KOMISJONI RAKENDUSOTSUS (EL) 2021/1773,

28. juuni 2021,

mis põhineb Euroopa Parlamendi ja nõukogu direktiivil (EL) 2016/680 ning käsitleb isikuandmete piisavat kaitset Ühendkuningriigis

(teatavaks tehtud numbri C(2021) 4801 all)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, ([1]) eelkõige selle artikli 36 lõiget 3,

ning arvestades järgmist:

1. SISSEJUHATUS

(1) Direktiiviga (EL) 2016/680 on kehtestatud eeskirjad isikuandmete edastamiseks liidus asuvatelt pädevatelt asutustelt kolmandatesse riikidesse ja rahvusvahelistele organisatsioonidele määral, mil see edastamine kuulub direktiivi kohaldamisalasse. Pädevate asutuste poolt isikuandmete rahvusvahelise edastamise eeskirjad on sätestatud direktiivi (EL) 2016/680 V peatükis, täpsemalt artiklites 35–40. Kuigi isikuandmete liikumine Euroopa Liidust väljaspool asuvatesse riikidesse ja neist riikidest Euroopa Liitu on vajalik tõhusa õiguskaitsekoostöö huvides, tuleb tagada, et sellise edastamisega ei alandata Euroopa Liidus isikuandmete kaitse taset ([2]).

(2) Direktiivi (EL) 2016/680 artikli 36 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. Sel tingimusel võib kolmandale riigile isikuandmeid edastada lisaloata (välja arvatud juhul, kui edastamiseks peab andma loa teine liikmesriik, kust andmed saadi), nagu on ette nähtud direktiivi (EL) 2016/680 artikli 35 lõikes 1 ja põhjenduses 66.

(3) Nagu on märgitud direktiivi (EL) 2016/680 artikli 36 lõikes 2, tuleb kaitse piisavuse otsuse vastuvõtmisel tugineda kolmanda riigi õiguskorra põhjalikule analüüsile. Komisjon peab hindamisel kindlaks määrama, kas kõnealune kolmas riik tagab kaitsetaseme, mis sisuliselt vastab Euroopa Liidus tagatud kaitsetasemele (direktiivi (EL) 2016/680 põhjendus 67). Sisulise vastavuse hindamise standard on sätestatud ELi õiguses, eelkõige direktiivis (EL) 2016/680 ja Euroopa Liidu Kohtu praktikas ([3]). Tähtis on ka Euroopa Andmekaitsenõukogu piisavuse võrdlusalus ([4]).

(4) Nagu Euroopa Liidu Kohus on selgitanud, ei eelda see identset kaitsetaset ([5]). Eelkõige võivad vahendid, mida asjaomane kolmas riik isikuandmete kaitsmiseks kasutab, erineda nendest, mida Euroopa Liidus rakendatakse, kuivõrd need osutuvad praktikas kaitse piisava taseme tagamisel tulemuslikuks ([6]). Kaitse piisavuse nõue ei eelda seega, et liidu õigusnorme tuleb punkt punktilt kopeerida. Küsimus on pigem selles, kas ELi-väline süsteem tervikuna tagab eraelu puutumatuse õiguse sisu, selle tõhusa rakendamise, järelevalve ja kohtuliku kaitse kaudu nõutava isikuandmete kaitse taseme ([7]).

([1]) ELT L 119, 4.5.2016, lk 89.

([2]) Vt direktiivi (EL) 2016/680 põhjendus 64.

([3]) Vt viimati otsus kohtuasjas C-311/18, Maximilian Schrems *vs.* Data Protection Commissioner (edaspidi „Schrems II“), ECLI:EU:C:2020:559.

([4]) Vt 2021. aasta veebruaris vastu võetud soovitused 01/2021 õiguskaitsedirektiivi kohase piisavuse võrdlusaluse kohta, kättesaadav aadressil https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_et

([5]) Kohtuasi C-362/14, Maximilian Schrems *vs.* Data Protection Commissioner (edaspidi „Schrems“), ECLI:EU:C:2015:650, punkt 73.

([6]) Schrems, punkt 74.

([7]) 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.

(5) Komisjon on hoolikalt analüüsinud Ühendkuningriigi asjaomaseid õigusnorme ja tavasid. Komisjon teeb allpool esitatud tähelepanekutele tuginedes järelduse, et Ühendkuningriik tagab direktiivi (EL) 2016/680 kohaldamisalasse kuuluvatelt liidus asuvatelt pädevatelt asutustelt 2018. aasta andmekaitseseaduse (Data Protection Act 2018) ([8]) 3. osa kohaldamisalasse kuuluvatele Ühendkuningriigi pädevatele asutustele edastatavate isikuandmete kaitse piisava taseme.

(6) Ilma et käesolev otsus piiraks direktiivi (EL) 2016/680 artiklis 35 sätestatud tingimuste kohaldamist, ei pea otsusest tulenevalt selliseks edastamiseks hankima lisaluba nelja-aastase ajavahemiku jooksul, mida võidakse pikendada.

2. EESKIRJAD, MIDA KOHALDATAKSE ISIKUANDMETE TÖÖTLEMISEL PÄDEVATE ASUTUSTE POOLT KRIMINAALÕIGUSKAITSE EESMÄRKIDEL

2.1. Põhiseaduslik raamistik

(7) Ühendkuningriik on parlamentaarne demokraatia. Sellel on kõigi muude valitsusasutuste suhtes ülimuslik suveräänne parlament, täidesaatvat võimu teostav valitsus, mille liikmed valitakse parlamendi liikmete hulgast ja mis annab aru parlamendile, ning sõltumatu kohtuvõim. Valitsuse volitused olenevad selle suutlikkusest võita valitud alamkoja usaldus. Valitsus annab aru mõlemale parlamendikojale (alamkoda ja ülemkoda ehk lordide koda), mis teostavad järelevalvet valitsuse üle ning arutavad ja võtavad vastu seadusi. Ühendkuningriigi parlament on delegeerinud Šotimaa parlamendile, Walesi parlamendile (*Senedd Cymru*) ja Põhja-Iirimaa assambleele vastutuse õigusloome eest teatavates Šotimaa, Walesi ja Põhja-Iirimaa siseküsimustes. Andmekaitse kuulub Ühendkuningriigi parlamendi pädevusse, st sama õigust kohaldatakse kogu riigis, kuid otsustusõigus käesoleva otsusega seotud muude poliitikavaldkondade üle on delegeeritud. Näiteks vastutus kriminaalõigussüsteemide, sealhulgas Šotimaa ja Põhja-Iirimaa politsei tegevuse eest on üle antud vastavalt Šotimaa parlamendile ja Põhja-Iirimaa assambleele ([9]).

