste suhtes neid

⁽²⁹⁷⁾ Nõutud teave sisaldab üksikasju tausta kohta (isikute/organisatsioonide/ruumide kirjeldus, pealtkuulatav teabevahetus) ja selle kohta, kuidas sellise teabe saamine aitab uurimist läbi viia, ning luba vajava tegevuse kirjeldust. Kui isikute/organisatsiooni/ruumide kirjeldamine ei ole võimalik, tuleb lisada selgitus selle kohta, miks see ei ole võimalik või miks on esitatud ainult üldine kirjeldus (teabevahetuse pealtkuulamise tegevusjuhend, punktid 5.32 ja 5.34, vt joonealune märkus nr 278).

⁽²⁹⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 17 lõige 2. Vt ka side pealtkuulamise tegevusjuhendi punkt 5.11 jj, vt joonealune märkus nr 278.

⁽²⁹⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 31 lõiked 4 ja 5.

⁽³⁰⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 31 lõige 8.

⁽³⁰¹⁾ Side pealtkuulamise tegevusjuhendi punktid 5.37 ja 5.38, vt joonealune märkus nr 278.

⁽³⁰²⁾ Kohtuvoliniku heakskiitu ei nõuta, kui minister leiab, et määruuse väljaandmiseks on kiireloomuline vajadus (uurimisvolituste seaduse paragrahvi 19 lõige 1). Kohtuvolinikku tuleb siiski teavitada lühikese aja jooksul ja ta peab otsustama, kas määruks heaks kiita või mitte. Kui ta määrust heaks ei kiida, kaotab see kehtivuse (2016. aasta uurimisvolituste seaduse paragrahvid 24 ja 25).

⁽³⁰³⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 23 lõige 1.

⁽³⁰⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 23 lõige 2.

⁽³⁰⁵⁾ Vt 2016. aasta uurimisvolituste seaduse paragrahvid 44–51 ja side pealtkuulamise tegevusjuhendi punkt 12 (vt joonealune märkus nr 278).

⁽³⁰⁶⁾ Näiteks juhul, kui pealtkuulamine on vajalik vanglas või psühhiaatriaiglas (et kontrollida kinnipeetava või patsiendi käitumist) või selleks, et postitietevõtja või telekommunikatsioonioperaator saaks avastada kuritahtlikku infosisu.

erijuhtumeid kohaldatakse (kes ei ole riiklikud julgeolekuasutused), kehtivad kõik 2018. aasta uurimisvolituste seaduse 2. osas ja Ühendkuningriigi isikuandmete kaitse üldmääruses sätestatud kaitsemeetmed, sealhulgas teabevoliniku järelevalve ja ettenähtud õiguskaitsemehhanismid. Lisaks 2018. aasta andmekaitseseaduses sätestatud kaitsemeetmetele on 2016. aasta uurimisvolituste seadusega mõnel juhul ette nähtud ka uurimisvolituste voliniku järelkontroll⁽³⁰⁷⁾.

- (194) Pealtkuulamise kohaldatakse pealtkuulatava(te) isiku(te) eristaatusega seotud täiendavaid piiranguid ja kaitsemeetmeid⁽³⁰⁸⁾. Näiteks on kutsesaladuse alla kuuluva teabe pealtkuulamine lubatud üksnes erandlike ja kaalukate asjaolude esinemisel; määrust välja andev isik peab nõudega hõlmatud teabe konfidentsiaalsuse puhul võtma arvesse avalikku huvi ning sellise materjali käitlemiseks, säilitamiseks ja avalikustamiseks peavad olema kehtestatud erinõuded⁽³⁰⁹⁾.
- (195) Peale selle on 2016. aasta uurimisvolituste seaduses sätestatud turvalisuse, säilitamise ja avalikustamisega seotud konkreetsed kaitsemeetmed, mida minister peab enne suunatud toimingute määruse tegemist arvesse võtma⁽³¹⁰⁾. Eelkõige on 2016. aasta uurimisvolituste seaduse paragrahvi 53 lõikes 5 sätestatud, et kõiki kõnealuse määruse alusel kogutud materjalist tehtud koopiaid tuleb säilitada turvaliselt ja need hävitatakse niipea, kui nende säilitamiseks ei ole enam asjakohast alust; seaduse paragrahvi 53 lõikega 2 on aga ette nähtud, et nende isikute arv, kellele materjal avalikustatakse, ja ulatus, mil määral materjal avalikustatakse, kättesaadavaks tehakse või kopeeritakse, peab piirduma seadusest tulenevatel eesmärkidel vajaliku miinimumiga.
- (196) Kui suunatud pealtkuulamise loa või vastastikuse abistamise määruse alusel pealtkuulatud materjal antakse üle kolmandale riigile („avalikustamine välisriigile“), on 2016. aasta uurimisvolituste seaduses sätestatud, et minister peab tagama asjakohase korra, millega tagatakse, et kõnealuses kolmandas riigis on andmete turvalisuse, säilitamise ja avalikustamise valdkonnas kehtestatud sarnased kaitsemeetmed⁽³¹¹⁾. Lisaks on 2018. aasta andmekaitseseaduse paragrahvi 109 lõikes 2 sätestatud, et luureteenistused võivad isikuandmeid edastada väljapoole Ühendkuningriigi territooriumit üksnes juhul, kui edastamine on vajalik ja proportsionaalne vastutava töötleja seadusjärgsete ülesannete täitmiseks või muudel eesmärkidel, mis on sätestatud 1989. aasta julgeolekuteenistuse seaduse paragrahvi 2 lõike 2 punktis a või 1994. aasta luureteenistuste seaduse paragrahvi 2 lõike 2 punktis a ja paragrahvi 4 lõike 2 punktis a⁽³¹²⁾. Oluline on, et need nõuded kehtivad ka juhtudel, kui 2018. aasta andmekaitseseaduse paragrahvi 110 kohaselt tuginetakse riigi julgeoleku erandile, kuna 2018. aasta andmekaitseseaduse paragrahvis 110 ei ole nimetatud 2018. aasta andmekaitseseaduse paragrahvi 109 nende sätete hulgas, mille kohaldamise võib peatada, kui riigi julgeoleku tagamiseks on vaja teha erandeid mõningatest sätetest.

3.3.1.1.2. Sideandmete suunatud kogumine ja säilitamine

- (197) 2016. aasta uurimisvolituste seadus võimaldab ministril nõuda telekommunikatsiooniooperaatoritelt sideandmete säilitamist, et eri ametiasutused, sealhulgas õiguskaitse- ja luureasutused saaksid neile kitsalt piiritletud tingimustel juurde pääseda. Seaduse 4. osaga on ette nähtud sideandmete säilitamine ning 3. osaga sideandmete suunatud kogumine. Seaduse 3. ja 4. osas on sätestatud ka nende volituste kasutamise konkreetsed piirangud ja ette nähtud konkreetsed kaitsemeetmed.

⁽³⁰⁷⁾ Seevastu vt uurimisvolituste seaduse paragrahvi 229 lõige 4.

⁽³⁰⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvides 26–29 on sätestatud piirangud suunatud pealtkuulamise loa ja suunatud läbivaatamise loa saamisel seoses parlamendiliikme (ükskõik millise Ühendkuningriigi parlamendi liikme) saadetud või tema jaoks mõeldud teadete pealtkuulamisega, kutsesaladuse alla kuuluva teabe pealtkuulamisega, sellise teabe pealtkuulamisega, mille puhul pealtkuulav asutus usub, et pealtkuulatav teave sisaldab konfidentsiaalset ajakirjanduslikku materjali, ja kui määruse eesmärk on tuvastada ajakirjandusliku teabe allikas või seda kinnitada.

⁽³⁰⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 26.

⁽³¹⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 19 lõige 1.

⁽³¹¹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 54. Välisriikide ametiasutustele andmete avalikustamisega seotud kaitsemeetmeid on täpsemalt kirjeldatud tegevusjuhendites: vt eeskätt side pealtkuulamise tegevusjuhendi punkt 9.26 jj ja punkt 9.87 ning seadmete tööse sekkumise tegevusjuhendi punkt 9.33 jj ja punkt 9.41 (vt joonealune märkus nr 278).

⁽³¹²⁾ Need eesmärgid on järgmised: julgeolekuteenistuse puhul raske kuriteo ennetamine või avastamine või kriminaalkohtumenetlus (1989. aasta julgeolekuteenistuse seaduse paragrahvi 2 lõike 2 punkt a), luureteenistuse puhul riigi julgeoleku huvid, raske kuriteo ennetamine või avastamine või kriminaalkohtumenetlus (1994. aasta luureteenistuste seaduse paragrahvi 2 lõike 2 punkt a) ja valitsusside peakorteri puhul kriminaalkohtumenetlus (1994. aasta luureteenistuste seaduse paragrahvi 4 lõike 2 punkt a). Vt 2018. aasta andmekaitseseaduse selgitavad märkused, kättesaadavad aadressil: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>.

- (198) Termin „sideandmed“ hõlmab vastuseid sidega seotud küsimustele „kes?“, „millal?“, „kust?“ ja „kuidas?“, kuid mitte sidevahendite kaudu edastatud teabe sisu, st seda, mida räägiti või kirjutati. Erinevalt pealtkuulamisest ei ole sideandmete kogumise ja säilitamise eesmärk mitte sidevahendite kaudu edastatud sisu hankimine, vaid teabe hankimine selliste küsimuste kohta nagu telefoniteenuse abonent või üksikasjalik arve. See võib hõlmata side aega ja kestust, teabevahetuse algataja ja vastuvõtja telefoninumbrit või e-posti aadressi ning mõnikord nende seadmete asukohta, mille kaudu side toimus ⁽³¹³⁾.
- (199) Tuleb märkida, et sideandmete säilitamine ja kogumine ei puuduta üldjuhul käesoleva otsuse kohaselt Ühendkuningriigile edastatud ELi andmesubjektide isikuandmeid. 2016. aasta uurimisvolituste seaduse 3. ja 4. osa kohane sideandmete säilitamise või avalikustamise kohustus hõlmab andmeid, mida Ühendkuningriigi telekommunikatsioonioperaatorid koguvad otse telekommunikatsiooniteenuse kasutajatelt ⁽³¹⁴⁾. Sedalaadi kliendiandmete töötlemine ei hõlma üldjuhul andmete edastamist käesoleva otsuse alusel, st edastamist ELi vastutavalt /volitatud töötlejal Ühendkuningriigis asuval vastutavale/volitatud töötlejale.
- (200) Täielikkuse huvides on järgmistes põhjendustes siiski analüüsitud sellise andmete kogumise ja säilitamise korra tingimusi ja kaitsemeetmeid.
- (201) Algatuseks tuleb märkida, et nii riiklikel julgeolekuasutustel kui ka osadel õiguskaitseasutustel on võimalik sideandmeid säilitada ja suunatult koguda ⁽³¹⁵⁾. Sideandmete säilitamise ja/või kogumise tingimused võivad olla erinevad, sõltuvalt sellest, mis on selle taotlemise aluseks, kas riigi julgeolekuga seotud või õiguskaitsealane eesmärk.
- (202) Kuigi uue korraga on kehtestatud üldine nõue, et kõigi sideandmete säilitamise ja/või kogumise juhtude jaoks (kas õiguskaitsealastel või riigi julgeolekuga seotud eesmärkidel) on vajalik sõltumatu organi eelnev luba, viidi pärast Euroopa Kohtu otsust kohtuasjas Tele2/Watson ⁽³¹⁶⁾ sisse konkreetsed kaitsemeetmed juhtudeks, kui sideandmete säilitamist ja/või kogumist taotletakse õiguskaitsealastel eesmärkidel. Kui sideandmete säilitamist või kogumist taotletakse õiguskaitsealasel eesmärgil, peab eelneva loa alati andma uurimisvolituste volinik. See ei kehti alati juhul, kui meedet taotletakse riigi julgeolekuga seotud eesmärgil, kuna, nagu allpool selgitatakse, võivad teataval juhtudel anda seda liiki meetmeteks loa teised luba andvad isikud. Lisaks on uue korraga ette nähtud, et sideandmete säilitamise ja kogumise lubamise künniseks on nüüd „rasked kuriteod“ ⁽³¹⁷⁾.
-
- ⁽³¹³⁾ „Sideandmed“ on määratletud 2016. aasta uurimisvolituste seaduse paragrahvi 261 lõikes 5. Sideandmed on jagatud „sündmuse andmeteks“ (andmed, mis tuvastavad telekommunikatsioonisüsteemis või selle kaudu toimuva sündmuse või kirjeldavad seda (olenemata sellest, kas viidatakse sündmuse toimumise kohale), kui sündmus koosneb ühest või mitmest üksusest, kes tegelevad konkreetsel ajal konkreetse tegevusega) ja „üksuse andmeteks“ (andmed, mis a) on seotud i) üksusega, ii) sideteenuse ja üksuse vahelise seosega või iii) seosega telekommunikatsiooniteenuse ja üksuse vahel, b) koosnevad üksust tuvastada võimaldavatest või kirjeldavatest andmetest (olenemata sellest, kas viidatakse sündmuse toimumise kohale) või sisaldavad selliseid andmeid ja c) ei ole sündmuse andmed.
- ⁽³¹⁴⁾ See tuleneb uurimisvolituste seaduse paragrahvi 261 lõikes 5 esitatud sideandmete määratlusest, mille kohaselt säilitab või kogub sideandmeid telekommunikatsioonioperaator ja mis on seotud kas mõne telekommunikatsiooniteenuse kasutajaga ja vastava teenuse osutamisega või mis on mõne sidevahendite kaudu edastatava sõnumiga hõlmatud, sellele lisatud või sellega loogiliselt seotud (vt ka sideandmete tegevusjuhend, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, punktid 2.22–2.33). Lisaks on 2016. aasta uurimisvolituste seaduse paragrahvi 261 lõikes 10 esitatud telekommunikatsioonioperaatori määratluses sätestatud, et telekommunikatsioonioperaator on isik, kes pakub või osutab telekommunikatsiooniteenust Ühendkuningriigis asuvatele isikutele või kes kontrollib või pakub telekommunikatsioonisüsteemi, mis (täielikult või osaliselt) asub Ühendkuningriigis või mida kontrollitakse Ühendkuningriigist. Need määratlused näitavad selgelt, et uurimisvolituste seaduse kohaseid kohustusi ei saa panna telekommunikatsioonioperaatoritele, kelle seadmed ei asu Ühendkuningriigis või ei ole Ühendkuningriigist kontrollitavad ning kes ei paku ega osuta teenuseid Ühendkuningriigis asuvatele isikutele (vt ka sideandmete tegevusjuhend, punkt 2.1). Kui ELi abonentid (olenemata sellest, kas nad asuvad ELis või Ühendkuningriigis) kasutavad Ühendkuningriigis teenuseid, ei kantaks selle teenuse osutamisega seotud teavet ELi listi üle, vaid seda koguks Ühendkuningriigi teenuseosutaja otse.
- ⁽³¹⁵⁾ Asjaomased asutused on loetletud 2016. aasta uurimisvolituste seaduse 4. lisas ning nende hulka kuuluvad politsei jõud, luureteenistused, mõned ministriumid ja valitsusasutused, riiklik kuritegevusevastase võitluse amet, maksu- ja tolliamet, konkurents- ja turuamet, teabevolinik, kiirabi-, tuletõrje- ja päästeteenistused ning näiteks tervishoiu ja toiduohutuse valdkonna ametiasutused.
- ⁽³¹⁶⁾ Liidetud kohtuasjad C-203/15 ja C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).
- ⁽³¹⁷⁾ Vt paragrahvi 61 lõike 7 punkt b sideandmete kogumise kohta ja paragrahvi 87 lõige 10A sideandmete säilitamise kohta.

i) Luba sideandmete hankimiseks

(203) 2016. aasta uurimisvolituste seaduse 3. osa kohaselt on asjaomastel riigiasutustel õigus saada sideandmeid telekommunikatsioonioperaatorilt või muult isikult, kes saab selliseid andmeid hankida ja avaldada. Luba ei tohi võimaldada seda kaudu edastatava teabe pealtkuulamist⁽³¹⁸⁾ ja see kaotab kehtivuse ühe kuu möödumisel⁽³¹⁹⁾ võimalusega seda täiendava loa olemasolul pikendada⁽³²⁰⁾. Sideandmete hankimiseks on vaja uurimisvolituste voliniku⁽³²¹⁾ luba (uurimisvolituste voliniku staatuse ja volituste kohta vt põhjendused 250–251). See kehtib kõikidel juhtudel, kui sideandmete hankimist taotleb asjaomane õiguskaitseasutus. 2016. aasta uurimisvolituste seaduse paragrahvis 61 on siiski sätestatud, et kui andmeid kogutakse Ühendkuningriigi riikliku julgeoleku huvides või riikliku julgeoleku seisukohast olulise majandusliku heaolu huvides või kui taotluse esitab mõne luureasutuse liige vastavalt paragrahvi 61 lõike 7 punktile b,⁽³²²⁾ võib teabe hankimist⁽³²³⁾ lubada kas uurimisvolituste volinik või selleks määratud kõrgem ametnik⁽³²⁴⁾. Määratud ametnik peab olema asjaomasest uurimisest või toimingust sõltumatu ning tal peavad olema praktilised teadmised inimõiguste põhimõtete ja õigusaktide, eelkõige vajalikkuse ja proportsionaalsuse kohta⁽³²⁵⁾. Määratud ametniku otsuse suhtes teeb uurimisvolituste volinik järelkontrolli (vt üksikasjalikumat teavet uurimisvolituste voliniku järelkontrolli ülesannete kohta põhjenduses 254).

(204) Sideandmete kogumise luba põhineb meetme vajalikkuse ja proportsionaalsuse hindamisel. Täpsemalt hinnatakse meetme vajalikkust õigusaktis loetletud aluste valguses⁽³²⁶⁾. Arvestades selle meetme kitsast suunitlust, peab see olema vajalik ka konkreetse uurimise või operatsiooni jaoks⁽³²⁷⁾. Täiendavad nõuded meetmete vajalikkuse hindamiseks on sätestatud sideandmete tegevusjuhendis⁽³²⁸⁾. Eelkõige on tegevusjuhendiga ette nähtud, et soovi esitanud asutuse taotluses tuleks esitada kolm miinimumelementi, mis õigustavad taotluse vajalikkust: i) uurimisalune sündmus, näiteks kuritegu või teadmata kadunud haavatava isiku asukoht; ii) isik, kelle kohta andmeid taotletakse, näiteks kahtlustatav, tunnistaja või teadmata kadunud isik, ja kuidas ta on sündmusega seotud, ja iii) taotletavad sideandmed, näiteks telefoninumber või IP-aadress, ning kuidas need andmed on seotud isiku ja sündmusega⁽³²⁹⁾.

(205) Lisaks peab sideandmete kogumine olema proportsionaalne eesmärgiga, mida soovitakse saavutada⁽³³⁰⁾. Sideandmete tegevusjuhendis on selgitatud, et sellise hindamise läbiviimisel peaks luba andev isik kaaluma „isiku õigustesse ja vabadustesse sekkumise ulatust võrreldes asjaomase ametiasutuse poolt avalikes huvides läbiviidava uurimise või operatsiooni konkreetse kasuga“ ning et konkreetse juhtumi kõiki asjaolusid arvesse võttes „ei pruugi

⁽³¹⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 60A lõige 6.

⁽³¹⁹⁾ Kiireloomulise loa andmisel lühendatakse seda tähtaega kolme päevani (2016. aasta uurimisvolituste seaduse paragrahvi 65 lõige 3A).

⁽³²⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 65 kohaselt kehtib pikendatud luba ühe kuu alates kuupäevast, kui esmane luba kaotab kehtivuse. Loa andnud isik võib loa igal ajal tühistada, kui ta leiab, et nõuded ei ole enam täidetud.

⁽³²¹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 60A lõige 1. Seda ülesannet täidab uurimisvolituste voliniku nimel sideandmete lubade amet (Office for Communications Data Authorisations) (vt sideandmete tegevusjuhendi punkt 5.6).

⁽³²²⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 61 lõike 7 punkti b kohane taotlus on esitatud „kuriteo vältimise eesmärgil“, mis tähendab seaduse paragrahvi 61 lõike 7A kohaselt järgmist: „kui sideandmed on täielikult või osaliselt sündmuse andmed, eesmärk on kuriteo vältimine või avastamine; kõigil muudel juhtudel on eesmärk kuriteo ennetamine või avastamine või korrariikumiste ärahoidmine“.