(8) Kuigi Ühendkuningriigil ei ole kodifitseeritud põhiseadust konkreetse konstitutiivse dokumendi tähenduses, on riigi põhiseaduslikud põhimõtted välja kujunenud aja jooksul ning põhinevad kohtupraktikal ja eelkõige tavadel. Tunnistatakse teatavate statuutide, näiteks Magna Carta, 1689. aasta õiguste deklaratsiooni (Bill of Rights 1689) ja 1998. aasta inimõiguste seaduse (Human Rights Act 1998) põhiseaduslikku väärtust. Põhiseadusliku korra osana on üksikisiku põhiõigusi laiendatud üldise õiguse, statuutide ja rahvusvaheliste lepingutega, eelkõige Euroopa inimõiguste konventsiooniga, mille Ühendkuningriik ratifitseeris 1951. aastal. Ühendkuningriik ratifitseeris 1987. aastal ka Euroopa Nõukogu isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (konventsioon 108) ([10]).

(9) 1998. aasta inimõiguste seadusega lisati Euroopa inimõiguste konventsioonis sisalduvad õigused Ühendkuningriigi õigusesse. Seadusega antakse igale isikule põhiõigused ja -vabadused, mis on ette nähtud Euroopa inimõiguste konventsiooni artiklites 2–12 ja artiklis 14, konventsiooni protokolli nr 1 artiklites 1–3 ning protokolli nr 13 artiklis 1 koostoimes Euroopa inimõiguste konventsiooni artiklitega 16–18. See hõlmab õigust era- ja perekonnaelu austamisele – mis omakorda hõlmab õigust isikuandmete kaitsele – ning õigust õiglasele kohtumenetlusele ([11]). Nimelt ei sekku ametivõimud Euroopa inimõiguste konventsiooni artikli 8 kohaselt eraelu puutumatuse õiguse kasutamisse muidu, kui kooskõlas seadusega ja 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.

([8]) 2018. aasta andmekaitseseadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Ühendkuningriigi kaitse piisavuse arutelude selgitava raamistiku (Explanatory Framework for Adequacy Discussion) osa F: õiguskaitse, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Esmalt rakendati konventsiooni 108 põhimõtted Ühendkuningriigi õigusesse 1984. aasta andmekaitseseadusega, mis asendati 1998. aasta ja seejärel 2018. aasta andmekaitseseadusega (koostoimes Ühendkuningriigi isikuandmete kaitse üldmäärusega). Ühendkuningriik allkirjastas 2018. aastal ka protokolli, millega muudetakse isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni, (konventsioon 108+) ja tegeleb praegu konventsiooni ratifitseerimisega.

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

(10) Vastavalt 1998. aasta inimõiguste seadusele peab avaliku sektori asutuste tegevus olema alati kooskõlas Euroopa inimõiguste konventsiooniga tagatud õigustega ([12]). Lisaks tuleb esmaseid ja teiseseid õigusakte tõlgendada ja rakendada viisil, mis on nende õigustega kooskõlas ([13]). Kui üksikisik leiab, et avaliku sektori asutused on rikkunud tema õigusi, sealhulgas eraelu puutumatuse õigus ja andmekaitse õigus, võib ta õiguskaitse saamiseks pöörduda 1998. aasta inimõiguste seaduse alusel Ühendkuningriigi kohtute poole ja kui riiklikud õiguskaitsevahendid on ammendatud, taotleda Euroopa inimõiguste konventsiooniga tagatud õiguste rikkumise korral õiguskaitset Euroopa Inimõiguste Kohtus.

2.2. **Ühendkuningriigi andmekaitseraamistik**

(11) Ühendkuningriik astus 31. jaanuaril 2020 liidust välja. Suurbritannia ja Põhja-Iiri Ühendkuningriigi Euroopa Liidust ja Euroopa Aatomienergiaühendusest väljaastumise lepingu ([14]) alusel jätkati Ühendkuningriigis liidu õiguse kohaldamist üleminekuperioodil kuni 31. detsembrini 2020. Enne väljaastumist ja üleminekuperioodi kestel koosnes Ühendkuningriigis isikuandmete kaitse õigusraamistik, millega reguleeritakse pädevates asutustes isikuandmete töötlemist süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil, 2018. aasta andmekaitseseaduse asjakohastest osadest, millega võeti üle direktiiv (EL) 2016/680.

(12) Valmistudes EList väljaastumiseks kehtestas Ühendkuningriigi valitsus 2018. aasta Euroopa Liidust väljaastumise seaduse (European Union (Withdrawal) Act 2018, edaspidi „väljaastumisseadus"), ([15]) millega inkorporeeriti vahetult kohaldatavad liidu õigusaktid Ühendkuningriigi õigusesse ja nähti ette, et nn ELi õigusel põhinevad siseriiklikud õigusaktid jäävad kehtima ka pärast üleminekuperioodi lõppu. 2018. aasta andmekaitseseaduse ([16]) 3. osa, millega võetakse üle direktiiv (EL) 2016/680, on väljaastumisseaduse tähenduses ELi õigusel põhinev siseriiklik õigusakt. Väljaastumisseaduse kohaselt peavad Ühendkuningriigi kohtud tõlgendama ELi õigusel põhinevaid siseriiklikke muutmata õigusakte vastavalt Euroopa Liidu Kohtu (Euroopa Kohus) asjakohasele praktikale ja liidu õiguse üldistele põhimõtetele, nii nagu need kehtisid vahetult enne üleminekuperioodi lõppu (vastavalt „jätkuvalt kohaldatav ELi kohtupraktika" ja „jätkuvalt kohaldatavad ELi õiguse üldpõhimõtted") ([17]).

(13) Väljaastumisseaduse kohaselt on Ühendkuningriigi ministritel volitused kehtestada seadusandlike dokumentidega teiseseid õigusakte, et teha jätkuvalt kohaldatavates ELi õigusaktides vajalikud muudatused, mis tulenevad Ühendkuningriigi väljaastumisest liidust. Seda õigust kasutati 2019. aasta andmekaitset, eraelu puutumatust, elektroonilist sidet, muudatusi jne käsitleva (EList väljaastumise) määrusega (edaspidi „andmekaitse, eraelu puutumatuse ja elektroonilise side määrus") ([18]). Sellega muudetakse Ühendkuningriigi andmekaitsealaseid õigusakte, sealhulgas 2018. aasta andmekaitseseadust, et viia see vastavusse siseriikliku kontekstiga ([19]).

([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 1–177 (edaspidi „väljaastumisleping"), kättesaadav aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=ET.

([15]) 2018. aasta Euroopa Liidust väljaastumise seadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2018/16/contents.

([16]) 2018. aasta andmekaitseseadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2018/12/contents.

([17]) 2018. aasta väljaastumisseaduse paragrahv 6.

([18]) 2019. aasta andmekaitset, eraelu puutumatust, elektroonilist sidet, muudatusi jne käsitlev (EList väljaastumise) määrus (The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019), kättesaadav aadressil https://www.legislation.gov.uk/uksi/2019/419/contents/made, mida on muudetud 2020. aasta andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega, kättesaadav aadressil https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) Väljaastumismäärusega tehakse mitu muudatust 2018. aasta andmekaitseseaduse 3. osas. Paljud neist on tehnilised muudatused, näiteks jäetakse välja viited liikmesriigile või õiguskaitsedirektiivile (vt näiteks 2018. aasta andmekaitseseaduse paragrahvi 48 lõige 8 või paragrahvi 73 lõike 5 punkt a koos siseriikliku õigusega), nii et pärast üleminekuperioodi lõppu toimib 3. osa siseriikliku õiguse sättena. Mõnes kohas tuli teha teist laadi muudatusi, näiteks et Ühendkuningriigi andmekaitse õigusraamistiku eesmärkidel võtab kaitse piisavuse otsuseid vastu minister, mitte enam Euroopa Komisjon (vt 2018. aasta andmekaitseseaduse paragrahv 74A).

(14) Seega on Ühendkuningriigis pärast väljaastumislepingukohase üleminekuperioodi lõppu pädevates asutustes isikuandmete töötlemise õigusnõuded süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil jätkuvalt sätestatud andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega muudetud 2018. aasta andmekaitseseaduse asjakohastes osades, eelkõige seaduse 3. osas. Sellist liiki töötlemisele ei kohaldata Ühendkuningriigi isikuandmete kaitse üldmäärust.

(15) 2018. aasta andmekaitseseaduse 3. osas on sätestatud eeskirjad isikuandmete töötlemise kohta kriminaalõiguskaitse eesmärkidel, sealhulgas andmekaitsepõhimõtted, töötlemise õiguslikud alused (õiguspärasus), andmesubjektide õigused, pädevate asutuste kui vastutavate töötlejate kohustused ja andmete edasisaatmise piirangud. 2018. aasta andmekaitseseaduse 5. ja 6. osas on sätestatud õiguskaitse valdkonnas kohaldatavad järelevalve, täitmise tagamise ja õiguskaitse eeskirjad.

(16) Arvestades politsei tähtsust õiguskaitse valdkonnas, tuleks tähelepanu pöörata ka politseitegevust käsitlevatele eeskirjadele. Kuna politseitegevus on delegeeritud valdkond, kohaldatakse a) Inglismaal ja Walesis, b) Šotimaal ja c) Põhja-Iirimaal politseitegevuse suhtes eri õigusakte, mis on ometi sisult sageli sarnased ([20]). Lisaks selgitatakse politsei volituste korrektset kasutamist eri liiki suunistes. Politseitegevuse suunisete kolm peamisest liiki on järgmised: 1) õigusaktidest tulenevad kohustuslikud suunised, näiteks 1996. aasta politseiseaduse (Police Act 1996) ([21]) alusel koostatud eetikakoodeks (Code of Ethics) ([22]) ja politseiteabe haldamise tegevusjuhend (Code of Practice on the Management of Police Information) ([23]) või politsei- ja kriminaaltõendite seaduse (Police and Criminal Evidence Act) ([24]) alusel koostatud PACE tegevusjuhendid (PACE codes); ([25]) 2) politseikolledži (College of Policing) avaldatud kinnitatud kutsetavad politseiteabe haldamise kohta (Authorised Professional Practice on the Management of Police Information) ([26]) ning 3) tegevussuunised (politsei avaldatud). Riiklik kõrgemate politseiametnike nõukogu (National Police Chiefs Council, Ühendkuningriigi politseijõudude koordineerimise asutus) avaldab tegevussuuniseid, mille on heaks kiitnud kõik politseijõud ja mida seetõttu kohaldatakse kogu riigis ([27]). Suuniste eesmärk on tagada, et politseiasutused haldavad teavet ühtselt ([28]).

(17) Minister avaldas politseiteabe haldamise tegevusjuhendi 2005. aastal, kasutades 1996. aasta politseiseaduse paragrahvis 39A sätestatud volitusi ([29]). Enne kui parlamendile esitatakse politseiseaduse alusel avaldatav tegevusjuhend, peab selle heaks kiitma minister ja selle üle tuleb konsulteerida riikliku kriminaalametiga. Politseiseaduse paragrahvi 39A lõikes 7 nõutakse, et politsei peab võtma arvesse seadusest tulenevaid koodekseid,

([20]) Üksikasjalikuma selgituse jaoks Ühendkuningriigi politseijõudude ja nende volituste kohta vt Ühendkuningriigi kaitse piisavuse arutelude selgitav raamistik, osa F: õiguskaitse (vt joonealune märkus 9).