⁽³²³⁾ Sideandmete tegevusjuhendis on sätestatud: „Kui riikliku julgeolekuga seotud taotlust saab esitada kas paragrahvi 60A või paragrahvi 61 alusel, teeb otsuse selle kohta, milline loa andmise viis on igal konkreetsel juhul kõige asjakohasem, vastav ametiasutuses. Ametiasutused, kes soovivad kasutada määratud kõrgema ametniku võimalust, peaksid kehtestama selged suunised selle kohta, millal kõnealune loamenetlus on asjakohane“ (sideandmete tegevusjuhendi punkt 5.19, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

⁽³²⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 70 lõikes 3 on esitatud „määratud ametniku“ määratlus, mis varieerub sõltuvalt asjaomasest ametiasutusest (nagu on sätestatud uurimisvolituste seaduse 4. lisas).

⁽³²⁵⁾ Täpsemad üksikasjad määratud kõrgema ametniku sõltumatuse kohta on esitatud sideandmete tegevusjuhendis (sideandmete tegevusjuhendi punktid 4.12–4.17, vt joonealune märkus nr 323).

⁽³²⁶⁾ Need alused on: i) riiklik julgeolek; ii) kuritegude või korrariikumiste ennetamine või avastamine (sündmuse andmete puhul ainult raske kuriteo korral); iii) Ühendkuningriigi majandusliku heaolu huvid, kui need huvid on olulised ka riigi julgeoleku jaoks; iv) ühiskondliku turvalisuse huvid; v) eesmärk hoida ära surm või vigastus või kahju isiku füüsilisele või vaimsele tervisele või leevendada kahju isiku füüsilisele või vaimsele tervisele; vi) eesmärk aidata uurida väidetavaid kohtumõistmise vigu või vii) eesmärk tuvastada surnud isik või isik, kes ei ole võimeline end teatava asjaolu tõttu identifitseerima (2016. aasta uurimisvolituste seaduse paragrahvi 61 lõige 7).

⁽³²⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 60A lõike 1 punkt b.

⁽³²⁸⁾ Vt ka sideandmete tegevusjuhendi punkt 3.3 jj, vt joonealune märkus nr 323.

⁽³²⁹⁾ Vt ka sideandmete tegevusjuhendi punkt 3.13, vt joonealune märkus nr 323.

⁽³³⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 60 lõike 1 punkt c.

üksikisiku õiguste riive siiski olla põhjendatud, sest negatiivne mõju teise üksikisiku või isikute rühma õigustele on liiga suur". Selleks, et hinnata konkreetselt meetme proportsionaalsust, on tegevusjuhendis loetletud mitu elementi, mis peaksid sisalduma soovi avaldanud asutuse taotluses ⁽³³¹⁾. Lisaks tuleb erilist tähelepanu pöörata kogutavate sideandmete liigile („üksuse“ või „sündmuse“ andmed ⁽³³²⁾) ning eelistada tuleb vähem sekkuvate andmekategooriate kasutamist ⁽³³³⁾. Sideandmete tegevusjuhend sisaldab ka konkreetseid juhiseid lubade kohta, mis sisaldavad sideandmeid teatavate kutsealade esindajate (arstid, juristid, ajakirjanikud, parlamendiliikmed või vaimulikud) ⁽³³⁴⁾ kohta, kelle suhtes kohaldatakse täiendavaid kaitsemeetmeid ⁽³³⁵⁾.

ii) *Sideandmete säilitamise teatis*

- (206) 2016. aasta uurimisvolituste seaduse 4. osas on sätestatud sideandmete säilitamise eeskirjad ja eelkõige kriteeriumid, mille alusel võib minister väljastada säilitamisteatise ⁽³³⁶⁾. Uurimisvolituste seadusega kehtestatud kaitsemeetmed on samad nii juhul, kui andmeid säilitatakse õiguskaitse eesmärgil, kui ka juhul, kui seda tehakse riigi julgeoleku huvides.
- (207) Selliste säilitamisteatiste väljastamise eesmärk on tagada, et telekommunikatsioonioperaatorid säilitaksid kuni 12 kuu jooksul asjakohased sideandmed, mis muidu kustutatakse, kui neid enam ärielistel eesmärkidel ei vajata ⁽³³⁷⁾. Säilitatavad andmed jäävad nõutava aja jooksul kättesaadavaks juhuks, kui ametiasutusel peaks hiljem olema vaja neid koguda 2016. aasta uurimisvolituste seaduse 3. osas sätestatud ja põhjendustes 203–205 kirjeldatud sideandmete suunatud kogumise loa alusel.
- (208) Kui minister kasutab õigust nõuda teatavate andmete säilitamist, kehtivad selle suhtes mitmed piirangud ja kaitsemeetmed. Minister saab väljastada säilitamisteatise ühele või mitmele operaatorile ⁽³³⁸⁾ ainult siis, kui ta leiab, et andmete säilitamise nõue on vajalik ühel seaduses sätestatud eesmärkidest ⁽³³⁹⁾ ja on proportsionaalne eesmärgiga, mida soovitakse saavutada ⁽³⁴⁰⁾. Nagu on selgitatud 2016. aasta

⁽³³¹⁾ Taotluses peab sisalduma järgmine teave: i) ülevaade sellest, kuidas andmete hankimine toob uurimisele või operatsioonile kasu; ii) selgitus taotluses mainitud ajavahemike asjakohasuse kohta, sealhulgas selle kohta, kuidas need ajavahemikud on uurimisaluse sündmusega proportsionaalsed; iii) selgitus selle kohta, kuidas sekkumise tase on põhjendatud, võttes arvesse kasu, mida andmed uurimisele annavad (selline põhjendus peaks hõlmama kaalumist, kas eesmärki oleks võimalik saavutada vähem sekkuvate uurimismeetoditega); iv) üksikisiku õiguste (eelkõige eraelu puutumatuse ja asjakohastel juhtudel sõnavabaduse) arvesse võtmine ning nende õiguste kõrvutamine uurimise jaoks saadava kasuga; v) üksikasjad selle kohta, kuidas sideandmete kogumisega võidakse koguda andmeid ka kõrvaliste isikute kohta ja kuidas taotletavad ajavahemikud mõjutavad kõrvaliste isikute kohta andmete kogumist (sideandmete tegevusjuhendi punktid 3.22–3.26, vt joonealune märkus nr 323).

⁽³³²⁾ Vt joonealune märkus nr 313.

⁽³³³⁾ Kui taotletakse sekkuvamaid sideandmeid (st sündmuste andmeid), täpsustatakse tegevusjuhendis, et on asjakohasem hankida esmase üksuse andmeid või piiratud kiireloomulistel juhtudel otse sündmuste andmeid (sideandmete tegevusjuhendi punktid 6.10–6.14, vt joonealune märkus nr 323).

⁽³³⁴⁾ Sideandmete tegevusjuhendi punktid 8.8–8.44, vt joonealune märkus nr 323.

⁽³³⁵⁾ Tegevusjuhendis on sätestatud: „Luba andev isik peab selliste taotluste läbivaatamisel olema eriti hoolikas, kaaludes muu hulgas täiendavalt, kas sellised taotlused võivad kaasa tuua soovimatuid tagajärgi ja kas taotlus teenib kõige paremini üldsuse huve“ (sideandmete tegevusjuhendi punkt 8.8). Lisaks tuleb seda tüüpi taotlused dokumenteerida ja järgmisel kontrollimisel tuleb juhtida nende uurimisvolituste voliniku tähelepanu (sideandmete tegevusjuhendi punkt 8.10, vt joonealune märkus nr 323).

⁽³³⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 87–89.

⁽³³⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 90 kohaselt võib telekommunikatsioonioperaator, kellele andmete säilitamise teatis saadetakse, taotleda selle väljastanud ministrilt selle läbivaatamist.

⁽³³⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 87 lõike 2 punkti a järgi võib säilitamisteatis puudutada „konkreetselt operaatorit või kirjeldatud operaatoreid“.

⁽³³⁹⁾ Eesmärgid on i) riikliku julgeoleku huvid; ii) kuriteo vältimise eesmärk (vastavalt 2016. aasta uurimisvolituste seaduse paragrahvi 87 lõikes 10A esitatud määratlusele); iii) Ühendkuningriigi majandusliku heaolu huvid, kui need huvid on olulised ka riikliku julgeoleku jaoks; iv) ühiskondliku turvalisuse huvid; v) eesmärk hoida ära surm või vigastus või kahju isiku füüsilisele või vaimsele tervisele või leevendada kahju isiku füüsilisele või vaimsele tervisele või vi) eesmärk aidata uurida väidetavaid kohtumõistmise vigu (uurimisvolituste seaduse paragrahv 87).

⁽³⁴⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahv 87. Lisaks kohaldatakse asjaomase tegevusjuhendi kohaselt säilitamisteatise proportsionaalsuse hindamiseks 2016. aasta uurimisvolituste seaduse paragrahvi 2 lõikes 2 sätestatud kriteeriume, eelkõige nõuet hinnata, kas teatisega taotletavat eesmärki on võimalik saavutada vähem sekkuvate vahenditega. Sarnaselt sideandmete kogumise proportsionaalsuse hindamisele selgitatakse sideandmete tegevusjuhendis, et selline hindamine hõlmab „isiku eraelu puutumatuse õigusesse sekkumise ulatuse kõrvutamist konkreetse kasuga uurimise jaoks“ (sideandmete tegevusjuhendi punkt 16.3, vt joonealune märkus nr 323).

uurimisvolituste seaduses, ⁽³⁴¹⁾ peab minister enne säilitamisteatise väljastamist võtma arvesse järgmist: teatisest saadav tõenäoline kasu ⁽³⁴²⁾; telekommunikatsiooniteenuste kirjeldus; kas oleks asjakohane piirata säilitatavaid andmeid viitega asukohale või nende isikute kirjeldustele, kellele telekommunikatsiooniteenuseid osutatakse ⁽³⁴³⁾; teatisega seotud telekommunikatsiooniteenuste kasutajate tõenäoline arv (kui see on teada) ⁽³⁴⁴⁾; teatise täitmise tehniline teostatavus; teatise täitmisega seotud tõenäolised kulud ja teatise muu mõju telekommunikatsiooniooperaatorile (või operaatorite kirjeldus), keda teatis puudutab ⁽³⁴⁵⁾. Nagu on üksikasjalikumalt kirjeldatud sideandmete tegevusjuhendi 17. peatükis, tuleb kõigis säilitamisteatistes täpsustada iga säilitatav andmeliik ja see, kuidas see andmeliik vastab säilitamiseks vajalikele kriteeriumidele.

- (209) Kõigil juhtudel (nii riigi julgeolekuga seotud kui ka õiguskaitsealaste eesmärkide korral) peab ministri otsuse säilitamisteatise väljaandmise kohta kinnitama sõltumatu kohtuvolinik nn topeltkinnituse menetluse raames; kohtuvolinik peab eeskätt kontrollima, kas teatis asjaomaste sideandmete säilitamise kohta on vajalik ühel või mitmel seaduses sätestatud eesmärkidest ja selle eesmärgi või nende eesmärkidega proportsionaalne ⁽³⁴⁶⁾.

3.3.1.1.3. Sekkumine seadmete töösse

- (210) Seadmete töösse sekkumise all mõistetakse selliste meetodite kogumit, mida kasutatakse mitmesuguste andmete saamiseks sellistest seadmetest ⁽³⁴⁷⁾ nagu arvutid, tahvelarvutid ja nutitelefonid, aga ka kaablid, juhtmed ja salvestusseadmed ⁽³⁴⁸⁾. Seadmete töösse sekkumine võimaldab saada andmeid nii sidevahendite kaudu edastatava teabe sisu kui ka seadmete kohta ⁽³⁴⁹⁾.
- (211) Vastavalt 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikele 1 on luureteenistuse poolt seadmete töösse sekkumiseks vaja luba, mis antakse uurimisvolituste seadusega kehtestatud nn topeltkinnituse menetluse alusel väljastatud määrusega, tingimusel et on olemas „seos Briti saartega“ ⁽³⁵⁰⁾. Ühendkuningriigi ametiasutuste esitatud selgituste kohaselt oleks olukorras, kus andmed edastatakse käesoleva otsuse kohaldamisalas Euroopa Liidust

⁽³⁴¹⁾ Vt 2016. aasta uurimisvolituste seaduse paragrahv 88.

⁽³⁴²⁾ Selline kasu võib olla olemas või prognoositav ning peab olema seotud seadusjärgsete eesmärkidega, milleks andmeid võib säilitada (sideandmete tegevusjuhendi punkt 17.17, vt joonealune märkus nr 323).

⁽³⁴³⁾ Need kaalutlused hõlmavad selle kindlakstegemist, kas säilitamisteatise puhul on täielik geograafiline ulatus vajalik ja proportsionaalne ning kas on vajalik ja proportsionaalne lisada või jätta välja isikute konkreetsed kirjeldused (sideandmete tegevusjuhendi punkt 17.17, vt joonealune märkus nr 323).

⁽³⁴⁴⁾ See aitab ministril võtta arvesse nii klientide eraelu puutumatuse sekkumise taset kui ka säilitatavate andmete tõenäolist kasu (sideandmete tegevusjuhendi punkt 17.17, vt joonealune märkus nr 323).

⁽³⁴⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahv 88.

⁽³⁴⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahv 89.

⁽³⁴⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 135 lõike 1 ja paragrahvi 198 lõike 1 kohaselt hõlmab „seade“ seadmeid, mis tekitavad elektromagnetilist, akustilist või muud kiirgust, ning mis tahes seadmeid, mida saab selliste seadmetega seoses kasutada.

⁽³⁴⁸⁾ „Code of Practice on Equipment Interference“ (seadmete töösse sekkumise tegevusjuhend), kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, punkt 2.2.

⁽³⁴⁹⁾ Seadmete andmed on määratletud 2016. aasta uurimisvolituste seaduse paragrahvis 100 kui süsteemi andmed ja andmed, mis a) on mõne sidevahendite kaudu edastatava sõnumi või muu teabega hõlmatud, sellele lisatud või sellega loogiliselt seotud (kas saatja poolt või muul viisil); b) mida on võimalik ülejäänud sõnumist või teabest loogiliselt eraldada ja c) kui see oleks nii eraldatud, ei ilmneks midagi sellest, mida võiks põhjendatult pidada teatise või teabe tähenduseks (kui see on olemas).

⁽³⁵⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikes 1 on lisaks ette nähtud, et määrus on vajalik, kui luureteenistuse toimingud kujutavad endast ühte või mitut rikkumist 1990. aasta arvutite väärkasutuse seaduse paragrahvide 1–3A alusel, mis enamikul juhtudel nii on, vt seadmete töösse sekkumise tegevusjuhendi punktid 3.32 ja 3.6–3.9). Vastavalt 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikele 2 on seos Briti saartega olemas juhul, kui a) luureteenistuse tegevus toimub Briti saartel (olenemata nende seadmete asukohast, mille töösse sekkutakse või võidakse sekkuda), b) luureteenistus usub, et seade, mille töösse sekkutakse või võidakse sekkuda, on või võib olla sekkumise toimumise ajal teataval hetkel Briti saartel või c) sekkumise eesmärk on hankida i) teavet, mida sidevahendite kaudu edastab isik või mis edastatakse isikule, kes viibib või kellest luureteenistus usub, et ta viibib sel ajal Briti saartel, ii) konfidentsiaalset teavet isiku kohta, kes viibib või kellest luureteenistus usub, et ta viibib sel ajal Briti saartel, või iii) teavet seadmete kohta, mis on osa punktides i või ii loetletud teabest või sellega seotud.

Ühendkuningriiki, alati olemas „seos Briti saartega“ ning kui seadmete töösse sekkutakse seoses selliste andmetega, kohaldataks seega 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikes 1 sätestatud kohustusliku määruse nõuet ⁽³⁵¹⁾.

- (212) Normid, mis reguleerivad määruste tegemist suunatud sekkumiseks seadmete töösse, on sätestatud 2016. aasta uurimisvolituste seaduse 5. osas. Sarnaselt suunatud pealtkuulamisele peab suunatud sekkumine seadmete töösse olema seotud konkreetse sihtmärgiga, mis tuleb määruks kindlaks määrata ⁽³⁵²⁾. Sihtmärgi kindlaksmääramise üksikasjad sõltuvad konkreetsest küsimusest ja selliste seadmete liigist, mille töösse kavatsetakse sekkuda. Täpsemalt on uurimisvolituste seaduse paragrahvi 115 lõikes 3 sätestatud elemendid, mis tuleb määruks esitada (nt isiku või organisatsiooni nimi, asukoha kirjeldus), sõltuvalt näiteks sellest, kas sekkumine on seotud seadmega, mis kuulub konkreetsele isikule või organisatsioonile või isikute rühmale või on nende kasutuses või valduses, asub konkreetsetes kohas jne ⁽³⁵³⁾. Eesmärk, milleks võib välja anda seadmete töösse suunatud sekkumise määruse, sõltub seda taotlevast ametiasutusest ⁽³⁵⁴⁾.
- (213) Sarnaselt suunatud pealtkuulamisele peab luba andev asutus kaaluma, kas meede on konkreetse eesmärgi saavutamiseks vajalik ja kas see on proportsionaalne eesmärgiga, mida soovitakse saavutada ⁽³⁵⁵⁾. Lisaks tuleks kaaluda, kas on võetud kaitsemeetmeid seoses andmete turvalisuse, säilitamise ja avalikustamisega ning seoses nende avalikustamisega välisriigile ⁽³⁵⁶⁾ (vt põhjendus 196).
- (214) Määruse peab heaks kiitma kohtuvolinik, välja arvatud kiireloomulistel juhtudel ⁽³⁵⁷⁾. Viimasel juhul tuleb kohtuvolinikku teavitada määruse väljastamisest ja ta peab selle kolme tööpäeva jooksul heaks kiitma. Kui kohtuvolinik keeldub seda heaks kiitmast, kaotab määruks kehtivuse ja seda ei saa pikendada ⁽³⁵⁸⁾. Peale selle on kohtuvolinikul õigus nõuda, et määruse alusel kogutud andmed kustutatakse ⁽³⁵⁹⁾. Asjaolu, et määruks anti välja kiirkorras ei mõjuta järelkontrolli (vt põhjendused 244–255) või üksikisikute võimalusi kasutada õiguskaitsevahendeid (vt põhjendused 260–270). Üksikisikud saavad esitada kaebuse teabevolinikule või asutuste väidetava tegevusega seotud nõude uurimisvolituste kohtule tavalises korras. Kui volinik otsustab, kas kiita määruks heaks või mitte, teeb ta kõikidel juhtudel vajalikkuse ja proportsionaalsuse kontrolli, mida kohaldatakse suunatud pealtkuulamise taotluste suhtes ⁽³⁶⁰⁾ (vt põhjendus 192).
- ⁽³⁵¹⁾ Täielikkuse huvides tuleks märkida, et isegi olukordades, kus seos Briti saartega puudub ja seadmete töösse sekkumise meetodi kasutamise suhtes ei kohaldata seetõttu 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikes 1 sätestatud kohustusliku määruse nõuet, näeb tegevuskord ette, et luureteenistus, kes kavatseb tegeleda tegevusega, milleks ta saab hankida laialdast seadmete töösse sekkumist käsitleva määruse, hangib sellise määruse (vt seadmete töösse sekkumise tegevusjuhendi punkt 3.24). Isegi kui 2016. aasta uurimisvolituste seaduse kohane seadmete töösse sekkumise määruks ei ole seaduse ega tegevuskorra alusel nõutav, kohaldatakse luureteenistuste meetmete suhtes mitmesuguseid tingimusi ja piiranguid 1994. aasta luureteenistuste seaduse paragrahvi 7 alusel. See hõlmab eelkõige nõuet, et selleks peab loa andma minister, kes peab olema veendunud, et ükski meede ei lähe kaugemale sellest, mis on vajalik luureteenistuse ülesannete nõuetekohaseks täitmiseks.
- ⁽³⁵²⁾ 2016. aasta uurimisvolituste seaduse paragrahvis 115 on sätestatud, et määruks peab sisaldama sihtmärki moodustavate isikute, organisatsioonide, asukoha või isikute rühma nime või kirjeldust, uurimise laadi kirjeldust ja nende tegevuste kirjeldust, mille jaoks seadmeid kasutatakse. Samuti tuleb selles kirjeldada seadmete liiki ja toiminguid, mida määruse adressaadil on lubatud teha.
- ⁽³⁵³⁾ Vt ka seadmete töösse sekkumise tegevusjuhendi punkt 5.7, vt joonealune märkus nr 348.
- ⁽³⁵⁴⁾ Riiklikud julgeolekuasutused võivad taotleda seadmete töösse sekkumise määruks, kui see on vajalik riikliku julgeoleku eesmärgil, raskete kuritegude avastamiseks ja/või Ühendkuningriigi majandusliku heaolu huvides, kui see on oluline ka riigi julgeoleku huvides (2016. aasta uurimisvolituste seaduse paragrahvid 102–103). Olenevalt asutusest võidakse taotleda seadmete töösse sekkumise määruks õiguskaitse eesmärgil, kui seda on vaja raske kuriteo avastamiseks või tõkestamiseks või isiku surma või füüsilise või vaimse tervise kahjustamise ärahoidmiseks või isiku füüsilisele või vaimsele tervisele tekitatud kahju leevendamiseks (vt 2016. aasta uurimisvolituste seaduse paragrahvi 106 lõiked 1 ja 3).
- ⁽³⁵⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 102 lõige 1.
- ⁽³⁵⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 129–131.
- ⁽³⁵⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahv 109.
- ⁽³⁵⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 109 lõige 4.
- ⁽³⁵⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 110 lõike 3 punkt b. Seadmete töösse sekkumise tegevusjuhendi punkti 5.67 kohaselt määratakse kiireloomulises kindlaks, kontrollides kas mõistlikult võttes oleks võimalik taotleda kohtuvoliniku heakskiitu määruse väljaandmisele nii, et määruks saaks vastavalt tegevus- või uurimisvajadusele õigeaegselt kasutada. Kiireloomulised määruksed peaksid olema kahte liiki: i) vahetu oht elule või raske tervisekahjustuse tekkimise vahetu oht – näiteks kui inimene on röövitud ja hinnatakse, et tema elu on vahetus ohus; või ii) piiratud kestusega võimalus koguda luureandmeid või uurida kuritegu – näiteks kui Ühendkuningriiki on sisenemas A-klassi narkootikumide saadeti ja õiguskaitseasutused tahavad raske kuriteo toimepanijaid jälgida, selleks et neid kinni pidada. Vt joonealune märkus nr 348.
- ⁽³⁶⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahv 108.