([21]) 1996. aasta politseiseadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/1996/16/contents.

([22]) Inglismaa ja Walesi kutselise politseitegevuse põhimõtete ja standardite koodeks „The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales“, kättesaadav aadressil https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; politseiteenistuse Põhja-Iirimaa eetikakoodeks „Police Service Northern Ireland Code of Ethic“, kättesaadav aadressil: https://www.nipolicingboard.org.uk/psni-code-ethics; Šotimaa politseitegevuse eetikakoodeks „Code of Ethics for policing in Scotland“, kättesaadav aadressil https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([23]) Politseiteabe haldamise tegevusjuhend, kättesaadav aadressil http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([24]) 1984. aasta politsei- ja kriminaaltõendite seadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/1984/60/contents.

([25]) 1984. aasta politsei- ja kriminaaltõendite seaduse tegevusjuhendid (PACE Codes of Practice), kättesaadavad aadressil https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([26]) Politseiteabe haldamise tegevusjuhend, kättesaadav aadressil https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Andmekaitse käsiraamat politsei andmekaitsespetsialistidele (Data Protection Manual for Police Data Protection Professionals), kättesaadav aadressil https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Näiteks politseiteabe haldamise tegevusjuhendit (vt joonealune märkus 22) kohaldatakse operatiivse politseiteabe säilitamise suhtes (vt käesoleva otsuse põhjendus 47).

([29]) Ühendkuningriigi ametiasutuste sõnul tegeles politseikolledž kaitse piisavuse arutelu perioodi ajal teabe- ja dokumendihalduse tegevusjuhendi koostamisega, mis pidi asendama politseiteabe haldamise tegevusjuhendi. Tegevusjuhend avaldati avalikuks konsulteerimiseks 25. jaanuaril 2021 ja see on kättesaadav aadressil https://www.college.police.uk/article/information-records-management-consultation

ning järelikult peab politsei seda nõuet täitma ([30]). Lisaks peavad muud kui õigusaktidest tulenevad suunised (näiteks kinnitatud kutsetavad politseiteabe haldamise kohta) olema alati kooskõlas politseiteabe haldamise tegevusjuhendiga, mis on selliste tavade suhtes ülimuslik ([31]). Kuigi võib esineda teatavaid operatiivolukordi, kus politseiametnikud peavad sellistest suunistest kõrvale kalduma, peavad nad ikkagi järgima 2018. aasta andmekaitseseaduse 3. osa nõudeid ([32]).

(18) Lisasuuniseid Ühendkuningriigi andmekaitsealaste õigusaktide kohta andmete töötlemiseks õiguskaitse valdkonnas annab teabevolinik (Information Commissioner) ([33]) (lisateave teabevoliniku kohta on esitatud põhjendustes 93–109). Kuigi suunised ei ole õiguslikult siduvad, peavad kohtud võtma kohtuasjades arvesse suuniste rikkumisi, sest suunised on tähtsad tõlgendamisel ja näitavad, kuidas volinik andmekaitsealaseid õigusakte praktikas tõlgendab ja tagab nende täitmise ([34]).

(19) Nagu mainitud põhjendustes 8–10, peavad Ühendkuningriigi õiguskaitseasutused tagama ka Euroopa inimõiguste konventsiooni ja konventsiooni 108 järgimise.

(20) Seega on Ühendkuningriigi kriminaalõiguskaitseasutuste andmetöötlust reguleeriv õigusraamistik ülesehituse ja peamiste osade poolest väga sarnane ELis kohaldatava raamistikuga. Samuti tugineb see raamistik lisaks riiklikus õiguses sätestatud kohustustele, mida on kujundanud ELi õigus, ka rahvusvahelises õiguses sätestatud kohustustele, eelkõige arvestades Ühendkuningriigi osalemist Euroopa inimõiguste konventsioonis ja konventsioonis 108 ning kuuluvust Euroopa Inimõiguste Kohtu alluvusse. Järelikult on need õiguslikult siduvatest rahvusvahelistest õigusaktidest tulenevad kohustused, eelkõige isikuandmete kaitsega seotud kohustused, käesolevas otsuses hinnatava õigusraamistiku tähtis osa.

2.3. **Sisuline ja territoriaalne kohaldamisala**

(21) 2018. aasta andmekaitseseaduse 3. osa kohaldamisala langeb kokku direktiivi (EL) 2016/680 kohaldamisalaga, mida on täpsustatud direktiivi artikli 2 lõikes 2. 3. osa kohaldatakse isikuandmete täielikult või osaliselt automatiseeritud töötlemisele pädeva asutuse poolt ja isikuandmete automatiseerimata töötlemisele pädeva asutuse poolt, kui kõnealused isikuandmed kuuluvad andmete kogumisse või kui need kavatsetakse andmete kogumisse kanda.

(22) Pealegi peab vastutav töötleja 3. osa kohaldamisalasse kuulumiseks olema pädev asutus ja töötlemine peab toimuma õiguskaitse eesmärgil. Seetõttu kohaldatakse käesolevas otsuses hinnatud andmekaitsekorda nende pädevate asutuste kogu õiguskaitsetegevuse suhtes.

(23) 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. 7. lisas loetletud pädevad asutused hõlmavad peale politseijõudude kõiki Ühendkuningriigi ministeeriume ja teisi uurimisülesannetega asutusi (nt Ühendkuningriigi maksu- ja tolliameti volinik (Commissioner for Her Majesty's Revenue and Customs), Walesi maksu- ja tolliamet (Welsh Revenue Authority), konkurentsi- ja turuamet (Competition and Markets Authority) ja Ühendkuningriigi kinnistusregister (Her Majesty's Land Registry) või riiklik kriminaalamet (National Crime Agency)), prokuratuuri organeid, muid kriminaalõiguse asutusi ja muid uurimisülesannetega

([30]) Kohtuasjas R *vs.* Commission of Police of the Metropolis [2014] EWCA Civ 585 kinnitati politseiteabe haldamise tegevusjuhendi õiguslik staatus ja kohtunik Laws teatas, et vastavalt 1996. aasta politseiseaduse paragrahvile 39A peab Londoni politseiameti juht võtma arvesse politseiteabe haldamise tegevusjuhendit ja kinnitatud kutsetavasid politseiteabe haldamise kohta.