- (215) Peale selle kohaldatakse ka seadmete töösse sekkumise suhtes suunatud pealtkuulamise suhtes kohaldatavaid erikaitsemeetmeid seoses määruse kehtivusaja, pikendamise ja muutmisega ning parlamendiliikmete, kutsesaladuse alla kuuluva teabe ja ajakirjandusliku materjali pealtkuulamisega (vt täpsemalt põhjendus 193).

3.3.1.1.4. Laialdaste volituste kasutamine

- (216) Laialdasi volitusi reguleerib 2016. aasta uurimisvolituste seaduse 6. osa. Üksikasjalikumalt on laialdaste volituste kasutamise suhtes kohaldatavaid nõudeid kirjeldatud tegevusjuhendites. Kuigi Ühendkuningriigi õiguses ei ole „laialdast volitust“ määratletud, on seda 2016. aasta uurimisvolituste seadusega seoses kirjeldatud kui selliste suurte andmehulkade kogumist ja säilitamist, mille valitsus on saanud eri vahendite abil (nt laialdase pealtkuulamise volitused, laialdane andmete kogumine, laialdane seadmete töösse sekkumine ja suured isikuandmete kogumid) ning millele ametiasutused saavad hiljem juurde pääseda. Selle kirjelduse täpsustamiseks on selgitatud, mida „laialdane volitus“ endast ei kujuta: see ei ole võrdväärne nn massilise jälgimisega, mille suhtes ei kohaldata piiranguid ega kaitsemeetmeid. Nagu allpool selgitatud, kaasnevad laialdaste volitustega just piirangud ja kaitsemeetmed, mille eesmärk on tagada, et andmetele ei võimaldata valimatut või põhjendamatu juurdepääsu⁽³⁶¹⁾. Eelkõige võib laialdasi volitusi kasutada üksnes juhul, kui on loodud seos riikliku luureasutuse kavandatava tehnilise meetme ja tegevuseesmärgi vahel, milleks sellist meetet taotletakse.
- (217) Lisaks on laialdased volitused kättesaadavad ainult luureasutustele ja nende suhtes kohaldatakse alati ministri väljaantud määrust, mille on heaks kiitnud kohtuvolinik. Luureandmete kogumise vahendite valimisel tuleb pöörata tähelepanu sellele, kas asjaomast eesmärki on võimalik saavutada „vähem sekkuvate vahenditega“⁽³⁶²⁾. Selline lähenemisviis tuleneb proportsionaalsuse põhimõttele tuginevast õigusraamistikust ja seab seetõttu andmete suunatud kogumise laialdase kogumise ees esikohale.

3.3.1.1.4.1. Laialdane pealtkuulamine ja laialdane seadmete töösse sekkumine

- (218) Laialdase pealtkuulamise kord on sätestatud 2016. aasta uurimisvolituste seaduse 6. osa 1. peatükis; sama osa 3. peatükis reguleeritakse laialdast seadmete töösse sekkumist. Kuna need korrad on sisuliselt samad, analüüsitakse kõnealuste määruste suhtes kohaldatavaid tingimusi ja täiendavaid kaitsemeetmeid koos.

i) Määruse väljaandmise tingimused ja kriteeriumid

- (219) Laialdase pealtkuulamise määrus on piiratud side pealtkuulamisega selliste sõnumite edastamise käigus, mille on saatnud või vastu võtnud väljaspool Briti saari viibivad isikud⁽³⁶³⁾ („välismaaga seotud side“⁽³⁶⁴⁾), samuti muude asjakohaste andmete pealtkuulamise ja sellele järgneva pealtkuulatud materjali valimisega

⁽³⁶¹⁾ Lord David Andersoni (terrorismialaste õigusaktide sõltumatu ülevaataja) poolt enne 2016. aasta uurimisvolituste seaduse heakskiitmist esitatud laialdaste volituste aruande kohaselt „peaks olema selge, et laialdaste andmete kogumine ja säilitamine ei võrdu nn massilise jälgimisega. Laialdaste volituste alla kuuluv õigussüsteem hõlmab alati piiranguid ja kaitsemeetmeid, mille eesmärk on tagada, et tundlikele andmetele [...] ei võimaldata valimatut või põhjendamatu juurdepääsu. Seaduse eelnõus on sellised piirangud ja kaitsemeetmed kindlasti olemas.“ Lord David Anderson, „Report of the bulk power review“ (Aruanne laialdaste volitustega seotud läbivaatamise kohta), august 2016, punkt 1.9 (rõhuasetus lisatud), kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF.

⁽³⁶²⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 2 lõige 2. Vt näiteks laialdase sideandmete kogumise tegevusjuhendi punkt 4.11, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf.

⁽³⁶³⁾ Briti saared hõlmavad Ühendkuningriiki, Kanalisaari ja Mani saart ning on määratletud 1978. aasta tõlgendamiseseaduse 1. lisas, mis on kättesaadav aadressil <https://www.legislation.gov.uk/ukpga/1978/30/schedule/1>.

⁽³⁶⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 136 kohaselt mõistetakse „välismaaga seotud side“ all järgmist: i) väljaspool Briti saari asuvate isikute sidevahendite kaudu saadetud sõnumid või ii) väljaspool Briti saari asuvate isikute sidevahendite kaudu saadud sõnumid. Ühendkuningriigi ametiasutuste kinnitusel hõlmab see kord ka kahe väljaspool Briti saari asuva isiku vahelist suhtlust. Euroopa Inimõiguste Kohtu suurkoda leidis asjas Big Brother Watch ja teised vs. Ühendkuningriik (vt joonealune märkus nr 279), punkt 376, sarnase side määratluse (nimetades seda „välismaaiseks sideks“) kohta, mida tohtis 2000. aasta uurimisvolituste reguleerimise seaduse alusel laialdaselt pealt kuulata, et see on piisavalt piiritletud ja ettenähtav.

läbivaatamiseks⁽³⁶⁵⁾. Laialdase seadmete töösse sekkumise määrus⁽³⁶⁶⁾ annab adressaadile õiguse sekkuda mis tahes seadmete töösse, et saada teavet välismaaga seotud side kohta (mis hõlmab kõnet, muusikat, helisid, visuaalseid kujutisi või mis tahes liiki andmeid), seadmete andmeid (andmed, mis võimaldavad või hõlbustavad postiteenuse, telekommunikatsioonisüsteemi või telekommunikatsiooniteenuse toimimist) või muud teavet⁽³⁶⁷⁾.

- (220) Minister võib laialdase volituse määruse välja anda ainult luureteenistuse juhi taotluse alusel⁽³⁶⁸⁾. Määrust, millega lubatakse laialdast pealtkuulamist või seadmete töösse sekkumist, tohib välja anda üksnes juhul, kui see on vajalik riikliku julgeoleku huvides või raske kuriteo ennetamiseks või avastamiseks või Ühendkuningriigi majandusliku heaolu huvides, kui see on riikliku julgeoleku seisukohast oluline⁽³⁶⁹⁾. Lisaks on 2016. aasta uurimisvolituste seaduse paragrahvi 142 lõikega 7 ette nähtud, et laialdase pealtkuulamise määruse vajalikkust tuleb selgitada üksikasjalikumalt kui lihtsalt viitega „riigi julgeoleku huvidele“, „Ühendkuningriigi majanduslikule heaolule“ ja „raskete kuritegude ennetamisele ja nende vastu võitlemisele“; tuleb luua seos taotletava meetme ja ühe või mitme operatiiveesmärgi vahel, mida tuleb määruses selgitada.
- (221) Operatiiveesmärgi valik on mitmekihilise protsessi tulemus. Paragrahvi 142 lõikes 4 on sätestatud, et määruses nimetatud operatiiveesmärgid peavad olema kindlaks määratud luureteenistuste juhtide hallatavas loetelus eesmärkidena, mida nad peavad operatiiveesmärkideks, mille puhul võib läbivaatamiseks valida laialdase pealtkuulamise määruse alusel pealtkuulatavat sisu või teiseid andmeid. Operatiiveesmärkide loetelu peab heaks kiitma minister. Minister võib anda sellise nõusoleku üksnes juhul, kui ta on veendunud, et operatiiveesmärk on määratletud üksikasjalikumalt kui määruse väljaandmise lubamise üldised alused (riiklik julgeolek või riiklik julgeolek ja majanduslik heaolu või raskete kuritegude ennetamine)⁽³⁷⁰⁾. Iga asjaomase kolmekuulise ajavahemiku lõpus peab minister esitama parlamendi luure- ja julgeolekukomisjonile operatiiveesmärkide loetelu koopia. Peale selle peab peaminister vähemalt kord aastas operatiiveesmärkide loetelu läbi vaatama⁽³⁷¹⁾. Kõrgema astme kohus märkis: „Kõnealuseid meetmeid ei tohi pidada ebaolulisteks kaitsemeetmeteks, kuna need moodustavad koos keeruka aruandlusviiside kogumi, mis hõlmab nii parlamenti kui ka valitsuse liikmeid kõige kõrgemal tasemel“⁽³⁷²⁾.
- (222) Sellised operatiiveesmärgid piiravad ka pealtkuulamismaterjali valikut läbivaatamise etapiks. Laialdaste volituste määruse alusel kogutud materjali läbivaatamiseks tehtav valik peab olema operatiiveesmärgi(/-eesmärgi) silmas pidades põhjendatud. Nagu Ühendkuningriigi ametiasutused on selgitanud, tähendab see, et minister peab hindama läbivaatamise praktilist korda juba määruse väljaandmise etapil, esitades piisavalt üksikasju 2016. aasta uurimisvolituste seaduse paragrahvide 152 ja 193 tulenevate seadusjärgsete kohustuste täitmiseks⁽³⁷³⁾. Kõnealuse korra kohta ministrile esitatavad üksikasjad peaksid sisaldama näiteks teavet (vajaduse korral) selle kohta, kuidas filtreerimiskord võib määruse jõusoleku ajal muutuda⁽³⁷⁴⁾. Selle protsessi ning filtreerimis- ja läbivaatamisetappide suhtes kohaldatavate kaitsemeetmete üksikasjad on esitatud põhjenduses 229.
-
- ⁽³⁶⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 136 lõige 4. Ühendkuningriigi valitsuselt saadud selgituste kohaselt saab laialdast pealtkuulamist kasutada näiteks selleks, et välja selgitada tundmatud ohud Ühendkuningriigi riiklikule julgeolekule, filtreerides ja analüüsides pealtkuulatavat materjali, et teha kindlaks luureväärtusega teabevahetus (Ühendkuningriigi selgitava raamistiku jaotis H: „National Security“ (Riiklik julgeolek), lk 27–28, vt joonealune märkus nr 29). Nagu Ühendkuningriigi ametiasutused on selgitanud, saab selliseid vahendeid kasutada seoste loomiseks teadaolevate huvipakkuvate subjektide vahel, samuti selliste isikute tegevuse jälgede otsimiseks, kes ei pruugi olla veel teada, kuid kes uurimise jooksul esile kerkivad, ning selliste tegevusmodelite kindlakstegemiseks, mis võivad viidata Ühendkuningriiki ähvardavale ohule.
- ⁽³⁶⁶⁾ Vastavalt 2016. aasta uurimisvolituste seaduse paragrahvi 13 lõikele 1 on luureteenistuse poolt seadmete töösse sekkumiseks vaja luba, mis antakse uurimisvolituste seadusega kehtestatud määrusega, tingimusel et on olemas „seos Briti saartega“, vt põhjendus 211.
- ⁽³⁶⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahv 176. Laialdase seadmete töösse sekkumise määrust ei tohi anda toiminguteks, mis (v.a juhul, kui neid tehakse seadusliku volituse alusel) kujutavad endast ebaseaduslikku pealtkuulamist (välja arvatud salvestatud sõnumite puhul). Vastavalt Ühendkuningriigi selgitavale raamistikule võib saadud teave olla vajalik huvipakkuvate subjektide kindlakstegemiseks ja vastab tavapäraselt asjakohastele laiaulatuslikele operatsioonidele (Ühendkuningriigi selgitava raamistiku H osa: „National Security“ (Riiklik julgeolek), lk 28, vt joonealune märkus nr 29).
- ⁽³⁶⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 138 lõige 1 ja paragrahvi 178 lõige 1.
- ⁽³⁶⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 138 lõige 2 ja paragrahvi 178 lõige 2.
- ⁽³⁷⁰⁾ Ühendkuningriigi ametiasutuste esitatud selgituste kohaselt võib operatiiveesmärk näiteks piirata meetme kohaldamisala ohu esinemisega mõnes konkreetses geograafilises piirkonnas.
- ⁽³⁷¹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 142 lõiked 4–10.
- ⁽³⁷²⁾ Kõrgema astme kohtu otsus kohtuasjas Liberty, [2019], EWHC 2057 (Admin), punkt 167.
- ⁽³⁷³⁾ 2016. aasta uurimisvolituste seaduse paragrahvidega 152 ja 193 on ette nähtud, et a) läbivaatamiseks valiku tegemisel lähtutakse ainult määruses märgitud operatiiveesmärkidest, b) läbivaatamiseks valiku tegemine lähtub kõigis olukordades vajalikkuse ja proportsionaalsuse põhimõttest ning c) läbivaatamiseks valiku tegemisel ei rikota keeldu, mis välistab sellise materjali valiku ja selliste sõnumite tuvastamise, mille on saatnud isikud või mis on saadatud isikutele, kes sel ajal viibivad teadaolevalt Briti saartel.
- ⁽³⁷⁴⁾ Vt side pealtkuulamise tegevusjuhendi punkt 6.6, vt joonealune märkus nr 278.

- (223) Laialdast volitust võib lubada ainult siis, kui see on proportsionaalne eesmärgiga, mida soovitakse saavutada ⁽³⁷⁵⁾. Nagu on sätestatud pealtkuulamise tegevusjuhendis, hõlmab proportsionaalsuse hindamine „eraelu puutumatusse sekkumise tõsiduse (ja muude paragrahvi 2 lõikes 2 esitatud kaalutluste) tasakaalustamist vajadusega juurdluse, tegevuse või suutlikkuse seisukohast olulise tegevuse järele“. Lubatud toimingud peaksid pakkuma realistlikku väljavaadet oodatava kasu saamiseks ja ei tohiks olla ebaproportsionaalsed ega meelevaldsed“ ⁽³⁷⁶⁾. Nagu juba mainitud, tähendab see praktikas seda, et proportsionaalsuse kriteerium põhineb tasakaalu otsimisel taotletava eesmärgi (operatiiveesmärk/-eesmärgid) ja olemasolevate tehniliste võimaluste vahel (nt suunatud või laialdane pealtkuulamine, seadmete töösse sekkumine, sideandmete kogumine), eelistades kõige vähem sekkuvaid vahendeid (vt põhjendused 181 ja 182). Kui eesmärgi saavutamiseks sobib rohkem kui üks meede, tuleb eelistada vähem sekkuvaid vahendeid.
- (224) Täiendav kaitsemeede taotletava meetme proportsionaalsuse hindamiseks on tagatud nõudega, et minister peab saama asjakohase teabe, mida ta vajab nõuetekohase hinnangu andmiseks. Eelkõige on pealtkuulamise tegevusjuhendis ja seadmete töösse sekkumise tegevusjuhendis nõutud, et pädeva asutuse esitatud taotluses tuleb märkida taotluse taust, pealtkuulitava side kirjeldus, abi osutamiseks vajalikud telekommunikatsioonioperaatorid, tegevusluba vajavate toimingute kirjeldus, operatiiveesmärgid ning selgitus, miks taotletav toiming on vajalik ja proportsionaalne ⁽³⁷⁷⁾.
- (225) Samuti on oluline, et ministri otsuse määruse väljaandmise kohta peab heaks kiitma sõltumatu kohtuvolinik, kes hindab kavandatava meetme vajalikkuse ja proportsionaalsuse hindamist, kasutades samu põhimõtteid, mida kohaldaks kohus kohtuliku kontrolli taotluse suhtes ⁽³⁷⁸⁾. Täpsemalt vaatab kohtuvolinik läbi ministri järeldused selle kohta, kas määrus on vajalik ja kas toiming on proportsionaalne, pidades silmas 2016. aasta uurimisvolituste seaduse paragrahvi 2 lõikes 2 sätestatud põhimõtteid (üldised kohustused seoses eraelu puutumatusega). Samuti vaatab kohtuvolinik läbi ministri järeldused selle kohta, kas iga määruks nimetatud operatiiveesmärgi puhul on valiku tegemine vajalik või võib olla vajalik. Kui kohtuvolinik keeldub määruse väljaandmise otsust heaks kiitmast, võib minister kas: i) otsust aktsepteerida ja seega määrust mitte välja anda või ii) suunata küsimuse otsustamiseks uurimisvolituste volinikule (välja arvatud juhul, kui uurimisvolituste volinik on teinud esialgse otsuse) ⁽³⁷⁹⁾.
- ii) *Täiendavad kaitsemeetmed*
- (226) 2016. aasta uurimisvolituste seadusega on kehtestatud täiendavad piirangud laialdase volituse määruse kestusele, pikendamisele ja muutmisele. Määruse kehtivusaeg võib olla maksimaalselt kuus kuud ning kõik otsused määrust pikendada või muuta (välja arvatud väiksemad muudatused) peab heaks kiitma ka kohtuvolinik ⁽³⁸⁰⁾. Pealtkuulamise tegevusjuhendis ja seadmete töösse sekkumise tegevusjuhendis on täpsustatud, et määruse operatiiveesmärkide muutmist käsitatakse määruse olulise muudatusena ⁽³⁸¹⁾.

⁽³⁷⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 138 lõike 1 punktid b ja c ning paragrahvi 178 punktid b ja c.

⁽³⁷⁶⁾ Side pealtkuulamise tegevusjuhendi punkt 4.10, vt joonealune märkus nr 278.

⁽³⁷⁷⁾ Side pealtkuulamise tegevusjuhendi punkt 6.20, vt joonealune märkus nr 278, ja seadmete töösse sekkumise tegevusjuhendi punkt 6.13, vt joonealune märkus nr 348.

⁽³⁷⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 138 lõike 1 punkt g ja paragrahvi 178 lõike 1 punkt f. Euroopa Inimõiguste Kohus on märkinud, et just sõltumatu organi antav eelnev luba on laialdase pealtkuulamise puhul oluline kaitsemeede kuritarvituste vastu. Euroopa Inimõiguste Kohus, Big Brother Watch ja teised vs. Ühendkuningriik (vt joonealune märkus 269), punktid 351 ja 352. Tuleb silmas pida, et see kohtuotsus puudutas varasemat õigusakti (2000. aasta uurimisvolituste reguleerimise seadus), mis ei sisaldanud mõningaid 2016. aasta uurimisvolituste seadusega kehtestatud kaitsemeetmeid (sealhulgas sõltumatu kohtuvoliniku eelneva loa nõuet).

⁽³⁷⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 159 lõiked 3 ja 4.

⁽³⁸⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 143–146 ja paragrahvid 184–188. Kiireloomulise muudatuse korral võib minister muudatuse teha ilma heakskiiduta, kuid peab sellest teavitama volinikku ja seejärel peab volinik otsustama, kas muudatus heaks kiita või tagasi lükata (2016. aasta uurimisvolituste seaduse paragrahv 147). Määrus tuleb tühistada, kui see ei ole enam vajalik või proportsionaalne või kui pealtkuulitava sisu, metaandmete või muude määruse alusel saadud andmete läbivaatamine ei ole enam vajalik ühelgi määruks märgitud operatiiveesmärgil (2016. aasta uurimisvolituste seaduse paragrahvid 148 ja 189).

⁽³⁸¹⁾ Side pealtkuulamise tegevusjuhendi punktid 6.44–6.47, vt joonealune märkus nr 278, ja seadmete töösse sekkumise tegevusjuhendi punkt 6.48, vt joonealune märkus nr 348.

- (227) Sarnaselt suunatud pealtkuulamisega on 2016. aasta uurimisvolituste seaduse 6. osas sätestatud, et minister peab tagama, et kehtestatud on kord, millega nähakse ette kaitsemeetmed, mida kohaldatakse määruse alusel saadud materjali säilitamise ja avalikustamise⁽³⁸²⁾ ning samuti selle välisriigile avalikustamise⁽³⁸³⁾ suhtes. Eelkõige on 2016. aasta uurimisvolituste seaduse paragrahvi 150 lõikega 5 ja paragrahvi 191 lõikega 5 ette nähtud, et kõiki kõnealuse määruse alusel kogutud materjalist tehtud koopiaid tuleb säilitada turvaliselt ja need hävitatakse niipea, kui nende säilitamiseks ei ole enam asjakohast alust; seaduse paragrahvi 150 lõikes 2 ja paragrahvi 191 lõikes 2 on aga sätestatud, et nende isikute arv, kellele materjal avalikustatakse, ja ulatus, mil määral materjal avalikustatakse, kättesaadavaks tehakse või kopeeritakse, peab piirduma seadusest tulenevatel eesmärkidel vajaliku miinimumiga⁽³⁸⁴⁾.
- (228) Kui kas laialdase pealtkuulamise või laialdase seadmete töösse sekkumise kaudu kogutud materjal antakse üle kolmandale riigile („avalikustamine välisriigile“), on 2016. aasta uurimisvolituste seaduses sätestatud, et minister peab tagama asjakohase korra, millega tagatakse, et kõnealuses kolmandas riigis on kehtestatud andmete turvalisuse, säilitamise ja avalikustamise valdkonnas sarnased kaitsemeetmed⁽³⁸⁵⁾. Peale selle on 2018. aasta andmekaitseaduse paragrahvis 109 sätestatud erinõuded isikuandmete rahvusvahelise edastamise kohta luureteenistuste poolt kolmandatele riikidele või rahvusvahelistele organisatsioonidele ning selle sätte kohaselt ei tohi isikuandmeid edastada väljaspool Ühendkuningriiki asuvale riigile või territooriumile või rahvusvahelisele organisatsioonile, välja arvatud juhul, kui edastamine on vajalik ja proportsionaalne vastutava töötleja seadusjärgsete ülesannete täitmiseks või muudel eesmärkidel, mis on sätestatud 1989. aasta julgeolekuteenistuse seaduse paragrahvi 2 lõike 2 punktis a või 1994. aasta luureteenistuste seaduse paragrahvi 2 lõike 2 punktis a ja paragrahvi 4 lõike 2 punktis a⁽³⁸⁶⁾. Oluline on, et need nõuded kehtivad ka juhtudel, kui 2018. aasta andmekaitseaduse paragrahvi 110 kohaselt tuginetakse riigi julgeoleku erandile, kuna 2018. aasta andmekaitseaduse paragrahvis 110 ei ole nimetatud 2018. aasta andmekaitseaduse paragrahvi 109 nende sätete hulgas, mille kohaldamise võib peatada, kui riigi julgeoleku tagamiseks on vaja teha erandeid mõningatest sätetest.
- (229) Kui määrus on heaks kiidetud ja andmeid on laialdaselt kogutud, tehakse andmete seas enne läbivaatamist valik. Valiku- ja läbivaatamisetapi proportsionaalsust kontrollib täiendavalt analüütik, kes määrab kindlaks valikukriteeriumid, lähtudes määruks sisalduvatest operatiiveesmärkidest (ja võimalikust filtreerimiskorrast). Nagu on sätestatud uurimisvolituste seaduse paragrahvides 152 ja 193, peab minister määruse väljaandmisel tagama, et on kehtestatud kord, millega garanteeritakse, et materjali valik toimub üksnes kindlaksmääratud operatiiveesmärkidel ning et see vastab igas olukorras vajalikkuse ja proportsionaalsuse kriteeriumidele. Sellega seoses selgitasid Ühendkuningriigi ametiasutused, et laialdaselt pealtkuulatava materjali hulgast tehakse esmane valik automaatselt filtreerimise teel, et kõrvaldada andmed, mis tõenäoliselt ei ole riigi julgeoleku seisukohast olulised. Filtreid muudetakse aeg-ajalt (sest internetiliikluse skeemid, liigid ja protokollid muutuvad) ning need sõltuvad tehnoloogiast ja tegevuskontekstist. Pärast seda etappi saab andmeid läbivaatamiseks valida ainult siis, kui see on vajalik määruks sätestatud operatiiveesmärkide täitmiseks⁽³⁸⁷⁾. 2016. aasta uurimisvolituste seaduses sätestatud kaitsemeetmeid kogutud materjali läbivaatamiseks kohaldatakse kõigi andmeliikide suhtes (nii pealtkuulatava sisu kui ka teisest andmete suhtes)⁽³⁸⁸⁾. 2016. aasta uurimisvolituste seaduse paragrahvides 152 ja 193 on sätestatud ka üldine keeld, millega välistatakse läbivaatamiseks sellise materjali valik, mis viitab Briti saartel viibivate isikute poolt või neile saadetud vestlustele. Kui ametiasutused soovivad selliseid materjale uurida, esitavad nad taotluse 2016. aasta uurimisvolituste seaduse 2. ja 4. osa alusel suunatud läbivaatamise määruse saamiseks, mille annab välja minister ja kiidab heaks kohtuvolinik⁽³⁸⁹⁾. Kui isik läbivaatamiseks pealtkuulatavat sisu valides rikub teadlikult õigusaktides sätestatud nõudeid, ⁽³⁹⁰⁾ paneb ta toime kuriteo ⁽³⁹¹⁾.

⁽³⁸²⁾ 2016. aasta uurimisvolituste seaduse paragrahv 156.

⁽³⁸³⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 150 ja 191.

⁽³⁸⁴⁾ Euroopa Inimõiguste Kohtu suurkoda leidis asjas Big Brother Watch ja teised vs. Ühendkuningriik (vt joonealune märkus nr 268), et 2000. aasta uurimisvolituste reguleerimise seaduses sätestatud täiendavate kaitsemeetmete süsteem andmete säilitamiseks, nende juurdepääsuks ja nende avalikustamiseks on piisav, vt punktid 392–394 ja 402–405. Sama kaitsemeetmete süsteem on ette nähtud 2016. aasta uurimisvolituste seadusega.

⁽³⁸⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 151 ja 192.

⁽³⁸⁶⁾ Nende eesmärkide kohta vt joonealune märkus 312.

⁽³⁸⁷⁾ Side pealtkuulamise tegevusjuhendites on sellega seoses täpsustatud, et „need töötlemissüsteemid töötlevad sideühenduste või -signaalide andmeid, mida pealtkuulav asutus on otsustanud pealt kuulata. Seejärel kohaldatakse nende ühenduste ja signaalide liikluse suhtes teatavat filtreerimisaset, mis on mõeldud võimaliku luureväärtusega sõnumiliikide väljavõtmiseks, jättes kõrvale need sõnumiliigid, mille luureväärtus on kõige vähem tõenäoline. Filtreerimine on töötlemissüsteemide lõikes erinev ja selle tulemusena jäetakse märkimisväärne osa nende linkide ja signaalide kaudu toimuvast teabevahetusest automaatselt kõrvale. Seejärel võidakse läbi viia täiendavaid keerulisi otsinguid, et teha kindlaks sõnumid, millel on kõige tõenäolisemalt suurim luureväärtus ja mis on seotud ameti põhikirjajärgsete ülesannetega. Need sõnumid võidakse seejärel valida läbivaatamiseks määruks kindlaks määratud ühel või mitmel operatiiveesmärgil, kui on täidetud vajalikkuse ja proportsionaalsuse tingimused. Volitatud isikud saavad läbivaatamiseks valida ainult need sõnumid, mida ei ole välja filtreeritud“ (side pealtkuulamise tegevusjuhendi punkt 6.6, vt joonealune märkus nr 278).

⁽³⁸⁸⁾ Vt 2016. aasta uurimisvolituste seaduse paragrahvi 152 lõike 1 punktid a ja b, mille kohaselt tohib mõlemat liiki andmeid (pealtkuulatavat sisu ja teiseseid andmeid) läbi vaadata üksnes märgitud eesmärgil ning läbivaatamine peab kõigis olukordades lähtuma vajalikkuse ja proportsionaalsuse põhimõttest.

⁽³⁸⁹⁾ Sellist määrust ei ole vaja, kui Briti saartel viibivate isikutega seotud andmed on „teisesed andmed“ (vt 2016. aasta uurimisvolituste seaduse paragrahvi 152 lõike 1 punkt c).

⁽³⁹⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 152 ja 193.

⁽³⁹¹⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 155 ja 196.

- (230) Analüütiku poolt materjali valiku kohta tehtava hindamise üle teostab järelkontrolli uurimisvolituste volinik, kes hindab vastavust 2016. aasta uurimisvolituste seaduses läbivaatamisetapi jaoks kehtestatud konkreetsetele kaitsemeetmetele ⁽³⁹²⁾ (vt ka põhjendus 229). Uurimisvolituste volinik peab kontrollima (sealhulgas auditi, inspekteerimise ja uurimise kaudu) seda, kuidas ametiasutused kasutavad 2016. aasta uurimisvolituste seaduses mainitud uurimisvolitusi ⁽³⁹³⁾. Sellega seoses on pealtkuulamise tegevusjuhendis ja seadmete töösse sekkumise tegevusjuhendis selgitatud, et asutus peab säilitama dokumente edasiseks läbivaatamiseks ja auditeerimiseks ning nendes dokumentides tuleb kirjeldada, miks on volitatud isikute juurdepääs materjalidele vajalik ja proportsionaalne ning millised on kohaldatavad operatiiveesmärgid ⁽³⁹⁴⁾. Näiteks järeldas uurimisvolituste voliniku büroo oma 2018. aasta aruandes, ⁽³⁹⁵⁾ et analüütikute esitatud põhjendused teatavate laialdaselt kogutud materjalide läbivaatamiseks vastasid nõutavale proportsionaalsuse tasemele, sest kirjeldasid piisavalt üksikasjalikult päringute põhjusi seoses taotletava eesmärgiga ⁽³⁹⁶⁾. 2019. aasta aruandes märkis uurimisvolituste voliniku büroo selgesti, et kavatseb jätkata laialdaste pealtkuulamiste kontrollide, sealhulgas põhjalikult uurida tunnuseid ja otsinguparameetreid ⁽³⁹⁷⁾. Samuti uurib ta hoolikalt ja juhtumipõhiselt jälgimismeetmete valikut (suunatud või laialdane) määruse taotluste läbivaatamisel nii topeltkinnituse menetluse käigus kui ka kontrollide ajal ⁽³⁹⁸⁾. Seda lisajärelevalvet võetakse nõuetekohaselt arvesse, kui komisjon teeb käesoleva otsuse üle järelevalvet, millele on osutatud põhjendustes 281–284.

3.3.1.1.4.2. Sideandmete laialdane kogumine

- (231) 2016. aasta uurimisvolituste seaduse 6. osa 2. peatükk reguleerib laialdase andmekogumise määrsi, millega antakse adressaadile luba nõuda telekommunikatsioonioperaatorilt operaatori valduses olevate sideandmete avaldamist või hankimist. Nende määrustega volitatakse ka taotluse esitanud asutust valida andmeid edasiseks läbivaatamiseks. Nagu sideandmete suunatud säilitamise ja hankimise puhul (vt põhjendus 199), ei ole ka sideandmete laialdane kogumine tavaliselt seotud käesoleva otsuse kohaselt Ühendkuningriigiile edastatavate ELi andmesubjektide isikuandmetega. 2016. aasta uurimisvolituste seaduse 6. osa 2. peatüki kohane sideandmete avalikustamise kohustus hõlmab andmeid, mida Ühendkuningriigi telekommunikatsioonioperaatorid koguvad otse telekommunikatsiooniteenuse kasutajatelt ⁽³⁹⁹⁾. Sedalaadi kliendiandmete töötlemine ei hõlma üldjuhul andmete edastamist käesoleva otsuse alusel, st edastamist ELi vastutavalt/volitatud töötlejalt Ühendkuningriigis asuvale vastutavale/volitatud töötlejale.
- (232) Täielikkuse huvides on siiski allpool kirjeldatud laialdase sideandmete kogumise korra tingimusi ja kaitsemeetmeid.

⁽³⁹²⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 152 ja 193.

⁽³⁹³⁾ 2016. aasta uurimisvolituste seaduse paragrahv 229.

⁽³⁹⁴⁾ Side pealtkuulamise tegevusjuhendi punkt 6.74, vt joonealune märkus nr 278, ja seadmete töösse sekkumise tegevusjuhendi punkt 6.78, vt joonealune märkus nr 348.

⁽³⁹⁵⁾ Uurimisvolituste voliniku büroo on loodud 2016. aasta uurimisvolituste seaduse paragrahvi 238 alusel, et tagada uurimisvolituste volinikule tema ülesannete täitmiseks vajalik personal, tööruumid, seadmed ning muud vahendid ja teenused (vt põhjendus 251).

⁽³⁹⁶⁾ Uurimisvolituste voliniku büroo 2018. aasta aruandes on märgitud, et valitsusside peakorteri analüütikute esitatud põhjendused „vastavad nõutavale standardile ja analüütikud arvestavad piisavalt üksikasjalikult laialdase andmekogumise päringute proportsionaalsust“. Uurimisvolituste voliniku 2018. aasta aruande punkt 6.22, vt joonealune märkus nr 464.

⁽³⁹⁷⁾ Uurimisvolituste voliniku 2019. aasta aruande punkt 7.6, vt joonealune märkus nr 463.

⁽³⁹⁸⁾ Uurimisvolituste voliniku 2019. aasta aruande punkt 10.22, vt joonealune märkus nr 463.

⁽³⁹⁹⁾ See tuleneb 2016. aasta uurimisvolituste seaduse paragrahvi 261 lõikes 5 esitatud sideandmete määratlusest, mille kohaselt säilitab või kogub sideandmeid telekommunikatsioonioperaator ja sideandmed on seotud kas mõne telekommunikatsiooniteenuse kasutajaga ja vastava teenuse osutamisega või sideandmed kuuluvad mõne sidevahendite kaudu edastatava sõnumi hulka, on sellele lisatud või sellega loogiliselt seotud (vt ka laialdase sideandmete kogumise tegevusjuhend, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Co_de_of_Practice.pdf, punktid 2.15–2.22). Lisaks on 2016. aasta uurimisvolituste seaduse paragrahvi 261 lõikes 10 esitatud telekommunikatsioonioperaatori määratluses sätestatud, et telekommunikatsioonioperaator on isik, kes pakub või osutab telekommunikatsiooniteenust Ühendkuningriigis asuvatele isikutele või kes kontrollib või pakub telekommunikatsioonisüsteemi, mis (täielikult või osaliselt) asub Ühendkuningriigis või mida kontrollitakse Ühendkuningriigist. Need määratlused näitavad selgelt, et uurimisvolituste seaduse kohaseid kohustusi ei saa panna telekommunikatsioonioperaatoritele, kelle seadmed ei asu Ühendkuningriigis või ei ole Ühendkuningriigist kontrollitavad ning kes ei paku ega osuta teenuseid Ühendkuningriigis asuvatele isikutele (vt ka laialdase sideandmete kogumise tegevusjuhendi punkt 2.2). Kui ELi abonendid (olenemata sellest, kas nad asuvad ELis või Ühendkuningriigis) kasutavad Ühendkuningriigis teenuseid, ei kantaks selle teenuse osutamisega seotud teavet ELi üle, vaid seda koguks Ühendkuningriigi teenuseosutaja otse.

- (233) 2016. aasta uurimisvolituste seadusega asendatakse õigusaktid, mis käsitlevad laialdast sideandmete hankimist ja mida käsitleti Euroopa Liidu Kohtu otsuses kohtuasjas Privacy International. Selles kohtuasjas vaidluse all olevad õigusnormid tunnistati kehtetuks ning uus kord näeb ette konkreetsed tingimused ja kaitsemeetmed, mille alusel võib sellist meetet lubada.
- (234) Erinevalt varasemast korrast, mille kohaselt oli ministril meetmele loa andmisel täielik kaalutusõigus, ⁽⁴⁰⁰⁾ on 2016. aasta uurimisvolituste seadusega nõutud, et minister annab määruse välja ainult juhul, kui meede on vajalik ja proportsionaalne. Praktikast tähendab see seda, et andmetele juurdepääsu ja taotletava eesmärgi vahel peaks olema seos ⁽⁴⁰¹⁾. Täpsemalt peab minister hindama seost taotletava meetme ja ühe või mitme määruuses märgitud operatiiveesmärgi (vt põhjendus 219) vahel seoses proportsionaalsuse hindamisega. Asjaomases tegevusjuhendis on öeldud: „Minister peab võtma arvesse, kas määrusega taotletavat eesmärki on võimalik saavutada muude, vähem sekkuvate vahenditega (seaduse paragrahvi 2 lõike 2 punkt a). Näiteks võib olla võimalik saada nõutavat teavet vähem sekkuva toiminguga, nagu sideandmete suunatud kogumise kaudu“ ⁽⁴⁰²⁾.
- (235) Sellise hinnangu andmisel tugineb minister andmetele, mida luurejuhid ⁽⁴⁰³⁾ peavad oma taotluses esitama, näiteks põhjused, miks meetet peetakse mõnel seadusest tuleneval alusel vajalikuks, ja põhjused, miks taotletavat eesmärki ei ole mõistlikult võimalik saavutada muude, vähem sekkuvate vahenditega ⁽⁴⁰⁴⁾. Lisaks piiravad operatiiveesmärgid määruse alusel saadud andmete valikut läbivaatamiseks ⁽⁴⁰⁵⁾. Nagu on täpsustatud asjaomases tegevusjuhendis, peavad operatiiveesmärgid kirjeldama selget nõuet ja sisaldama piisavalt üksikasju, et minister saaks veenduda, et saadud andmeid võib läbivaatamiseks valida ainult konkreetsetel põhjustel ⁽⁴⁰⁶⁾. Tegelikult peab minister enne määruse heakskiitmist tagama, et on kehtestatud erikord, millega tagatakse, et läbivaatamiseks valitakse välja üksnes see materjal, mida peetakse operatiiveesmärgil ja seadusjärgsel eesmärgil vajalikuks, ning et igas olukorras oleks täidetud proportsionaalsuse ja vajalikkuse kriteeriumid. See konkreetne nõue, mis kajastub 2016. aasta uurimisvolituste seaduse paragrahvides 158 ja 172 ⁽⁴⁰⁷⁾ ning käsitleb valikukriteeriumide vajalikkuse ja proportsionaalsuse eelnevat hindamist, on veel üks oluline uuendus 2016. aasta uurimisvolituste seadusega kehtestatud korras, võrreldes varem kehtinud korraga.
- (236) 2016. aasta uurimisvolituste seadusega kehtestati ka ministri kohustus tagada, et enne laialdast sideandmete kogumist käsitleva määruse väljaandmist on kehtestatud kogutud isikuandmete turvalisuse, säilitamise ja avalikustamise suhtes konkreetsed piirangud ⁽⁴⁰⁸⁾. Välisriigile avalikustamise korral kohaldatakse põhjenduses 227 seoses laialdase pealtkuulamise ja seadmete töösse sekkumisega kirjeldatud kaitsemeetmeid ka selles kontekstis ⁽⁴⁰⁹⁾. Õigusaktidega on kehtestatud täiendavad piirangud laialdase volituse määruste kestusele. ⁽⁴¹⁰⁾ pikendamisele ⁽⁴¹¹⁾ ja muutmisele ⁽⁴¹²⁾.
- (237) Nagu teiste laialdaste volituste puhul on siingi oluline, et minister peab enne määruse väljaandmist saama kohtuvoliniku heakskiidu ⁽⁴¹³⁾. See on 2016. aasta uurimisvolituste seadusega kehtestatud korra põhielement.