([31]) Seda, kas politsei järgib politseiteabe haldamise tegevusjuhendit, kontrollib Tema Majesteedi politseiteenistuse ning tuletõrje- ja päästeteenistuse inspektoraat (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, HMICFRS).

([32]) Vt sellega seoses politseikolledži seisukohta kinnitatud kutsetavade järgimise kohta kõigis politseitöö aspektides; seisukohas selgitatakse, et „ametlik politseiasutus (politseikolledž) on kinnitanud kutsetavad kui kutselise politseitegevuse ametliku allika. Politseiametnikelt ja -töötajatelt eeldatakse kinnitatud kutsetavade arvessevõtmist oma kohustuste täitmisel. Võib esineda asjaolusid, kus politseil on õiguspärane operatiivne põhjus kinnitatud kutsetavadest kõrvalekaldumiseks, kuid see põhjus peab olema selge. Politsei vastutab riiklikult kokkulepitud suunistega vastuolus olevast tegevusest tuleneva kohaliku ja riikliku riski eest ning kui selle tagajärjeks on intsident või uurimine (näiteks politseitegevuse sõltumatu järelevalveasutuse kaudu), vastutab riski eest politsei.", kättesaadav aadressil https://www.app.college.police.uk/faq-page/.

([33]) Õiguskaitse eesmärgil andmete töötlemise juhend, kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Vt kohtuasi Bridges *vs.* the Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), kus kõrge kohus küll möönis, et voliniku suunised ei tulene õigusaktidest, kuid märkis, et „[k]aaludes, kas vastutav töötleja on või ei ole täitnud paragrahvist 64 tulenevat kohustust [viia suure riskiga andmetöötluse kohta läbi andmekaitse mõjuhindamine], võtab kohus arvesse suuniseid, mille teabevolinik on avaldanud andmekaitse mõjuhindamiste kohta".

isikuid või õiguskaitsega tegelevaid organisatsioone ([35]). 2018. aasta andmekaitseseaduse 3. osa – välja arvatud andmesubjektide õiguste ja teabevoliniku büroo teostatava järelevalvega seotud osad – kohaldatakse ka kohtutele nende õigusemõistmise ülesannete täitmisel ([36]). Pädevate asutuste loetelu 7. lisas ei ole ammendav ja minister võib seda ajakohastada määrusega, võttes arvesse avaliku sektori asutuste korralduslikke muudatusi ([37]).

(24) Samuti peab kõnealune töötlemine toimuma õiguskaitse eesmärgil, mis on määratletud kui süütegude tõkestamine, uurimine, avastamine ja nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas kaitse avalikku julgeolekut ähvardavate ohtude eest ja nende ennetamine ([38]). Pädeva asutuse poolset isikuandmete töötlemist ei reguleerita 2018. aasta andmekaitseseaduse 3. osaga, kui töötlemine ei toimu õiguskaitse eesmärkidel, näiteks kui konkurentsi- ja turuamet uurib juhtumeid, mis ei kuulu kriminaalõiguse alla (nt ettevõtete ühinemine). Sellisel juhul kohaldatakse Ühendkuningriigi isikuandmete kaitse üldmäärust koos 2018. aasta andmekaitseseaduse 2. osaga, sest pädevad asutused töötlevad isikuandmeid muudel kui õiguskaitse eesmärkidel. Selleks et teha kindlaks, millist andmekaitsekorda konkreetsete isikuandmete töötlemisele kohaldada (2018. aasta andmekaitseseaduse 2. või 3. osa), peab pädev asutus, st vastutav töötleja, kaaluma, kas sellise töötlemise peamine eesmärk on seotud 2018. aasta andmekaitseseaduse kohase õiguskaitsega.

(25) 2018. aasta andmekaitseseaduse 3. osa territoriaalse kohaldamisala kohta on paragrahvi 207 lõikes 2 ette nähtud, et andmekaitseseadust kohaldatakse sellise isiku tegevuse raames toimuvale isikuandmete töötlemisele, kelle üksus asub kogu Ühendkuningriigi territooriumil. See hõlmab Inglismaa, Walesi, Šotimaa ja Põhja-Iirimaa territooriumil asuvaid avaliku sektori asutusi, mis kuuluvad 2018. aasta andmekaitseseaduse 3. osa kohaldamisalasse ([39]).

2.3.1. *Isikuandmete ja töötlemise määratlus*

(26) Tähtsaimad mõisted „isikuandmed“ ja „isikuandmete töötlemine“ on määratletud 2018. aasta andmekaitseseaduse paragrahvis 3 ning neid kohaldatakse kogu andmekaitseseaduses. Määratlused on tihedalt seotud direktiivi (EL) 2016/680 artiklis 3 sätestatud vastavate määratlustega. 2018. aasta andmekaitseseaduse kohaselt tähendavad isikuandmed igasugust teavet tuvastatud või tuvastatava elava isiku kohta ([40]). 2018. aasta andmekaitseseaduse paragrahvi 3 lõike 3 kohaselt on isik tuvastatav, kui teda saab teabe põhjal otseselt või kaudselt tuvastada, sealhulgas nime või identifitseerimistunnuse põhjal või selle isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal. Mõiste „isikuandmete töötlemine“ on määratletud kui teabe või teabe kogumitega tehtav toiming või toimingute kogum, nagu a) kogumine, dokumenteerimine, korrastamine, struktureerimine või säilitamine; b) kohandamine või muutmine; c) päringute tegemine, lugemine või kasutamine; d) edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine; e) ühitamine või ühendamine või f) piiramine, kustutamine või hävitamine. Seaduses määratletakse ka mõiste „tundlike isikuandmete töötlemine“ kui „a) selliste isikuandmete töötlemine, millest ilmneb rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused või ametiühingusse kuulumine; b) geneetiliste või biomeetriliste andmete töötlemine isiku kordumatuks tuvastamiseks; c) terviseandmete töötlemine; d) isiku seksuaalelu või seksuaalset sättumust käsitlevate andmete töötlemine“ ([41]). Nendega seotud mõisted „biomeetrilised andmed“, ([42]) „terviseandmed“ ([43]) ja „geneetilised andmed“ ([44]) on määratletud 2018. aasta andmekaitseseaduse paragrahvis 205.