⁽⁴⁰⁰⁾ 1984. aasta telekommunikatsiooniseaduse paragrahvi 94 lõikes 1 on sätestatud, et minister võib anda „üldjuhiseid, mida minister peab vajalikuks või otstarbekaks riigi julgeoleku huvides [...]“ (vt joonealune märkus nr 451).

⁽⁴⁰¹⁾ Vt kohtuotsus Privacy International, punkt 78.

⁽⁴⁰²⁾ Vt laialdase sideandmete kogumise tegevusjuhendi punkt 4.11 (vt joonealune märkus nr 399).

⁽⁴⁰³⁾ Laialdase andmekogumise määrust võivad taotleda üksnes luureteenistuste juhid, kes on: i) turvateenistuse peadirektor; ii) salaluureteenistuse ülem või iii) valitsusside peakorterit direktor (vt 2016. aasta uurimisvolituste seaduse paragrahvid 158 ja 263).

⁽⁴⁰⁴⁾ Laialdase sideandmete kogumise tegevusjuhendi punkt 4.5 (vt joonealune märkus nr 399).

⁽⁴⁰⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvis 161 on sätestatud, et määruuses nimetatud operatiiveesmärgid peavad olema kindlaks määratud luureteenistuste juhtide hallatavas loetelus (operatiiveesmärkide loetelu) eesmärkidena, mida nad peavad operatiiveesmärkideks, mille puhul võib läbivaatamiseks valida laialdase andmekogumise määruse alusel saadud andmeid.

⁽⁴⁰⁶⁾ Laialdase sideandmete kogumise tegevusjuhendi punkt 6.6 (vt joonealune märkus nr 399).

⁽⁴⁰⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 172 kohaselt tuleb kehtestada konkreetsed kaitsemeetmed laialdaselt kogutud sideandmete läbivaatamisele eelneva filtreerimis- ja valikuetapi jaoks. Nende kaitsemeetmetega vastuolus olev tahtlik läbivaatamine on kuritegu (2016. aasta uurimisvolituste seaduse paragrahv 173).

⁽⁴⁰⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahv 171.

⁽⁴⁰⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 171 lõige 9.

⁽⁴¹⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahv 162.

⁽⁴¹¹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 163.

⁽⁴¹²⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 164–166.

⁽⁴¹³⁾ 2016. aasta uurimisvolituste seaduse paragrahv 159.

- (238) Laialdaselt kogutud materjali (sideandmete) läbivaatamismenetluse üle teeb järelkontrolli uurimisvolituste volinik (vt põhjendus 254). Sellega seoses kehtestati 2016. aasta uurimisvolituste seadusega nõue, et läbivaatamist tegev luureametnik peab enne läbivaatamiseks andmete valimist dokumenteerima põhjuse, miks kavandatud läbivaatamine on konkreetse operatiiveesmärgi jaoks vajalik ja proportsionaalne⁽⁴¹⁴⁾. Uurimisvolituste voliniku 2019. aasta aruandes leiti valitsusside peakorteri ja MI5 tava kohta, et „laialdaselt kogutud sideandmete kriitiline roll valitsusside peakorteri toimingutes oli inspekteeritud juhtumites hästi välja toodud. Kaalusime taotletud andmete laadi ja esitatud luurealaseid nõudeid ning leidsime, et dokumendid näitasid, et nende lähenemisviis oli vajalik ja proportsionaalne“⁽⁴¹⁵⁾. MI5 dokumenteeritud põhjendused olid heal tasemel ning vastasid vajalikkuse ja proportsionaalsuse põhimõtetele“⁽⁴¹⁶⁾.

3.3.1.1.4.3. Suurte isikuandmete kogumite säilitamine ja läbivaatamine

- (239) Suurte isikuandmete kogumite määrustega⁽⁴¹⁷⁾ antakse luureasutustele õigus säilitada ja läbi vaadata andmekogusid, mis sisaldavad mitme isiku isikuandmeid. Ühendkuningriigi ametiasutuste esitatud selgituste kohaselt võib selliste andmekogude analüüs olla „ainsaks viisiks, kuidas luureaparaat saab viia ellu uurimisi ja tuvastada terroriste väga piiratud luurevihjete alusel või kui nendevahelist teabevahetust on tahtlikult varjatud“⁽⁴¹⁸⁾. Suurte isikuandmete kogudega seotud määruseid on kaht liiki: kategooriapõhised määrused,⁽⁴¹⁹⁾ mis puudutavad teatavat andmekogude kategooriat, st andmeid, mis on sisult ja kavandatud kasutuselt sarnased ning mis eeldavad sarnaseid kaalutlusi, näiteks seoses sekkumismäära ja tundlikkuse tasemega ning andmete kasutamise proportsionaalsusega, võimaldades seega ministril kaaluda kõigi asjaomasesse klassi kuuluvate andmete kogumise vajalikkust ja proportsionaalsust korraga. Näiteks võib kategooriapõhine määrus hõlmata sarnaste marsruutidega seotud reisiandmekogumeid⁽⁴²⁰⁾; erimäärused⁽⁴²¹⁾ seevastu käsitlevad ühte konkreetset andmekogumit, näiteks mõnd uudset või ebatavalist liiki teavet sisaldavat andmekogumit, mis ei kuulu ühegi olemasoleva kategooriapõhise määruse alla, või andmekogumit, mis käsitleb teatavat liiki isikuandmeid⁽⁴²²⁾ ja vajab seetõttu täiendavaid kaitsemeetmeid⁽⁴²³⁾. 2016. aasta uurimisvolituste seaduse suurte isikuandmete kogumitega seotud sätted võimaldavad selliseid andmekogumeid läbi vaadata ja säilitada üksnes juhul, kui see on vajalik ja proportsionaalne⁽⁴²⁴⁾ ning kooskõlas eraelu puutumatusega seotud üldiste kohustustega⁽⁴²⁵⁾.
- (240) Suure isikuandmete kogumi määruse väljaandmise volituse suhtes kohaldatakse topeltkinnituse menetlust: meetme vajalikkust ja proportsionaalsust hindab kõigepealt minister ja seejärel kohtuvolinik⁽⁴²⁶⁾. Minister on kohustatud kaaluma taotletava määruse liigi laadi ja ulatust, asjaomaste andmete kategooriat ja konkreetsete suurte isikuandmete kogumite arvu, mis võivad kuuluda konkreetset liiki määruse alla⁽⁴²⁷⁾. Nagu on märgitud luureteenistuste tegevusjuhendis suurte isikuandmete kogumite säilitamiseks ja kasutamiseks, tuleb menetlus üksikasjalikult dokumenteerida ja selle suhtes kohaldatakse uurimisvolituste voliniku auditit⁽⁴²⁸⁾. Suurte isikuandmete kogumite säilitamine ja läbivaatamine 2016. aasta uurimisvolituste seaduses sätestatud piiranguid järgimata on kuritegu⁽⁴²⁹⁾.

⁽⁴¹⁴⁾ Uurimisvolituste voliniku 2019. aasta aruande punkt 8.6, vt joonealune märkus nr 463.

⁽⁴¹⁵⁾ Uurimisvolituste voliniku 2019. aasta aruande punkt 10.4, vt joonealune märkus nr 463.

⁽⁴¹⁶⁾ Uurimisvolituste voliniku 2019. aasta aruande punkt 8.37, vt joonealune märkus nr 463.

⁽⁴¹⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahv 200.

⁽⁴¹⁸⁾ „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu H: „National Security“ (Riiklik julgeolek), lk 34, vt joonealune märkus nr 29.

⁽⁴¹⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 204.

⁽⁴²⁰⁾ Luureteenistuste tegevusjuhend suurte isikuandmete kogumite säilitamiseks ja kasutamiseks, punkt 4.7, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf.

⁽⁴²¹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 205.

⁽⁴²²⁾ Näiteks tundlikud isikuandmed, vt 2016. aasta uurimisvolituste seaduse paragrahv 202 ning luureteenistuste tegevusjuhend suurte isikuandmete kogumite säilitamiseks ja kasutamiseks, punktid 4.21 ja 4.12, vt joonealune märkus nr 469.

⁽⁴²³⁾ Erimääruse taotlust peab minister kaaluma individuaalselt, st seoses ühe konkreetse andmekogumiga. Luureteenistus peab uurimisvolituste seaduse paragrahvi 205 kohaselt lisama konkreetse erimääruse taotlusele üksikasjaliku selgituse kõnealuse materjali laadi ja ulatuse kohta ning loetelu operatiiveesmärkidest, mille jaoks asjaomane luureteenistus soovib suurt isikuandmete kogumit läbi vaadata (kui luureteenistus taotleb nii säilitamist kui ka läbivaatamist ja mitte ainult säilitamist määrust). Kategooriapõhist määrust välja andes kaalub minister seevastu kogu andmekogumite kategooriat korraga.

⁽⁴²⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahv 204 ja 205.

⁽⁴²⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahv 2.

⁽⁴²⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 204 ja 205.

⁽⁴²⁷⁾ Luureteenistuste tegevusjuhend suurte isikuandmete kogumite säilitamiseks ja kasutamiseks, punkt 5.2, vt joonealune märkus nr 420.

⁽⁴²⁸⁾ Luureteenistuste tegevusjuhend suurte isikuandmete kogumite säilitamiseks ja kasutamiseks, punktid 8.1–8.15, vt joonealune märkus nr 420.

⁽⁴²⁹⁾ „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu H: „National Security“ (Riiklik julgeolek), lk 34, vt joonealune märkus nr 29.

3.3.2. Kogutud teabe edasine kasutamine

- (241) 2018. aasta andmekaitseseaduse 4. osa alusel töödeldavaid isikuandmeid ei tohi töödelda viisil, mis on vastuolus nende kogumise eesmärgiga ⁽⁴³⁰⁾. 2018. aasta andmekaitseasutuses on sätestatud, et vastutav töötaja võib töödelda andmeid muul eesmärgil kui see, milleks andmed koguti, kui see on kooskõlas algse eesmärgiga ja tingimusel, et vastutav töötaja on seadusega volitatud andmeid töötleva ning et töötlemine on vajalik ja proportsionaalne ⁽⁴³¹⁾. Lisaks on 1989. aasta julgeolekuteenistuse seaduses ja 1994. aasta luureteenistuste seaduses täpsustatud, et luureasutuste juhid on kohustatud tagama, et teavet ei koguta ega avaldata, välja arvatud niivõrd, kuivõrd see on vajalik asutuse ülesannete nõuetekohaseks täitmiseks või muudel asjaomastes sätetes loetletud piiratud ja konkreetsetel eesmärkidel ⁽⁴³²⁾.
- (242) Lisaks on 2018. aasta andmekaitseseaduse paragrahvis 109 sätestatud erinõuded isikuandmete rahvusvahelise edastamise kohta luureteenistuste poolt kolmandatele riikidele või rahvusvahelistele organisatsioonidele. Selle sätte kohaselt ei tohi isikuandmeid edastada väljaspool Ühendkuningriiki asuvale riigile või territooriumile või rahvusvahelisele organisatsioonile, välja arvatud juhul, kui edastamine on vajalik ja proportsionaalne vastutava töötaja seadusjärgsete ülesannete täitmiseks või muudel eesmärkidel, mis on sätestatud 1989. aasta julgeolekuteenistuse seaduse paragrahvi 2 lõike 2 punktis a või 1994. aasta luureteenistuste seaduse paragrahvi 2 lõike 2 punktis a ja paragrahvi 4 lõike 2 punktis a ⁽⁴³³⁾. Oluline on, et need nõuded kehtivad ka juhtudel, kui 2018. aasta andmekaitseseaduse paragrahvi 110 kohaselt tuginetakse riigi julgeoleku erandile, kuna 2018. aasta andmekaitseaduse paragrahvis 110 ei ole nimetatud 2018. aasta andmekaitseseaduse paragrahvi 109 nende sätete hulgas, mille kohaldamise võib peatada, kui riigi julgeoleku tagamiseks on vaja teha erandeid mõningatest sätetest.
- (243) Peale selle, nagu teabevolnik on rõhutanud oma suunistes isikuandmete töötlemise kohta luureteenistuste poolt, kui luureasutus jagab andmeid kolmanda riigi luureasutusega, kehtivad tema suhtes lisaks 2018. aasta andmekaitseaduse 4. osas sätestatud kaitsemeetmetele ka teistes tema suhtes kohaldatavates õigusaktides sätestatud kaitsemeetmed tagamaks, isikuandmeid saadakse, jagatakse ja töödeldakse õiguspäraselt ja vastutustundlikult ⁽⁴³⁴⁾. Näiteks on 2016. aasta uurimisvolituste seaduses sätestatud täiendavad kaitsemeetmed seoses sellise materjali edastamisega kolmandasse riiki, mis on kogutud suunatud pealtkuulamise, ⁽⁴³⁵⁾ seadmete töösse suunatud sekkumise, ⁽⁴³⁶⁾ laialdase pealtkuulamise, ⁽⁴³⁷⁾ laialdase sideandmete kogumise ⁽⁴³⁸⁾ ja seadmete töösse laialdase sekkumisega ⁽⁴³⁹⁾ („avalikustamine välisriigile“). Eelkõige peab määruse välja andnud asutus tagama, et on kehtestatud kord, millega tagatakse, et andmeid vastuvõttev kolmas riik piirab materjaliga tutvuvate isikute arvu, avalikustamise ulatuse ja mis tahes materjalist tehtud koopiaite arvu 2016. aasta uurimisvolituste seaduses sätestatud lubatud eesmärkide täitmiseks vajaliku miinimumiga ⁽⁴⁴⁰⁾.

3.3.3. Järelevalve

- (244) Kui valitsusel on riikliku julgeoleku eesmärgil juurdepääs isikuandmetele, teevad selle üle järelevalvet mitu eri asutust. Teabevolnik teeb järelevalvet isikuandmete töötlemise üle 2018. aasta andmekaitseaduse kontekstis (lisateavet voliniku sõltumatus, ametisse nimetamise, ülesannete ja volituste kohta vt põhjendused 85–98), samas kui sõltumatut ja õiguslikku järelevalvet 2016. aasta uurimisvolituste seaduse alusel uurimisvolituste kasutamise üle

⁽⁴³⁰⁾ 2018. aasta andmekaitseaduse paragrahvi 87 lõige 1.

⁽⁴³¹⁾ 2018. aasta andmekaitseaduse paragrahvi 87 lõige 3. Kuigi vastutavaid töötajaid võib 2018. aasta andmekaitseaduse paragrahvi 110 alusel sellest põhimõttest vabastada sel määral, mil see on vajalik riikliku julgeoleku tagamiseks, tuleb sellist erandit hinnata iga juhtumi puhul eraldi ja sellele saab tugineda üksnes juhul, kui konkreetse sätte kohaldamine avaldaks riigi julgeolekule negatiivset mõju (vt põhjendus 132). Ühendkuningriigi luureteenistuste riigi julgeoleku sertifikaadid (kättesaadavad aadressil <https://ico.org.uk/about-the-ico/our-information/national-security-certificates/>) ei hõlma 2018. aasta andmekaitseaduse 87. jaotise punkti 3. Kuna töötlemine muul eesmärgil peab olema seadusega lubatud, peab luureteenistustel olema edasiseks töötlemiseks selge õiguslik alus.

⁽⁴³²⁾ Nende eesmärkide kohta vt joonealune märkus 312.

⁽⁴³³⁾ Vt joonealune märkus nr 312.

⁽⁴³⁴⁾ Teabevolniku suunistes isikuandmete töötlemise kohta luureteenistuste poolt (vt joonealune märkus nr 161).

⁽⁴³⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahv 54.

⁽⁴³⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahv 130.

⁽⁴³⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahv 151.

⁽⁴³⁸⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 171 lõige 9.

⁽⁴³⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 192.

⁽⁴⁴⁰⁾ Kord peab sisaldama meetmeid tagamaks, et kõiki sellisest materjalist tehtud koopiaid hoitakse turvaliselt nii kaua, kuni materjali säilitatakse. Määruse alusel saadud materjal ja kõik sellisest materjalist tehtud koopiaid tuleb hävitada niipea, kui nende säilitamiseks ei ole enam asjakohast alust (vt 2016. aasta uurimisvolituste seaduse paragrahvi 150 lõiked 2 ja 5 ning paragrahvi 151 lõige 2). Tasub märkida, et Euroopa Inimõiguste Kohus leidis, et sarnased kaitsemeetmed, mis olid sätestatud varasemas õigusaktis (2000. aasta uurimisvolituste reguleerimise seadus), vastavad EIK poolt laialdase pealtkuulamise teel saadud materjali välisriikide või rahvusvaheliste organisatsioonidega jagamisele kehtestatud nõuetele (Euroopa Inimõiguste Kohus (suurkoda), Big Brother Watch ja teised vs. Ühendkuningriik (vt joonealune märkus 279), punktid 362 ja 399).

teeb uurimisvolituste volinik. Uurimisvolituste volinik jälgib 2016. aasta uurimisvolituste seaduse alusel uurimisvolituste kasutamist nii õiguskaitseasutuste kui ka riiklike julgeolekuasutuste poolt. Poliitilise järelevalve tagab parlamendi luureteenistuse komisjon.

3.3.3.1. Järelevalve andmekaitseseaduse 4. osa alusel

- (245) 2018. aasta andmekaitseseaduse 4. osa alusel luureteenistuste poolt teostatava isikuandmete töötlemise üle teeb järelevalvet teabevolinik ⁽⁴⁴¹⁾.
- (246) Teabevolniku üldised ülesanded seoses 2018. aasta andmekaitseseaduse 4. osa kohaldamisalasse kuuluvate isikuandmete töötlemisega luureteenistuste poolt on sätestatud 2018. aasta andmekaitseseaduse 13. lisas. Need ülesanded hõlmavad muu hulgas 2018. aasta andmekaitseseaduse 4. osa õigusnormide täitmise järelevalvet ja tagamist, üldsuse teadlikkuse suurendamist, parlamendi, valitsuse ja muude institutsioonide nõustamist seadusandlike ja haldusmeetmete küsimustes, vastutavate ja volitatud töötajate teadlikkuse suurendamist nende kohustustest, andmesubjekti teavitamist andmesubjekti õiguste kasutamisest, uurimiste läbiviimist jne.
- (247) Nagu ka 2018. aasta andmekaitseseaduse 3. osa puhul, on volinikul õigus teavitada vastutavaid töötajaid väidetavast rikkumisest, hoiatada, et töötlemine võib tõenäoliselt eeskirju rikkuda, ning teha noomitusi, kui rikkumine leiab kinnitust. Samuti võib ta välja anda täitmisteateid ja trahviteateid õigusakti teatavate sätete rikkumise eest ⁽⁴⁴²⁾. Erinevalt 2018. aasta andmekaitseseaduse muudest osadest ei saa volinik aga esitada hindamisteadet riiklikule julgeolekuasutusele ⁽⁴⁴³⁾.
- (248) Lisaks on 2018. aasta andmekaitseseaduse paragrahviga 110 ette nähtud erand voliniku teatavate volituste kasutamisest, kui see on vajalik riikliku julgeoleku tagamiseks. See puudutab voliniku õigust anda andmekaitseseaduse kohaselt välja (mis tahes liiki) teateid (teabenõudeid, hindamis-, täitmise- ja trahviteateid), volitusi teha kontrollle kooskõlas rahvusvaheliste kohustustega, sisenemis- ja kontrollivolitusi ning süütegusid käsitlevaid norme ⁽⁴⁴⁴⁾. Nagu on selgitatud põhjenduses 126, kohaldatakse neid erandeid ainult juhul, kui see on vajalik ja proportsionaalne, ning iga üksiku juhtu vaadatakse eraldi.
- (249) Teabevolinik ja Ühendkuningriigi luureteenistused on allkirjastanud vastastikuse mõistmise memorandum, ⁽⁴⁴⁵⁾ millega luuakse koostööraamistik mitmetes küsimustes, sealhulgas andmetega seotud rikkumistest teatamine ja andmesubjektide kaebuste käsitlemine. Eelkõige on selles sätestatud, et kaebuse saamisel hindab teabevolinik, kas riigi julgeoleku erandit on kohaldatud nõuetekohaselt. Kui teabevolinik teeb konkreetse kaebuse läbivaatamise käigus luureasutusele päringu, peab luureasutus sellele vastama 20 tööpäeva jooksul, kasutades asjakohaseid turvalisi kanaleid, kui päring puudutab salastatud teavet. Alates 2018. aasta aprillist on teabevolinik saanud üksikisikutelt 21 kaebust luureteenistuste kohta. Iga kaebust on hinnatud ja hindamise tulemusest on andmesubjekti teavitatud ⁽⁴⁴⁶⁾.