([35]) Nende seas on 2018. aasta andmekaitseseaduse 7. lisas loetletud prokuratuuri direktorid, Põhja-Iirimaa prokuratuuri direktor või teabevolinik.

([36]) 2018. aasta andmekaitseseaduse paragrahvi 43 lõige 3.

([37]) 2018. aasta andmekaitseseaduse paragrahvi 30 lõige 3. Luureteenistused (salaluureteenistus, julgeolekuteenistus ja valitsusside peakorter) ei ole pädevad asutused (vt 2018. aasta andmekaitseseaduse paragrahvi 30 lõige 2) ja nende tegevuse suhtes ei kohaldata 2018. aasta andmekaitseseaduse 3. osa. Nende tegevus kuulub 2018. aasta andmekaitseseaduse 4. osa alla.

([38]) 2018. aasta andmekaitseseaduse paragrahv 31.

([39]) Seega ei kohaldata 2018. aasta andmekaitseseadust ega seetõttu käesolevat otsust Briti krooni sõltkondade ja muude Ühendkuningriigi ülemereterritooriumide, nagu Falklandi saarte ja Gibraltari territooriumi suhtes.

([40]) 2018. aasta andmekaitseseaduse kohaldamisalasse ei kuulu surnud isikute andmed.

([41]) 2018. aasta andmekaitseseaduse paragrahvi 35 lõige 8.

([42]) „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.

([43]) „Terviseandmed“ – isiku füüsilise ja vaimse tervisega seotud isikuandmed, sealhulgas temale tervishoiuteenuste osutamist käsitlevad andmed, mis annavad teavet tema terviseseisundi kohta.

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

(27) 2018. aasta andmekaitseseaduse paragrahvis 32 täpsustatakse mõistete „vastutav töötleja“ ja „volitatud töötleja“ määratlust seoses isikuandmete töötlemisega õiguskaitse eesmärkidel. Määratlused on väga sarnased direktiivis (EL) 2016/680 kasutatud vastavate määratlustega. Vastutav töötleja on pädev asutus, kes määrab kindlaks isikuandmete töötlemise eesmärgid ja vahendid. Kui isikuandmete töötlemine on seadusega ette nähtud, on vastutav töötleja pädev asutus, kellele selline kohustus on seadusega kehtestatud. Volitatud töötleja on määratletud kui isik, kes töötleb isikuandmeid vastutava töötleja nimel (ja kes ei ole vastutava töötleja töötaja).

2.4. **Kaitsemeetmed, õigused ja kohustused**

2.4.1. *Isikuandmete töötlemise seaduslikkus ja õiglus*

(28) 2018. aasta andmekaitseseaduse paragrahvi 35 kohaselt peab isikuandmete töötlemine olema seaduslik ja õiglane sarnaselt direktiivi (EL) 2016/680 artikli 4 lõike 1 punktile a. 2018. aasta andmekaitseseaduse paragrahvi 35 lõike 2 kohaselt on isikuandmete töötlemine õiguskaitse eesmärgil seaduslik vaid siis, kui see põhineb õigusel ja andmesubjekt on andnud nõusoleku isikuandmete töötlemiseks sellel eesmärgil või isikuandmete töötlemine on vajalik pädeva asutuse poolt selle eesmärgi kohase ülesande täitmiseks.

2.4.1.1. Isikuandmete töötlemine õiguse alusel

(29) Selleks et tagada 2018. aasta andmekaitseseaduse 3. osa alla kuuluva isikuandmete töötlemise seaduslikkus, peab selline isikuandmete töötlemine põhinema õigusel, nagu on ka sätestatud direktiivi (EL) 2016/680 artiklis 8. Seaduslik isikuandmete töötlemine tähendab, et selleks on luba antud kas statuudi, üldise õiguse või kuninglike eesõigustega ([45]).

(30) Pädevate asutuste volitusi reguleeritakse üldjuhul statuutidega: see tähendab, et nende ülesanded ja volitused on selgesti sätestatud parlamendi vastu võetud õigusaktides ([46]). Teatavatel juhtudel võivad politsei ja teised 2018. aasta andmekaitseseaduse 7. lisas loetletud pädevad asutused tugineda andmete töötlemisel üldisele õigusele ([47]). Üldine õigus on kujunenud kohtuotsustega loodud pretsedentide põhjal. Üldisest õigusest tulenevad politsei volitused ja keskne ülesanne kaitsta kodanikke kuritegevuse avastamise ja tõkestamise kaudu ([48]). Selle ülesande täitmiseks võivad politseijõud aga

([45]) 2018. aasta andmekaitseseaduse selgitavad märkused, punkt 181, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Näiteks riikliku kriminaalameti (National Crime Agency) volitused tulenevad 2013. aasta kuritegevuse vastu võitlemise ja kohtute seadusest, mis on kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2013/22/contents. Samamoodi on toidustandardiameti (Food Standards Agency) volitused ette nähtud 1999. aasta toidustandardiseaduses, mis on kättesaadav aadressil https://www.legislation.gov.uk/ukpga/1999/28/contents. Teisi näiteid: süüteo eest vastutusele võtmise 1985. aasta seadus, millega loodi Ühendkuningriigi prokuratuur (vt https://www.legislation.gov.uk/ukpga/1985/23/contents); 2005. aasta maksu- ja tolliameti seadus, millega loodi Ühendkuningriigi maksu- ja tolliamet (vt https://www.legislation.gov.uk/ukpga/2005/11/contents); Šotimaa 1995. aasta kriminaalmenetlusseadus, millega loodi Šotimaa kriminaalasjade järelevalve komisjon (Scottish Criminal Cases Review Commission) (vt https://www.legislation.gov.uk/ukpga/1995/46/contents); Põhja-Iirimaa 2002. aasta kohtuseadus, millega loodi Põhja-Iirimaa prokuratuur (vt https://www.legislation.gov.uk/ukpga/2002/26/contents), ning 1987. aasta kriminaalõigusseadus, millega loodi raskete pettuste amet ja sätestati selle volitused (vt https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Näiteks Ühendkuningriigi ametiasutuste antud teabe põhjal tulenevad Šotimaa prokuratuuri (Crown Office and Procurator Fiscal Service) juhtiva õigusnõuniku (Lord Advocate) volitused uurida surmajuhtumeid ja võtta vastutusele süütegude eest üldisest õigusest, samas kui osa tema ülesannetest on kehtestatud statuudiga. Lisaks tulenevad monarhi ja seega ka valitsussektori, ministeeriumite ja ministrite volitused õigusaktidest, üldisest õigusest ja kuninglikust eesõigusest (need on monarhile üldise õiguse alusel antud volitused, mida teostavad ministrid).

([48]) Ühendkuningriigi kaitse piisavuse arutelude selgitava raamistiku (Explanatory Framework for Adequacy Discussion) osa F: õiguskaitse, lk 8 (vt joonealune märkus 9).

tugineda nii üldisest õigusest tulenevatele kui ka seadusandlikele volitustele ([49]). Valdkondades, kus politseil on seadusjärgsed volitused, on need ülimuslikud üldisest õigusest tulenevate volituste suhtes ([50]).

(31) Kohtud on tunnistanud politseiametnike üldisest õigusest tulenevate volituste ja kohustuste ulatust, sedastades, et need hõlmavad kõiki meetmeid, mis näivad politseiametnikule vajalikud rahu hoidmiseks, kuritegevuse tõkestamiseks või vara kaitsmiseks kuritegeliku kahju eest ([51]). Üldisest õigusest tulenevad volitused ei ole absoluutsed volitused. Neile kehtib mitu piirangut, sealhulgas kohtute ([52]) ja õigusaktidega, eelkõige 1998. aasta inimõiguste seaduse (Human Rights Act 1998) ja 2010. aasta võrdõiguslikkuse seadusega (Equality Act 2010), ([53]) kehtestatud kitsendused. 2018. aasta andmekaitseseaduse 3. osa alusel andmeid töötlevate pädevate asutuste puhul hõlmab see üldisest õigusest tulenevate volituste kasutamist kooskõlas 2018. aasta andmekaitseseaduses sätestatud nõuetega ([54]). Andmete töötlemise teostamise otsuse puhul tuleb lisaks arvesse võtta kohaldatavate suuniste, näiteks politseiteabe haldamise tegevusjuhendi ja Ühendkuningriigi maadele eriomaste suuniste ([55]) nõudeid. Valitsus ja operatiivtööga tegelevad politseiorganid on avaldanud mitu suunisdokumenti, mis aitavad tagada, et politseiametnikud kasutavad oma isikuandmete töötlemise alaseid volitusi üldises õiguses või asjakohases statuudis ([56]) sätestatud piirides.

(32) Õiguse üks osadest on kuninglikud eesõigused, millest tulenevad monarhile teatavad volitused, mida rakendab täidesaatev võim ja mis ei põhine statuudil, vaid tulenevad monarhi suveräänsusest ([57]). Õiguskaitse kontekstis on väga vähe näiteid asjakohastest eesõiguslikest volitustest. Nende hulka kuulub vastastikuse õigusabi raamistik, mis võimaldab ministril jagada õiguskaitse eesmärkidel andmeid kolmandate riikidega ja sellisel viisil andmete jagamise

([49]) Tähtsaimad õigusaktid, milles on ette nähtud politsei peamiste volituste (vahistamine, läbiotsimine, jätkuva kinnipidamise lubamine, sõrmejälgede võtmine, intiimsete proovide võtmine, pealtkuulamine, juurdepääs sideandmetele) kord, on: i) Inglismaal ja Walesis 1984. aasta politsei- ja kriminaaltõendite seadus (PACE), kättesaadav aadressil https://www.legislation.gov.uk/ukpga/1984/60/contents (mida on muudetud 2012. aasta vabaduste kaitse seadusega, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2012/9/contents), ning 2016. aasta uurimisvolituste seadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2016/25/contents; ii) Šotimaal 2016. aasta kriminaalõigusseadus, kättesaadav aadressil https://www.legislation.gov.uk/asp/2016/1/contents, ja 1995. aasta kriminaalmenetluse seadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/1995/46/contents; iii) Põhja-Iirimaal 1989. aasta politsei- ja kriminaaltõendite määrus, kättesaadav aadressil https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Ühendkuningriigi ametiasutused on selgitanud, et õigusaktide ülimuslikkus on Ühendkuningriigis pikaajaline tava, mis pärineb juba otsusest kohtuasjas Entick *vs.* Carrington [1765] EWHC KB J98, milles tunnistati, et täidesaatva võimu volitustel on piirid, ning kehtestati põhimõte, et üldisest õigusest tulenevad volitused ning monarhi ja valitsuse eesõiguslikud volitused on allutatud riigis kehtivatele seadustele.

([51]) Vt kohtuasi Rice *vs.* Connolly [1966] 2 QB 414.

([52]) Vt kohtuasi R (Catt) *vs.* Association of Chief police Officers [2015] AC 1065, kus seoses politsei volitustega hankida ja hoida teavet isiku kohta (kes oli toime pannud süüteo), otsustas Lord Sumption, et üldise õiguse kohaselt on politseil volitus hankida ja säilitada teavet politseitöö eesmärkidel, st üldiselt võttes avaliku korra säilitamiseks ning kuritegevuse tõkestamiseks ja avastamiseks. Need volitused ei võimalda kasutada teabe hankimiseks sekkuvaid meetodeid, nagu eravaldusesse sisenemine või rünnakuks liigitatav tegevus (v.a vahistamine üldisest õigusest tulenevate volituste raames). Kohtunik leidis, et antud juhul olid üldisest õigusest tulenevad volitused piisavad, et võimaldada nendes kaebustes käsitletava avaliku teabe hankimist ja säilitamist.