⁽⁴⁴¹⁾ 2018. aasta andmekaitseseaduse paragrahv 116.

⁽⁴⁴²⁾ 2018. aasta andmekaitseseaduse 13. lisa lõike 2 kohaselt võib vastutavale või volitatud töötajale esitada täitmise- ja trahviteate seoses 2018. aasta andmekaitseseaduse 4. osa 2. peatüki rikkumisega (töötlemise põhimõtted), 2018. aasta andmekaitseseaduse 4. osa sättega, millega antakse andmesubjektile õigusi, nõudega teavitada volinikku isikuandmetega seotud rikkumisest 2018. aasta andmekaitseseaduse paragrahvi 108 alusel ning isikuandmete kolmandatele riikidele, konventsiooniga mitteühinenud riikidele ja rahvusvahelistele organisatsioonidele edastamise põhimõtete, mis on esitatud 2018. aasta andmekaitseseaduse paragrahvis 109 (üksikisajalikumalt vt täitmisteate ja karistuse määramise teate kohta põhjendus 92).

⁽⁴⁴³⁾ 2018. aasta andmekaitseseaduse paragrahvi 147 lõike 6 kohaselt ei või teabevolinik esitada 2000. aasta teabevabaduse seaduse paragrahvi 23 lõikes 3 nimetatud organile hindamisteadet. Nende organite hulka kuuluvad julgeolekuteenistus (MI5), salaluureteenistus (MI6) ja valitsusside peakorter).

⁽⁴⁴⁴⁾ Erandi võib teha järgmistest sätetest: paragrahv 108 (volinikule isikuandmetega seotud rikkumisest teatamine), paragrahv 119 (kontroll kooskõlas rahvusvaheliste kohustustega), paragrahvid 142–154 ja 15. lisa (voliniku teated ning sisenemis- ja kontrolliõigused) ning paragrahvid 170–173 (isikuandmetega seotud süüteod). Lisaks seoses 13. lisa (voliniku muud üldfunktsioonid) lõike 1 punktides a ja g ning lõikes 2 kirjeldatud luureteenistustepoolse töötlemisega.

⁽⁴⁴⁵⁾ Teabevolniku ja Ühendkuningriigi luureasutuste vaheline vastastikuse mõistmise memorandum, vt joonealune märkus nr 165.

⁽⁴⁴⁶⁾ Seitsmel juhul soovitas teabevolinik kaebuse esitajal tõstatada küsimus vastutava töötaja juures (seda juhul, kui üksikisik on tõstatanud küsimuse teabevolniku juures, kuid oleks pidanud kõigepealt pöörduma vastutava töötaja poole), ühel juhul andis teabevolinik vastutavale töötajale üldist nõu (seda tehakse juhul, kui vastutava töötaja tegevus ei näi olevat õigusaktidega vastuolus, kuid tavade parandamisega saanuks vältida probleemi tõstatamist teabevolniku juures), ja ülejäänud 13 juhul ei oodatud vastutavalt töötajalt meetmete võtmist (seda juhul, kui isiku tõstatatud küsimus kuulub küll 2018. aasta andmekaitseseaduse kohaldamisalasse, sest on seotud isikuandmete töötlemisega, kuid esitatud teabe põhjal ei näi vastutav töötaja olevat seadust rikkunud).

3.3.3.2. Järelevalve 2016. aasta uurimisvolituste seaduse kohaste uurimisvolituste kasutamise üle

- (250) Vastavalt 2016. aasta uurimisvolituste seaduse 8. osale teeb järelevalvet uurimisvolituste kasutamise üle uurimisvolituste volinik. Uurimisvolituste volinikku abistavad teised kohtuvolinikud, keda koos nimetatakse kohtuvolinikeks⁽⁴⁴⁷⁾. 2016. aasta uurimisvolituste seaduses on sätestatud tagatised kohtuvolinike sõltumatuse kaitseks. Kohtuvolinikud peavad töötama või olema töötanud kohtus kõrgel ametikohal (st nad peavad olema või olema olnud kohtunikud kõrgeimates kohtutes)⁽⁴⁴⁸⁾ ning neil on valitsusest sõltumatu staatus nagu igal kohtusüsteemi liikmel⁽⁴⁴⁹⁾. 2016. aasta uurimisvolituste seaduse paragrahvi 227 kohaselt nimetab peaminister ametisse uurimisvolituste voliniku ja nii palju kohtuvolinikke, kui ta vajalikuks peab. Kõiki volinikke, olgu nad siis endised või praegused kohtunikud, saab ametisse nimetada üksnes kolme (Inglismaa & Walesi, Šotimaa ja Põhja-Iirimaa) ülemkohtuniku ning lordkantsleri (Lord Chancellor) ühise soovitusel alusel⁽⁴⁵⁰⁾. Minister peab tagama uurimisvolituste volinikule personali, tööruumid, seadmed ning muud vahendid ja teenused⁽⁴⁵¹⁾. Volinike ametiaeg on kolm aastat ja neid võib ametisse tagasi nimetada⁽⁴⁵²⁾. Kohtuvolinike sõltumatuse lisatagatiseks on asjaolu, et neid saab ametist tagandada üksnes juhul, kui täidetud on ranged tingimused, mis näevad ette kõrge künnise: kas peaminister 2016. aasta uurimisvolituste seaduse paragrahvi 228 lõikes 5 ammendavalt loetletud konkreetsetel asjaoludel (nagu pankrot või vangistus) või kui mõlemad parlamendikojad on vastu võtnud tagandamist heakskiitva otsuse⁽⁴⁵³⁾.
- (251) Uurimisvolituste volinikku ja kohtuvolinikke abistab nende ülesannete täitmisel uurimisvolituste voliniku büroo. Uurimisvolituste voliniku büroo töötajate hulka kuuluvad inspektorite meeskond, asutusesisesed õigus- ja tehnilised eksperdid ning tehnoloogia nõuandekogu, kes annab eksperdinõu. Nagu kohtuvolinike puhul, on ka uurimisvolituste voliniku büroo sõltumatus tagatud. Uurimisvolituste voliniku büroo on siseministeeriumi „autonoomne allüksus“, mida rahastab siseministeerium, kuid mis täidab oma ülesandeid sõltumatult⁽⁴⁵⁴⁾.
- (252) Kohtuvolinike peamised ülesanded on sätestatud 2016. aasta uurimisvolituste seaduse paragrahvis 229⁽⁴⁵⁵⁾. Eelkõige on kohtuvolinikel ulatuslikud eelneva heakskiitmise volitused, mis on osa Ühendkuningriigi õigusraamistikus 2016. aasta uurimisvolituste seadusega kehtestatud kaitsemeetmetest. Kohtuvolinikud peavad heaks kiitma kõik määrused, mis puudutavad suunatud pealtkuulamist, seadmete tööse sekkumist, suuri isikuandmete kogumeid, laialdast sideandmete kogumist ning sideandmete säilitamist⁽⁴⁵⁶⁾. Uurimisvolituste volinik peab alati eelnevalt heaks kiitma ka sideandmete kogumise õiguskaitse eesmärgil⁽⁴⁵⁷⁾. Kui mõni kohtuvolinik keeldub määrust heaks kiitmast, võib minister esitada kaebuse uurimisvolituste volinikule, kelle otsus on lõplik.
-
- ⁽⁴⁴⁷⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 227 lõigete 7 ja 8 kohaselt on uurimisvolituste volinik kohtuvolinik ning uurimisvolituste volinikku ja teisi kohtuvolinikke tuleb kollektiivselt nimetada kohtuvolinikeks. Praegu on kohtuvolinikke 15.
- ⁽⁴⁴⁸⁾ 2005. aasta põhiseaduse reformi seaduse (Constitutional Reform Act 2005) 3. osa paragrahvi 60 lõike 2 kohaselt on mõistetakse „kõrge kohtuametniku“ all kohtuniku ametikohta ühes järgmistest kohtutest: i) ülemkohus (Supreme Court); ii) Inglismaa ja Walesi apellatsioonikohus (Court of Appeal); iii) Inglismaa ja Walesi kõrgema astme kohus (High Court); iv) kõrge tsiviilkohus (Court of Session); v) Põhja-Iirimaa apellatsioonikohus; vi) Põhja-Iirimaa kõrgema astme kohus või ülemkoja apellatsioonilord (Lord of Appeal in Ordinary).
- ⁽⁴⁴⁹⁾ Kohtusüsteemi sõltumatus põhineb taval ja seda on laialdaselt tunnustatud alates 1701. aasta troonipärimisseadusest (Act of Settlement).
- ⁽⁴⁵⁰⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 227 lõige 3. Kohtuvolinikke peab soovitama ka uurimisvolituste volinik, 2016. aasta uurimisvolituste seaduse paragrahvi 227 lõike 4 punkt e.
- ⁽⁴⁵¹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 238.
- ⁽⁴⁵²⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 227 lõige 2.
- ⁽⁴⁵³⁾ Ametist vabastamise protsess on samasugune kui teiste Ühendkuningriigi kohtunike ametist vabastamise protsess (vt näiteks 1981. aasta kõrgemate kohtute seaduse (Senior Courts Act 1981) paragrahvi 11 lõige 3 ja 2005. aasta põhiseaduse reformi seaduse paragrahv 33, milles on samuti ette nähtud, et otsuse peavad heaks kiitma mõlemad parlamendikojad). Seni ei ole ühtegi kohtuvolinikku ametist tagandatud.
- ⁽⁴⁵⁴⁾ Autonoomne allüksus on organisatsioon või asutus, mida rahastab valitsus, kuid mis suudab tegutseda sõltumatult (määratlust ja lisateavet autonoomsete allüksuste kohta vt avalik-õiguslike asutuste liigitusest riigikantselei käsiraamatus „Handbook of the Cabinet Office“, mis on kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public-Bodies-Guidance-for-Departments.pdf, ja alamkoja avaliku halduse erikomisjoni 2014.–2015. aasta istungjärgu esimesest aruandest, mis on kättesaadav aadressil <https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf>).
- ⁽⁴⁵⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvi 229 järgi on kohtuvolinikul ulatuslikud järelevalvevolitused, mille hulka kuulub ka järelevalve luureasutuste kogutud andmete säilitamise ja avalikustamise üle.
- ⁽⁴⁵⁶⁾ Otsuse selle kohta, kas kiita heaks ministri otsus anda välja määrus, teevad kohtuvolinikud ise. Kui mõni kohtuvolinik keeldub määrust heaks kiitmast, võib minister esitada kaebuse uurimisvolituste volinikule, kelle otsus on lõplik.
- ⁽⁴⁵⁷⁾ Uurimisvolituste voliniku luba taotletakse alati, kui sideandmeid kogutakse õiguskaitse eesmärgil (2016. aasta uurimisvolituste seaduse paragrahv 60A). Kui sideandmeid kogutakse riikliku julgeoleku eesmärgil, võib loa anda uurimisvolituste volinik või teise võimalusena asjaomase ametiasutuse määratud vanemametnik (vt 2016. aasta uurimisvolituste seaduse paragrahvid 61 ja 61A ning põhjendus 203).

- (253) Eraelu puutumatuse õigusega tegelev ÜRO eriraportöör väljendas suurt heameelt kohtuvolinike institutsiooni loomise üle 2016. aasta uurimisvolituste seadusega, kuna „kõik tundlikumad või sekkuvad jälitustegevuse taotlused peavad heaks kiitma nii kabinetiminister kui ka uurimisvolituste voliniku büroo“. Eelkõige rõhutas ta: „See kohtuliku kontrolli element [uurimisvolituste voliniku ülesannete kaudu], mida toetab kogenud inspektoritest ja tehnoloogiaekspertidest koosnev meeskond, kellele on tagatud varasemast paremad võimalused, on üks kõige olulisemaid uurimisvolituste seadusega kehtestatud uusi kaitsemeetmeid“, mis asendab varasemat killustatud järelevalveasutuste süsteemi ning täiendab parlamendi luure- ja julgeolekukomisjoni ning uurimisvolituste kohtu rolli“⁽⁴⁵⁸⁾.
- (254) Lisaks on uurimisvolituste volinikul õigus teha järelkontrolli⁽⁴⁵⁹⁾, sealhulgas auditeid, kontrolle ja uurimisi, 2016. aasta uurimisvolituste seaduse alusel uurimisvolituste ning mõnede muude asjakohastes õigusaktides sätestatud volituste ja ülesannete täitmise üle⁽⁴⁶⁰⁾. Järelkontrolli tulemused sisalduvad aruandes, mille uurimisvolituste volinik peab igal aastal koostama ja peaministrile esitama⁽⁴⁶¹⁾ ning mis tuleb avaldada ja parlamendile esitada⁽⁴⁶²⁾. Aruanne sisaldab asjakohaseid statistilisi andmeid ja teavet uurimisvolituste kasutamise kohta luureasutuste ja õiguskaitseasutuste poolt, samuti kaitsemeetmete rakendamise kohta seoses kutsesaladuse alla kuuluva teabe, konfidentsiaalse ajakirjandusliku materjali ja ajakirjandusliku teabe allikatega, ning teavet rakendatud korra ja operatiivse märkide kohta, mida on kasutatud seoses laialdaste volituste määrustega. Samuti on uurimisvolituste voliniku aastaaruandes täpsustatud, millises valdkonnas on antud ametiasutustele soovitusi ja kuidas neid on arvesse võetud⁽⁴⁶³⁾.
- (255) 2016. aasta uurimisvolituste seaduse paragrahvi 231 kohaselt peab uurimisvolituste volinik juhul, kui ta saab teada olulisest veast, mille ametiasutused on teinud oma uurimisvolituste kasutamisel, teavitama asjaomast isikut, kui ta leiab, et viga on tõsine ja kui see on üldsuse huvides, et asjaomast isikut sellest teavitataks⁽⁴⁶⁴⁾. Eelkõige on 2016. aasta uurimisvolituste seaduse paragrahvis 231 sätestatud, et kui uurimisvolituste volinik teavitab isikut veast, peab ta isikule teatama, kas isikul on õigus pöörduda uurimisvolituste kohtusse, ning esitama teabe, mida volinik peab selle õiguse kasutamiseks vajalikuks ning mille avalikustamiseks on olemas avalik huvi⁽⁴⁶⁵⁾.

⁽⁴⁵⁸⁾ Eraelu puutumatuse õigusega tegeleva eriraportööri Suurbritannia ja Põhja-Iiri Ühendkuningriigi missiooni lõpu aruanne (vt joonealune märkus nr 281).

⁽⁴⁵⁹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 229. Kohtuvoliniku uurimisvolitused ja õigused teavet saada on sätestatud 2016. aasta uurimisvolituste seaduse paragrahvis 235.

⁽⁴⁶⁰⁾ Nende hulka kuuluvad 2000. aasta uurimisvolituste reguleerimise seaduse raames võetavad jälgimismeetmed, 1997. aasta politseiseaduse (Police Act 1997) 3. osas sätestatud ülesannete täitmine (omandiga seotud tegevuse lubamine) ja 1994. aasta luureteenistuste seaduse paragrahvides 5–7 sätestatud ülesannete täitmine ministri poolt (määrused raadiotelegraafi töö häirimiseks, valdustesse sisenemiseks ja nende elektrooniliseks jälgimiseks) (2016. aasta uurimisvolituste seaduse paragrahv 229).

⁽⁴⁶¹⁾ 2016. aasta uurimisvolituste seaduse paragrahv 230. Samuti võib uurimisvolituste volinik teha omal algatusel peaministrile ettekandeid kõigis küsimustes, mis on seotud tema ülesannetega. Uurimisvolituste volinik peab peaministri taotluse korral talle aru andma ning peaminister võib anda volinikule korralduse luureteenistuste ülesandeid läbi vaadata.

⁽⁴⁶²⁾ Mõned osad võib välja jätta, kui nende avaldamine oleks vastuolus riikliku julgeolekuga.

⁽⁴⁶³⁾ Näiteks on uurimisvolituste voliniku 2019. aasta aruandes (punkt 6.38) märgitud, et MI5-l soovitati muuta suurte isikuandmete kogumite säilitamise poliitikat, kuna oleks tulnud kaaluda lähenemist, mille puhul oleks kaalutud säilitatavate suurte isikuandmete kogumite kõikide väljade ja iga säilitatava suure isikuandmete kogumi proportsionaalsust. 2018. aasta lõpus ei olnud uurimisvolituste volinik veendunud, et seda soovitusi järgiti, ning 2019. aasta aruandes selgitati, et MI5 kehtestab nüüd selle nõude täitmiseks uue menetluse. 2019. aasta aruandes (punkt 8.22) on mainitud ka seda, et valitsusside peakorterile anti mitu soovitusi seoses dokumendiga, kus kirjeldatakse laialdaselt kogutud andmete kohta tehtud päringute proportsionaalsust. Aruandes on kinnitatud, et 2018. aasta lõpus on selles valdkonnas parandusi tehtud. Uurimisvolituste voliniku büroo 2019. aasta aruanne, kättesaadav aadressil https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Peale selle, iga kord, kui uurimisvolituste voliniku büroo kontrollib avaliku sektori asutust, koostatakse aruanne, mis esitatakse asutusele ja mis sisaldab kontrolli käigus saadud teabel põhinevaid soovitusi. Edaspidi alustab uurimisvolituste volinik iga järgmist kontrolli ülevaatega eelmisel korral tehtud soovitustest ja järgmises kontrolliaruandes märgitakse, kas eelmised soovitusid on täidetud või esitatakse need uuesti.

⁽⁴⁶⁴⁾ Viga loetakse tõsiseks, kui volinik leiab, et see on põhjustanud asjaomasele isikule olulist kahju (2016. aasta uurimisvolituste seaduse paragrahvi 231 lõige 2). 2018. aastal teatati 22 veast, millest kaheksat peeti tõsiseks ja millest tulenevalt anti asjaomasele isikule teavet. Vt uurimisvolituste voliniku büroo 2018. aasta aruande C lisa (vt <https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202018%20final.pdf>). 2019. aastal loeti 14 viga tõsiseks. Vt uurimisvolituste voliniku büroo 2019. aasta aruande C lisa, vt joonealune märkus nr 463.

⁽⁴⁶⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahvis 231 on sätestatud, et kui uurimisvolituste volinik teavitab isikut veast, peab ta esitama üksikasjad, mida volinik peab nende õiguste teostamiseks vajalikuks, võttes eelkõige arvesse seda, mil määral oleks üksikasjade avalikustamine vastuolus avaliku huviga või kahjustaks raskete kuritegude ennetamist või avastamist, Ühendkuningriigi majanduslikku heaolu või luureteenistuste ülesannete jätkuvat täitmist.

3.3.3.3. Parlamentaarne järelevalve luureteenistuste üle

- (256) Parlamentaarse järelevalvet teostab luure- ja julgeolekukomisjon, mille õiguslik alus on 2013. aasta kohtu- ja julgeolekuseadus (Justice and Security Act – JSA 2013) ⁽⁴⁶⁶⁾. Selle seadusega loodi Ühendkuningriigi parlamendi luure- ja julgeolekukomisjon. Alates 2013. aastast on luure- ja julgeolekukomisjonile antud suuremad volitused, sealhulgas turvateenistuste operatiivtegevuse järelevalve. 2013. aasta kohtu- ja julgeolekuseaduse paragrahvi 2 kohaselt on luure- ja julgeolekukomisjoni ülesanne teostada järelevalvet riiklike julgeolekuasutuste kulude, halduse, poliitika ja operatsioonide üle. 2013. aasta kohtu- ja julgeolekuseaduses on täpsustatud, et luure- ja julgeolekukomisjon võib viia läbi juurdlusi operatiivküsimustes, kui need ei ole seotud käimasolevate operatsioonidega ⁽⁴⁶⁷⁾. Peaministri ning luure- ja julgeolekukomisjoni vahel kokku lepitud vastastikuse mõistmise memorandumis ⁽⁴⁶⁸⁾ täpsustatakse üksikasjalikult elemendid, mida tuleb arvesse võtta, kui kaalutakse, kas tegevus on mõne käimasoleva operatsiooni osa ⁽⁴⁶⁹⁾. Samuti võib peaminister paluda luure- ja julgeolekukomisjonil uurida käimasolevaid operatsioone ja vaadata läbi asutuste vabatahtlikult esitatud teave.
- (257) 2013. aasta kohtu- ja julgeolekuseaduse 1. lisa kohaselt võib luure- ja julgeolekukomisjon paluda kõigi kolme luureteenistuse juhtidel mis tahes teavet avaldada. Agentuur peab sellise teabe kättesaadavaks tegema, välja arvatud juhul, kui minister sellele veto paneb ⁽⁴⁷⁰⁾. Ühendkuningriigi ametiasutuste esitatud selgituste kohaselt jääb luure- ja julgeolekukomisjonil tegelikult väga vähe teavet saamata ⁽⁴⁷¹⁾.
- (258) Luure- ja julgeolekukomisjon koosneb parlamendi mõlema koja liikmetest, kelle nimetab ametisse peaminister pärast opositsiooni juhiga konsulteerimist ⁽⁴⁷²⁾. Komisjon peab igal aastal esitama parlamendile aruande oma ülesannete täitmise kohta ja muud aruanded, mida ta peab asjakohaseks ⁽⁴⁷³⁾. Lisaks on komisjonil õigus saada iga kolme kuu järel loetelu operatiiveesmärkidest, millest lähtutakse laialdaselt kogutud materjali läbivaatamisel ⁽⁴⁷⁴⁾. Uurimisvolituste voliniku uurimiste, inspekteerimiste või auditite koopiaid jagab peaminister luure- ja julgeolekukomisjoniga, kui aruannete teema on komisjoni seadusliku pädevuse seisukohast oluline ⁽⁴⁷⁵⁾. Samuti võib luure- ja julgeolekukomisjon paluda uurimisvolituste volinikul viia läbi uurimine ja volinik peab komisjonile teatama, kas ta otsustab sellise uurimise läbi viia ⁽⁴⁷⁶⁾.
- (259) Luure- ja julgeolekukomisjon andis oma panuse ka 2016. aasta uurimisvolituste seaduse eelnõusse, mille tulemusena tehti mitu muudatust, mis nüüd seaduses kajastuvad ⁽⁴⁷⁷⁾. Eelkõige soovitas luure- ja julgeolekukomisjon eraelu puutumatuse kaitse tugevdamiseks kehtestada eraelu puutumatuse kaitse meetmed, mida kohaldatakse kõigi

⁽⁴⁶⁶⁾ Nagu selgitasid Ühendkuningriigi ametiasutused, laiendas kohtu- ja julgeolekuseadus luure- ja julgeolekukomisjoni volitusi, et lisada sinna luureparaadi järelevalve ülesanded, mis lähevad kolmest ametist kaugemale, ning võimaldada tagasiulatuvat järelevalvet ametite operatiivtegevuse üle olulise riikliku huviga seotud küsimustes.

⁽⁴⁶⁷⁾ 2013. aasta kohtu- ja julgeolekuseaduse paragrahv 2.

⁽⁴⁶⁸⁾ Peaministri ning luure- ja julgeolekukomisjoni vaheline vastastikuse mõistmise memorandum, kättesaadav aadressil <http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf>.

⁽⁴⁶⁹⁾ Peaministri ning luure- ja julgeolekukomisjoni vahelise vastastikuse mõistmise memorandum punkt 14, vt joonealune märkus nr 468.

⁽⁴⁷⁰⁾ Minister võib panna veto teabe avaldamisele üksnes kahel põhjusel: teave on tundlik ja seda ei tohiks luure- ja julgeolekukomisjonile avaldada riikliku julgeoleku huvides või on tegemist sellist laadi teabega, et kui ministrile esitatakse taotlus avaldada see alamkoja erikomisjonile, peaks minister (põhjustel, mis ei piirdu riikliku julgeolekuga) vajalikuks seda mitte teha (2013. aasta kohtu- ja julgeolekuseaduse 1. lisa lõike 4 punkt 2).

⁽⁴⁷¹⁾ „UK Explanatory Framework for Adequacy Discussions“ (Ühendkuningriigi kaitse piisavust käsitlevate arutelude selgitav raamistik), jagu H: „National Security“ (Riigi julgeolek), lk 43, vt joonealune märkus nr 31.

⁽⁴⁷²⁾ 2013. aasta kohtu- ja julgeolekuseaduse paragrahv 1. Ministrid ei saa olla komisjoni liikmed. Parlamendiliikmed on komisjonis ametis kogu parlamendi selle ametiaja jooksul, mil nad ametisse nimetati. Parlamendiliige võidakse ametist vabastada selle koja otsusega, millega ta ametisse nimetati, või juhul, kui ta ei ole enam parlamendiliige või saab ministriks. Samuti võib liige tagasi astuda.

⁽⁴⁷³⁾ Komisjoni aruanded ja avaldused on kättesaadavad järgmisel veebiaadressil: <https://isc.independent.gov.uk/publications/>. 2015. aastal avaldas luure- ja julgeolekukomisjon aruande „Privacy and Security: A modern and transparent legal framework“ (Eraelu puutumatuse ja julgeolek: tänapäevane ja läbipaistev õigusraamistik), vt: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf, milles analüüsiti luureasutuste kasutatavate jälgimistehnike õigusraamistikku ja esitati mitmesuguseid soovitusi, mida seejärel kaaluti ja mis integreeriti 2016. aasta uurimisvolituste seaduse eelnõusse. Valitsuse vastus eraelu puutumatust ja julgeolekut käsitlevale aruandele on kättesaadav aadressil https://b1cba9b3-a-5e6631fd-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

⁽⁴⁷⁴⁾ 2016. aasta uurimisvolituste seaduse paragrahvid 142, 161 ja 183.

⁽⁴⁷⁵⁾ 2016. aasta uurimisvolituste seaduse paragrahv 234.

⁽⁴⁷⁶⁾ 2016. aasta uurimisvolituste seaduse paragrahv 236.

⁽⁴⁷⁷⁾ Parlamendi luure- ja julgeolekukomisjoni aruanne uurimisvolituste seaduse eelnõu kohta, kättesaadav aadressil https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

uurimisvolituste ulatuses ⁽⁴⁷⁸⁾. Samuti soovitas ta muudatusi kavandatud pädevustes seoses seadmete tööse sekkumise, suurte isikuandmete kogumite ja sideandmetega ning taotles teatavate muude muudatuste tegemist, et tugevdada uurimisvolituste kasutamise piiranguid ja kaitsemeetmeid ⁽⁴⁷⁹⁾.

3.3.4. Õiguskaitse

- (260) Seoses valitsuse juurdepääsuga riikliku julgeoleku eesmärkidel peab andmesubjektil olema võimalus kasutada õiguskaitsevahendeid sõltumatus ja erapooletus kohtus, et tutvuda enda isikuandmetega või lasta neisse parandusi teha või neid kustutada ⁽⁴⁸⁰⁾. Sellisel kohtuorganil peab eelkõige olema õigus võtta vastu siduvaid otsuseid luureteenistuse kohta ⁽⁴⁸¹⁾. Ühendkuningriigis, nagu on selgitatud põhjendustes 261–271, on andmesubjektidel mitu võimalust selliseid õiguskaitsevahendeid taotleda ja saada.

3.3.4.1. Õiguskaitsemehhanismid andmekaitseaduse 4. osa alusel

- (261) 2018. aasta andmekaitseaduse paragrahvi 165 kohaselt on andmesubjektil õigus esitada teabevolinikule kaebus, kui andmesubjekt leiab, et seoses temaga seotud isikuandmetega on rikutud 2018. aasta andmekaitseaduse 4. osa. Teabevolinikul on õigus hinnata, kas vastutav ja volitatud töötleja täidavad 2018. aasta andmekaitseaduse nõudeid, ning nõuda neilt vajalike meetmete võtmist. 2018. aasta andmekaitseaduse 4. osa alusel on isikul ka õigus pöörduda kõrge kohtu poole (Šotimaal kõrge tsiviilkohus), et kehtestada vastutavale töötlejale korraldus austada andmetega tutvumise õigust, ⁽⁴⁸²⁾ töötlemise vaidlustamise õigust ⁽⁴⁸³⁾ ning õigust andmete parandamisele või kustutamisele ⁽⁴⁸⁴⁾.
- (262) Isikul on ka õigus nõuda vastutavalt töötlejalt või volitatud töötlejalt hüvitist 2018. aasta andmekaitseaduse 4. osa nõude rikkumise tõttu kantud kahju eest ⁽⁴⁸⁵⁾. Kahju hõlmab nii rahalist kahju kui ka kannatusi, millega ei kaasne rahalist kahju ⁽⁴⁸⁶⁾.

3.3.4.2. Õiguskaitsemehhanismid 2016. aasta uurimisvolituste seaduse alusel

- (263) Üksikisikud võivad saada 2016. aasta uurimisvolituste seaduse rikkumiste eest õiguskaitset uurimisvolituste kohtus (Investigatory Powers Tribunal).
- (264) Uurimisvolituste kohus on loodud 2000. aasta uurimisvolituste reguleerimise seadusega ja on täitevvõimust sõltumatu ⁽⁴⁸⁷⁾. Vastavalt 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 nimetab kuninganna nimetatud kohtu liikmed ametisse viieks aastaks. Tema Majesteet võib kohtu liikme ametist tagandada pärast mõlema parlamendikoja pöördumist ⁽⁴⁸⁸⁾ selles küsimuses ⁽⁴⁸⁹⁾.

⁽⁴⁷⁸⁾ Need eraelu puutumatusega seotud üldised kohustused on nüüd sätestatud 2016. aasta uurimisvolituste seaduse paragrahvi 2 lõikes 2, milles on sätestatud, et uurimisvolituste seaduse alusel tegutsev ametiasutus peab võtma arvesse seda, kas määrase, loa või teatega taotletavat eesmärki on mõistlikult võimalik saavutada muude, vähem sekkuvate vahenditega ning kas määrase, loa või teate alusel teabe saamise suhtes kohaldatava kaitse tase on kõrgem selle teabe erilise tundlikkuse, avaliku huvi tõttu telekommunikatsioonisüsteemide ja postiteenuste usaldusväärsuse ja turvalisuse vastu ning muude eraelu puutumatusega seotud aspektide tõttu.

⁽⁴⁷⁹⁾ Näiteks on luure- ja julgeolekukomisjoni taotlusel vähendatud päevade arvu, mille jooksul kiireloomuline määrus võib kehtida, enne kui kohtuvolinik selle heaks kiidab, viielt tööpäevalt kolmele ning luure- ja julgeolekukomisjonile anti õigus edastada küsimusi uurimiseks uurimisvolituste volinikule.

⁽⁴⁸⁰⁾ Kohtuotsus Schrems II, punkt 194.

⁽⁴⁸¹⁾ Kohtuotsus Schrems II, punkt 197.

⁽⁴⁸²⁾ 2018. aasta andmekaitseaduse paragrahvi 94 lõige 11.

⁽⁴⁸³⁾ 2018. aasta andmekaitseaduse paragrahvi 99 lõige 4.

⁽⁴⁸⁴⁾ 2018. aasta andmekaitseaduse paragrahvi 100 lõige 1.

⁽⁴⁸⁵⁾ 2018. aasta andmekaitseaduse paragrahv 169 lubab nõudeid esitada isikul, kes kannab kahju tulenevalt andmekaitsealastes õigusaktides sätestatud nõude rikkumisest. Ühendkuningriigi ametiasutuste esitatud teabe kohaselt esitatakse luureteenistuste vastu tegelikult nõudeid või kaebusi tõenäoliselt uurimisvolituste kohtule (*Investigatory Powers Tribunal*), kellel on lai pädevus, kes saab määrata hüvitise/kahjutasu ja kus nõude esitamine ei too kaasa kulusid.

⁽⁴⁸⁶⁾ 2018. aasta andmekaitseaduse paragrahvi 169 lõige 5.

⁽⁴⁸⁷⁾ 2000. aasta uurimisvolituste reguleerimise seaduse 3. lisa kohaselt peab liikmetel olema kohtus töötamise kogemus ja nad võidakse uuesti ametisse nimetada.

⁽⁴⁸⁸⁾ Pöördumine on parlamendile esitatav ettepanek, mille eesmärk on teavitada monarhi parlamendi arvamusest teatavas küsimuses.

⁽⁴⁸⁹⁾ 2000. aasta uurimisvolituste reguleerimise seaduse 3. lisa lõike 1 punkt 5.

- (265) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 kohaselt on uurimisvolituste kohus kohtuorgan, kuhu saavad kaevata isikud, keda on kahjustanud 2016. aasta uurimisvolituste seaduse või 2000. aasta uurimisvolituste reguleerimise seaduse kohane tegevus või luureasutuste mis tahes tegevus ⁽⁴⁹⁰⁾
- (266) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 alusel peab isik uurimisvolituste kohtusse hagi esitamiseks („kaebeõiguse eeldus“) uskuma, ⁽⁴⁹¹⁾ et luureteenistuse tegevus on seotud temaga, tema varaga, tema poolt või temale saadetud või talle mõeldud teabega või postiteenuse või telekommunikatsiooniteenuse või -süsteemi kasutamisega tema poolt ⁽⁴⁹²⁾. Lisaks peab hageja uskuma, et tegevus on toimunud vaidlustatavates oludes ⁽⁴⁹³⁾ või tegevuse on ellu viinud luureteenistused või see on toimunud nende nimel ⁽⁴⁹⁴⁾. Kuna „uskumise“ nõuet on tõlgendatud üsna laialt, ⁽⁴⁹⁵⁾ ei ole kaebeõiguse eeldused uurimisvolituste kohtusse hagi esitamiseks piiravad.
- (267) Esitatud kaebust arutades on uurimisvolituste kohtu ülesanne uurida, kas isikud, kelle vastu on kaebuses süüdistusi esitatud, on olnud seotud kaebuse esitajaga, ja uurida asutust, mis on väidetavalt rikkumises osalenud, ning seda, kas väidetav tegevus on aset leidnud ⁽⁴⁹⁶⁾. Kohus peab menetluses otsuse tegemisel kohaldama samu põhimõtteid, mida kasutatakse kohtuliku kontrolli taotluse korral ⁽⁴⁹⁷⁾. Lisaks on 2016. aasta uurimisvolituste seaduse kohaste määruste või teatiste adressaadid ja kõik teised isikud, kes töötavad riigiametis või politseijõududes või politseiuurimiste ja politsei tegevuse läbivaatamise voliniku teenistuses, kohustatud avaldama või esitama kohtule kõik dokumendid ja teabe, mida kohus võib oma pädevuse teostamiseks vajada ⁽⁴⁹⁸⁾.
- (268) Uurimisvolituste kohus peab teavitama kaebuse esitajat sellest, kas tema kasuks on tehtud otsus või mitte ⁽⁴⁹⁹⁾. Vastavalt 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67 lõigetele 6 ja 7 on kohtul õigus teha ajutisi korraldusi ja mõista välja selliseid kahjuhüvitisi või teha muid määrusi, mida ta peab sobivaks. Uurimisvolituste kohus võib anda korralduse määrus või luba tühistada ning korralduse hävitada dokumendid, mis

⁽⁴⁹⁰⁾ 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõige 5.

⁽⁴⁹¹⁾ „Uskumise“ kontrolli kohta vt kohtuasi Human Rights Watch vs. Secretary of State [2016] UKIPTrib15_165-CH, punkt 41. Selles asjas leidis uurimisvolituste kohus, viidates Euroopa Inimõiguste Kohtu praktikale, et sobiv kriteerium leidmaks, kas väidetaval usul, et luureteenistuste poolt või nimel on toime pandud tegevus, mis kuulub 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 68 lõike 5 kohaldamisalasse, on alust ja isik võib väita, et ta on langenud sellise rikkumise ohvriks, mille on põhjustanud ainult salajaste meetmete olemasolu või salajaste meetmete võtmist lubavate õigusaktide olemasolu, on see, kas isik saab tõendada, et tema isiklikust olukorrast tulenevalt on oht, et tema suhtes võidakse selliseid meetmeid võtta.

⁽⁴⁹²⁾ 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõike 4 punkt a.

⁽⁴⁹³⁾ Sellised olud tähendavad, et avaliku sektori asutus tegutseb loa (nt teabe hankimist lubava määru, loa/teate jms) alusel või et (olenemata sellise loa olemasolust) ei oleks tegevus olnud asjakohane ilma selle loata või vähemalt nõuetekohase kaalumiset, kas selline luba tuleks hankida. Kohtuvoliniku poolt lubatud toimingud loetakse toimunuks vaidlustatavatel asjaoludel (2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõige 7ZA), samal ajal kui muid kohtuniku loal toimunud toiminguid ei peeta toimunuks vaidlustatavatel asjaoludel (2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõiked 7 ja 8).

⁽⁴⁹⁴⁾ Ühendkuningriigi esitatud teabe kohaselt tähendab kaebuse tegemise madal lävi, et kohtu uurimise käigus selgub tihti, et avaliku sektori asutus ei uurinudki tegelikult kunagi kaebuse esitajat. Uurimisvolituste kohtu viimases statistilises aruandes on märgitud, et 2016. aastal sai kohus 209 kaebust, millest 52 % loeti põhjendamatuks või pahatahtlikuks ja 25 % lõppes tulemusega „kindlaks tegemata“. Ühendkuningriigi ametiasutused selgitasid, et see tähendab kas seda, et kaebuse esitaja suhtes ei rakendatud varjatud tegevust/volitusi, või seda, et kasutati varjatud meetodeid ja kohus leidis, et tegevus oli seaduslik. Lisaks oli 11 % hagidest sellised, mille puhul leiti, et need ei kuulu kohtu pädevusse või mis võeti tagasi või tunnistati kehtetuks ning 5 % esitati ettenähtud ajast hiljem; 7 % hagide puhul tegi kohust otsuse kaebuse esitaja kasuks. Uurimisvolituste kohtu 2016. aasta statistiline aruanne, kättesaadav aadressil <https://www.ipt-uk.com/docs/IPT%20Statistical%20Report%202016.pdf>.

⁽⁴⁹⁵⁾ Vt kohtuasi Human Rights Watch vs. Secretary of State [2016] UKIPTrib15_165-CH. Selles asjas leidis uurimisvolituste kohus Euroopa Inimõiguste Kohtu praktikale viidates, et asjakohane test seoses usuga, et 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 68 lõike 5 alla kuuluva tegevuse on ellu viinud luureteenistused või see on tehtud nende nimel, on see, kas sellisel usul on alust, sealhulgas asjaolu, et isik võib väita, et on ainuüksi salameetmete olemasolust või salameetmeid lubavatest õigusaktidest tuleneva rikkumise ohver, vaid siis, kui ta suudab tõestada, et tema isikliku olukorra tõttu on olemas oht, et selliseid meetmeid võidakse tema suhtes kohaldada (vt Human Rights Watch vs. Secretary of State, punkt 41).

⁽⁴⁹⁶⁾ 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67 lõige 3.

⁽⁴⁹⁷⁾ 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67 lõige 2.

⁽⁴⁹⁸⁾ 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 68 lõiked 6–7.

⁽⁴⁹⁹⁾ 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 68 lõige 4.

käsitlevad määruse, loa või teatisega antud volituste alusel saadud teavet või muul viisil ametiasutuse valduses isiku kohta olevat teavet ⁽⁵⁰⁰⁾. Vastavalt 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvile 67A võib kohtu otsuse edasi kaevata, kui uurimisvolituste kohus või asjaomane apellatsioonikohus on selleks loa andnud.

- (269) Lõpetuseks väärrib märkimist, et uurimisvolituste kohtu rolli on arutatud mitmel korral Euroopa Inimõiguste Kohtule esitatud hagide raames, eelkõige kohtuasjas *Kennedy vs. Ühendkuningriik* ⁽⁵⁰¹⁾ ja viimasel ajal kohtuasjas *Big Brother Watch jt vs. Ühendkuningriik*, ⁽⁵⁰²⁾ kus kohus sedastas, et „uurimisvolituste kohus kujutab endast tõhusat õiguskaitsevahendit isikutele, kes kahtlustavad, et luureasutused on nende sidet pealt kuulanud“ ⁽⁵⁰³⁾.

3.3.4.3. Muud olemasolevad õiguskaitsemehhanismid

- (270) Nagu on selgitatud põhjendustes 109–111, kohaldatakse riigi julgeoleku valdkonnas õiguskaitsevahendeid ka 1998. aasta inimõiguste seaduse alusel, samuti on võimalus pöörduda Euroopa Inimõiguste Kohtusse ⁽⁵⁰⁴⁾. 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõikega 2 on ette nähtud uurimisvolituste kohtu ainupädevus kõigi selliste inimõiguste seadusele tuginevate nõuete lahendamisel, mis on seotud luureasutustega ⁽⁵⁰⁵⁾. Nagu märkis kõrgema astme kohus, tähendab see, et „küsimuse, kas konkreetse juhtumi asjaoludega seoses on inimõiguste seadust rikutud, võib põhimõtteliselt tõstatada ja lahendada sõltumatu kohus, kellel on juurdepääs kõigile asjakohastele materjalidele, sealhulgas salajastele materjalidele. [...] Sellega seoses pöörame tähelepanu ka sellele, et kohtul endal on nüüd võimalus esitada apellatsioonkaebus asjakohasele apellatsioonikohtule (Inglismaal ja Walesis on selleks Court of Appeal) ning et ülemkohus otsustas hiljuti, et uurimisvolituste kohtu suhtes võib põhimõtteliselt kohaldada kohtulikku kontrolli: vt *R (Privacy International) vs. Investigatory Powers Tribunal*, [2019], UKSC 22; [2019] 2 WLR 1219“ ⁽⁵⁰⁶⁾.
- (271) Eeltoodust järeldub, et kui Ühendkuningriigi õiguskaitseasutused või riiklikud julgeolekuasutused pääsevad juurde käesoleva otsuse kohaldamisalasse kuuluvatele isikuandmetele, reguleeritakse sellist juurdepääsu õigusaktidega, millega kehtestatakse juurdepääsu tingimused ning tagatakse, et andmetele juurdepääs ja nende edasine kasutamine piirduks sellega, mis on vajalik ja proportsionaalne, pidades silmas taotletavat õiguskaitse või riigi julgeoleku eesmärki. Lisaks on selliseks juurdepääsuks enamikul juhtudel vaja kohtuorgani eelnevat luba määruse või andmeesitamismääruse heakskiitmise kujul ning igal juhul kohaldatakse sõltumatut järelevalvet. Kui ametiasutused on andmetele juurde pääsenud, kohaldatakse nende töötlemise, sealhulgas edasise jagamise ja edasisaatmise suhtes konkreetseid andmekaitsemeetmeid õiguskaitseasutustepoolse töötlemise puhul 2018. aasta andmekaitseseaduse 3. osa alusel, mis peegeldavad direktiiviga (EL) 2016/680 ette nähtud kaitsemeetmeid, ja luureasutustepoolse töötlemise puhul andmekaitseseaduse 4. osa alusel. Lisaks on andmesubjektide käsutuses selles valdkonnas tõhusad halduslikud ja kohtulikud õiguskaitsevahendid, sealhulgas õigus tutvuda oma andmetega või neid parandada või kustutada.
- (272) Võttes arvesse, kui olulised on sellised tingimused, piirangud ja kaitsemeetmed käesoleva otsuse seisukohast, jälgib komisjon tähelepanelikult Ühendkuningriigi nende õigusnormide kohaldamist ja tõlgendamist, mis reguleerivad valitsuse juurdepääsu andmetele. Selle hulka kuuluvad asjakohased seadusandlikud, regulatiivsed ja kohtupraktikaalased muudatused, samuti teabevoliniku ja teiste selle valdkonna järelevalveorganite tegevus. Tähelepanelikult

⁽⁵⁰⁰⁾ Üks näide nende volituste rakendamisest on kohtuasi *Liberty & Others vs. the Security Service, SIS, GCHQ*, [2015], UKIP Trib 13_77-H_2. Kohus tegi otsuse kahe kaebaja kasuks, sest ühel juhul säilitati nende andmeid kehtestatud piiridest kauem ja teisel juhul ei järgitud läbivaatamise menetlust, nagu on ette nähtud valitsusside peakorteri sise-eeskirjades. Esimesel juhul nõudis kohus, et luureteenistused hävitaksid teabe, mida säilitati asjaomastest tähtajast kauem. Teisel juhul hävitamiskorraldust ei antud, sest teavet ei säilitatud.

⁽⁵⁰¹⁾ Kohtuasja *Kennedy* kohta vt joonealune märkus 129.

⁽⁵⁰²⁾ Euroopa Inimõiguste Kohus, *Big Brother Watch* ja teised vs. Ühendkuningriik (vt joonealune märkus 268), punktid 413–415.

⁽⁵⁰³⁾ Euroopa Inimõiguste Kohus, *Big Brother Watch*, punkt 425.

⁽⁵⁰⁴⁾ Nagu on näha Euroopa Inimõiguste Kohtu suurkoja hiljutisest otsusest asjas *Big Brother Watch* ja teised vs. Ühendkuningriik (vt joonealune märkus 279), võimaldab see rahvusvahelise kohtu tulemuslikku kohtulikku kontrolli – mis on sarnane ELi liikmesriikide suhtes tehtavale kontrollile – selle üle, kas avaliku sektori asutused järgivad isikuandmete kasutamisel põhiõigusi. Peale selle teeb Euroopa Inimõiguste Kohtu otsuste täitmise üle erijärelevalvet Euroopa Nõukogu.

⁽⁵⁰⁵⁾ Kohtuotsuses *Belhaj* ja teised, [2017], UKSC 3, põhines kutsesaladuse alla kuuluva materjali pealtkuulamise õigusvastasuse tuvastamine otseselt Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni artiklil 8 (vt järeldus 11).

⁽⁵⁰⁶⁾ Kõrgema astme kohtu otsus kohtuasjas *Liberty*, [2019], EWHC 2057 (Admin), punkt 170.

jälgitakse, kuidas täidab Ühendkuningriik Euroopa Inimõiguste Kohtu asjakohaseid otsuseid, sealhulgas viib ellu EIK otsuste täitmise järelevalve raames ministrite komiteele esitatud tegevuskavades ja tegevusaruannetes esitatud meetmeid.

4. KOKKUVÕTE

- (273) Komisjon leiab, et Ühendkuningriigi isikuandmete kaitse üldmäärus ja 2018. aasta andmekaitseseadus tagavad Euroopa Liidust edastavate isikuandmete kaitse taseme, mis sisuliselt vastab määrusega (EL) 2016/679 tagatud kaitsetasemele.
- (274) Lisaks leiab komisjon, et Ühendkuningriigi õiguses ettenähtud järelevalvemehhanismid ja õiguskaitse võimalused võimaldavad rikkumised praktikas tuvastada ja nende eest karistusi määrata ning pakuvad andmesubjektile õiguskaitsevahendeid temaga seotud isikuandmetele juurdepääsu saamiseks ning vajaduse korral nende parandamiseks või kustutamiseks.
- (275) Lisaks leiab komisjon Ühendkuningriigi õigussüsteemi kohta kättesaadava teabe põhjal, et selliste üksikisikute põhiõiguste riivamine Ühendkuningriigi avaliku sektori asutuste poolt avaliku julgeoleku eesmärgil ning eriti õiguskaitse tagamise ja riikliku julgeoleku eesmärgil, kelle isikuandmeid edastatakse Euroopa Liidust Ühendkuningriiki, piirdub asjaomase seadusliku eesmärgi saavutamiseks rangelt vajalikuga ning tagatud on tõhus õiguskaitse selliste riivete vastu.
- (276) Seetõttu tuleks käesoleva otsuse järelduste valguses otsustada, et Ühendkuningriik tagab piisava kaitsetaseme määruse (EL) 2016/679 artikli 45 tähenduses, mida tõlgendatakse Euroopa Liidu põhiõiguste hartat silmas pidades.
- (277) See järeldus põhineb nii Ühendkuningriigi asjaomasel riigisisel korral kui ka rahvusvahelistel kohustustel, eelkõige Euroopa inimõiguste konventsiooni järgimisel ja Euroopa Inimõiguste Kohtu jurisdiktsioonile allumisel. Selliste õigusaktide jätkuv järgimine on seega käesoleva otsuse aluseks oleva hindamise eriti oluline element.

5. KÄESOLEVA OTSUSE MÕJU JA ANDMEKAITSEASUTUSTE TEGEVUS

- (278) Liikmesriigid ja nende organid peavad võtma liidu institutsioonide õigusaktide järgimiseks vajalikud meetmed, kuna eeldatakse nende õiguspärasust ja neil on seega õiguslikud tagajärjed seni, kuni neid ei ole tagasi võetud, tühistamishagi menetlemise tulemusena tühistatud ega eelotsusemenetluse tulemusel või õigusvastasuse väite alusel kehtetuks tunnistatud.
- (279) Seega on komisjoni poolt määruse (EL) 2016/679 artikli 45 lõike 3 alusel vastu võetud kaitse piisavuse otsus siduv kõikide otsuse adressaadiks olevate liikmesriikide organitele, sealhulgas sõltumatutele järelevalveasutustele. Eelkõige võib käesoleva otsuse kohaldamise ajal edastamine Euroopa Liidu vastutavalt või volitatud töötajalt Ühendkuningriigis asuvatele vastutavatele või volitatud töötajatele toimuda ilma täiendava loata.
- (280) Vastavalt määruse (EL) 2016/679 artikli 58 lõikele 5 ja nagu Euroopa Kohus on selgitanud Schremsi kohtuotsuses, ⁽⁵⁰⁷⁾ peab samas olema juhuks, kui riiklik andmekaitseasutus kahtleb, sealhulgas laekunud kaebuse põhjal, komisjoni kaitse piisavuse otsuse kooskõlas üksikisiku põhiõigustega eraelu puutumatusele ja andmekaitsele, liikmesriigi õigusega ette nähtud õiguskaitsevahend, mis võimaldab tal edastada need vastuväited siseriiklikule kohtule, kellelt võidakse nõuda asja kohta Euroopa Kohtule eelotsusetaotluse esitamist ⁽⁵⁰⁸⁾.

⁽⁵⁰⁷⁾ Kohtuotsus Schrems, punkt 65.

⁽⁵⁰⁸⁾ Kohtuotsus Schrems, punkt 65: „Sellega seoses on liikmesriigi seadusandja kohustatud ette nägema õiguskaitsevahendid, mis võimaldavad järelevalveasutusel esitada siseriiklikes kohtutes väiteid, mida ta peab põhjendatuks, selleks et kohtud juhul, kui neil on komisjoni otsuse kehtivuse suhtes samasugused kahtlused, esitaksid eelotsusetaotluse kõnealuse otsuse kehtivuse analüüsimiseks“.

6. KÄESOLEVA OTSUSE JÄRELEVALVE, PEATAMINE, TÜHISTAMINE VÕI MUUTMINE

- (281) Määruse (EL) 2016/679 artikli 45 lõike 4 kohaselt jälgib komisjon pidevalt asjakohaseid arengusuundi Ühendkuningriigis pärast käesoleva otsuse vastuvõtmist, et hinnata, kas see tagab endiselt sisuliselt vastava kaitsetaseme. Selline järelevalve on käesoleval juhul eriti oluline, kuna Ühendkuningriik hakkab haldama, kohaldama ja jõustama uut andmekaitsekorda, mille suhtes enam ei kohaldata Euroopa Liidu õigust ja mis võib muutuda. Sellega seoses pööratakse erilist tähelepanu Ühendkuningriigi nende normide kohaldamisele praktikas, mis reguleerivad isikuandmete edastamist kolmandatele riikidele, ja sellele, millist mõju see võib avaldada käesoleva otsuse alusel edastatud andmete kaitse tasemele; üksikisikute õiguste tulemuslikule teostamisele, sealhulgas kõigile asjakohastele arengusuundadele õiguses ja praktikas, mis võivad viia üksikisiku õigustest erandite tegemiseni või nende piiramiseni (eeskätt sisserände tulemusliku kontrolli säilitamise erandile); ning valitsuse juurdepääsuga seotud piirangute ja kaitsemeetmete järgimisele. Muude elementide hulgas võtab komisjon jälgimisel arvesse arenguid kohtupraktikas ning teabevoliniku ja teiste sõltumatute organite tehtavat järelevalvet.
- (282) Järelevalve hõlbustamiseks palutakse Ühendkuningriigi ametiasutustel teavitada komisjoni kiiresti Ühendkuningriigi õiguskorra igast olulisest muudatusest, mis mõjutab käesolevas otsuses käsitletavat õigusraamistikku, samuti käesolevas otsuses hinnatud isikuandmete töötlemisega seotud tavade muutumisest, seda seoses nii isikuandmete töötlemisega vastutavate ja volitatud töötlejate poolt kui ka piirangute ja kaitsemeetmetega, mida kohaldatakse avaliku sektori asutuste juurdepääsu suhtes isikuandmetele. Eeltoodu hulka peaksid kuuluma ka arengusuunad põhjenduses 281 nimetatud küsimustes.
- (283) Selleks et komisjonil oleks võimalik tõhusalt täita oma järelevalvefunktsiooni, peaksid liikmesriigid teavitama komisjoni kõikidest asjakohastest meetmetest, mida riiklikud andmekaitseasutused võtavad, eelkõige seoses ELi andmesubjektide päringute või kaebustega, mis puudutavad isikuandmete edastamist liidust Ühendkuningriigis asuvatele vastutavatele või volitatud töötlejatele. Komisjoni tuleks teavitada ka võimalikest märkidest, et kuritegude ennetamise, uurimise, avastamise või nende eest süüdimõistmise või riigi julgeoleku eest vastutavate Ühendkuningriigi avaliku sektori asutuste tegevus, samuti järelevalveasutuste tegevus ei taga nõutavat kaitsetaset.
- (284) Kui kättesaadavast teabest, eriti käesoleva otsuse järelevalvest tulenevast või Ühendkuningriigi või liikmesriikide ametiasutuste esitatud teabest ilmneb, et Ühendkuningriigi pakutav kaitsetase ei pruugi enam olla piisav, peaks komisjon kohe teavitama sellest Ühendkuningriigi pädevaid asutusi ning nõudma, et asjakohaseid meetmeid võetaks kindlaksmääratud tähtaja jooksul, mis ei või olla pikem kui kolm kuud. Vajaduse korral võib seda tähtaega pikendada kindlaksmääratud tähtaja võrra, võttes arvesse tõstatatud küsimuse ja/või võetavate meetmete laadi. Näiteks käivitataks selline menetlus juhul, kui andmete edasisaatmisel, kaasa arvatud ministri vastuvõetud uute kaitse piisavuse määruste või Ühendkuningriigi sõlmitud rahvusvaheliste lepingute alusel, ei järgitaks enam kaitsemeetmeid, millega tagatakse kaitse jätkuvus määruse (EL) 2016/679 artikli 44 tähenduses.
- (285) Kui Ühendkuningriigi pädevad asutused ei ole kindlaksmääratud ajavahemiku möödumisel neid meetmeid võtnud või muul viisil rahuldavalt tõendanud, et käesolev otsus põhineb endiselt piisaval kaitsetasemel, algatab komisjon määruse (EL) 2016/679 artikli 93 lõikes 2 osutatud menetluse käesoleva otsuse osaliseks või täielikuks peatamiseks või kehtetuks tunnistamiseks.
- (286) Teise võimalusena algatab komisjon menetluse käesoleva otsuse muutmiseks, et eelkõige kehtestada andmete edastamise lisatingimused või piirata kaitse piisavuse otsuse kohaldamisala selliselt, et selle alla kuuluks üksnes andmeedastus, mille puhul on tagatud kaitse jätkumine.
- (287) Nõuetekohaselt põhjendatud, tungivalt vajalikul ja kiireloomulisel juhul kasutab komisjon võimalust võtta kooskõlas määruse (EL) 2016/679 artikli 93 lõikes 3 osutatud menetlusega vastu viivitamata kohaldatavad rakendusaktid, millega otsus peatatakse või tunnistatakse kehtetuks või seda muudetakse.

7. OTSUSE KEHTIVUSAEG JA PIKENDAMINE

- (288) Komisjon peab võtma arvesse, et väljaastumislepingus ette nähtud üleminekuperioodi ning ELi ja Ühendkuningriigi kaubandus- ja koostöölepingu artikli 782 kohase ajutise sätte kohaldamise lõppemisel haldab ja kohaldab Ühendkuningriik sellist uut andmekaitsekorda ja tagab selle täitmise, mis erineb korrast, mis kehtis, kui Ühendkuningriigile oli siduv ELi õigus. On oluline silmas pidada, et see võib hõlmata käesolevas otsuses hinnatud andmekaitse- raamistiku muutmist ning muid olulisi muutusi.

- (289) Seepärast on asjakohane sätestada, et käesolevat otsust kohaldatakse nelja aasta jooksul alates selle jõustumisest.
- (290) Kui eelkõige käesoleva otsuse järelevalvest tulenev teave näitab, et Ühendkuningriigis tagatud kaitse taseme piisavusega seotud tähelepanekud on endiselt faktiliselt ja õiguslikult põhjendatud, peaks komisjon hiljemalt kuus kuud enne käesoleva otsuse kohaldamise lõppu algatama käesoleva otsuse muutmise menetluse, et pikendada selle kohaldamisega põhimõtteliselt veel nelja aasta võrra. Selline käesolevat otsust muutev rakendusakt tuleb vastu võtta määruse (EL) 2016/679 artikli 93 lõikes 2 osutatud korras.

8. LÕPPMÄRKUSED

- (291) Euroopa Andmekaitsekoostöögrupi avaldas arvamuse, ⁽⁵⁰⁹⁾ mida on käesoleva otsuse koostamisel arvesse võetud.
- (292) Käesoleva otsusega ettenähtud meetmed on kooskõlas määruse (EL) 2016/679 artikli 93 kohaselt loodud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

1. Määruse (EL) 2016/679 artikli 45 tähenduses tagab Ühendkuningriik määruse (EL) 2016/679 kohaldamisalas Euroopa Liidust Ühendkuningriiki edastatavate isikuandmete kaitse piisava taseme.
2. See otsus ei puuduta isikuandmeid, mida edastatakse Ühendkuningriigi sisserände kontrolliga seotud eesmärkidel või mis kuuluvad muul moel Ühendkuningriigi 2018. aasta andmekaitseseaduse 2. lisa lõike 4 punktiga 1 ette nähtud normi kohaldamisalasse, millega tehakse erand mõnedest andmesubjekti õigustest sisserände tulemusliku kontrolli säilitamiseks.

Artikkel 2

Kui liikmesriikide pädevad järelevalveasutused kasutavad isikute kaitsmiseks seoses nende isikuandmete töötlemisega määruse (EL) 2016/679 artikli 58 kohaseid volitusi artiklis 1 sätestatud kohaldamisalas toimuva andmeedastuse suhtes, teavitab asjaomane liikmesriik komisjoni viivitamata.

Artikkel 3

1. Komisjon jälgib pidevalt käesoleva otsuse aluseks oleva õigusraamistiku kohaldamist, sealhulgas tingimusi, mida kohaldatakse andmete edasisaatmisele, üksikisikute õiguste teostamisele ja Ühendkuningriigi avaliku sektori asutuste juurdepääsule käesoleva otsuse alusel edastatud andmetele, et hinnata, kas Ühendkuningriik tagab jätkuvalt piisava kaitsetaseme artikli 1 tähenduses.
2. Liikmesriigid ja komisjon teavitavad üksteist juhtudest, mil teabevolirik või muu Ühendkuningriigi pädev institutsioon ei ole suutnud tagada vastavust käesoleva otsuse aluseks olevale õigusraamistikule.
3. Liikmesriigid ja komisjon teavitavad üksteist kõikidest märkidest, mis osutavad sellele, et Ühendkuningriigi ametiasutuste sekkumine üksikisikute isikuandmete kaitse õigusesse ületab rangelt vajalikku või et sellise sekkumise vastu puudub tõhus õiguskaitse.
4. Kui komisjonil on põhjust arvata, et piisav kaitsetase ei ole enam tagatud, teavitab komisjon Ühendkuningriigi pädevaid asutusi ning võib käesoleva otsuse kohaldamise peatada, otsuse kehtetuks tunnistada või seda muuta.

⁽⁵⁰⁹⁾ Arvamus 14/2021 Euroopa Komisjoni määruse (EL) 2016/679 kohase rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset Ühendkuningriigis, kättesaadav aadressil: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

5. Komisjon võib otsuse kohaldamise peatada, otsuse kehtetuks tunnistada või seda muuta ka juhul, kui Ühendkuningriigi valitsuse koostöö puudumine takistab komisjoni tegemast kindlaks, kas artikli 1 lõikes 1 tehtud järelduse paikapidavus on kahtluse all.

Artikkel 4

Käesolev otsus kehtib kuni 27. juunini 2025, kui selle kehtivust ei pikendata määruse (EL) 2016/679 artikli 93 lõikes 2 osutatud korras.

Artikkel 5

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 28. juuni 2021

Komisjoni nimel
komisjoni liige
Didier REYNERS