([53]) 2010. aasta võrdõiguslikkuse seadus, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Vt kõrge kohtu otsus kohtuasjas Bridges *vs.* the Chief Constable of South Wales Police (vt joonealune märkus 33) – näide juhtumi kohta, kus politsei üldisest õigusest tulenevaid volitusi hinnatakse 1998. aasta andmekaitseseaduse raamistikus. Vt ka kohtuasjad Vidal-Hall *vs.* Google Inc [2015] EWCA Civ 311 ja Richard *vs.* BBC [2018] EWHC 1837 (Ch).

([55]) Vt näiteks Põhja-Iirimaa politseiteenistuse suunised andmehalduse teenistusjuhendis, kättesaadav aadressil https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Alamkoda on avaldanud infodokumendi, milles on sätestatud Inglismaa ja Walesi politsei peamised üldisest õigusest ja seadusõigusest tulenevad volitused (vt https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Kui selle dokumendi kohaselt tulenevad näiteks monarhi kehtestatud rahu tagamise ja jõu kasutamise volitused üldisest õigusest, siis läbiotsimisvolitused tulenevad alati statuudist. Politsei vahistamis- ja läbiotsimisvolituste kohta on esitatud teavet Šotimaa valitsuse veebisaidil (vt https://www.gov.scot/policies/police/police-powers/).

([57]) Ühendkuningriigi ametiasutuste antud teabe põhjal hõlmavad valitsuse rakendatavad eesõiguslikud volitused näiteks lepingute koostamist ja ratifitseerimist, diplomaatiat ning relvajõudude kasutamist Ühendkuningriigis, et aidata politseil tagada rahu.

volitus ei ole alati sätestatud statuudis ([58]). Kuninglikele eesõigustele kehtivad üldise õiguse põhimõtted ([59]) ja need on allutatud statuudile, mistõttu kohaldatakse eesõiguste suhtes 1998. aasta inimõiguste seaduse ja 2018. aasta andmekaitseseadusega ette nähtud piiranguid ([60]).

(33) Sarnaselt direktiivi (EL) 2016/680 artikliga 8 näeb Ühendkuningriigi kord ette, et seaduslikkuse põhimõtte järgimiseks peaksid pädevad asutused tagama, et kui isikuandmete töötlemine põhineb õigusel, peab see ühtlasi olema õiguskaitse eesmärgi kohase ülesande täitmiseks vajalik. Teabevoliniku büroo selgitab seda järgmiselt: „see peab olema sihipärane ja proportsionaalne viis eesmärgi täitmiseks. Isikuandmete töötlemine ei põhine õigusel, kui eesmärki saab mõistlikult täita muul vähem sekkuval viisil. Ei piisa väitest, et töötlemine on vajalik, sest olete otsustanud oma tegevust konkreetsel viisil ellu viia. Küsimus on selles, kas töötlemine on vajalik sedastatud eesmärgi täitmiseks“ ([61]).

2.4.1.2. Isikuandmete töötlemine andmesubjekti nõusoleku alusel

(34) Nagu mainitakse põhjenduses 28, on 2018. aasta andmekaitseseaduse paragrahvi 35 lõikes 2 ette nähtud võimalus töödelda isikuandmeid isiku nõusoleku alusel.

(35) Nõusolek ei näi aga olevat käesoleva otsuse kohaldamisalasse kuuluvate töötlemistoimingute puhul asjakohane õiguslik alus. Käesoleva otsusega hõlmatud töötlemistoimingud on nimelt alati seotud andmetega, mille liikmesriigi pädev asutus on edasi saatnud Ühendkuningriigi pädevale asutusele direktiivi (EL) 2016/680 alusel. Seetõttu ei hõlma need tavaliselt avaliku sektori asutuse ja andmesubjektide vahelist otsest suhtlust (kogumine), mis võiks põhineda 2018. aasta andmekaitseseaduse paragrahvi 35 lõike 2 punkti a kohasel nõusolekul.

(36) Kuigi seega ei peeta käesoleva otsuse kohase hindamise jaoks nõusolekut asjakohaseks, tuleb täielikkuse huvides märkida, et õiguskaitse kontekstis ei põhine isikuandmete töötlemine kunagi vaid nõusolekul, sest pädeval asutusel peab alati olema volitus, mis võimaldab tal andmeid töödelda ([62]). Konkreetsemalt tähendab see, et samamoodi, nagu on lubatud direktiivi (EL) 2016/680 ([63]) kohaselt, on nõusoleku vajalikkus lisatingimus, mis võimaldab teatavaid piiratud ja spetsiifilisi töötlemistoiminguid, mida ei saaks muul juhul teha, näiteks sellise isiku DNA-proovi kogumine ja töötlemine, kes ei ole kahtlusalune. Kui sellisel juhul nõusolekut ei anta või see võetakse tagasi, siis töötlemist ei toimu ([64]).

([58]) Selle kohta vt Ühendkuningriigi andmete edasisaatmise korra hindamine põhjendustes 74–87.

([59]) Vt kohtuasi Bancoult *vs.* Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, kus kohtud otsustasid, et ka eesõiguslikule volitusele teha kuninglikke korraldusi kehtivad kohtuliku kontrolli tavapärased alused.

([60]) Vt kohtuasi Attorney-General *vs.* De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, kus kohus leidis, et eesõiguslikke volitusi ei saa kasutada, kui neid asendavad seadusõigusest tulenevad volitused; kohtuasi Laker Airways Ltd *vs.* Department of Trade 1977] QB 643, kus kohus leidis, et eesõiguslikke volitusi ei saa kasutada õigusaktide kohaldamise vältimiseks; kohtuasi R *vs.* Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, kus kohus leidis, et eesõiguslikke volitusi ei saa kasutada, kui need on vastuolus kehtestatud õigusaktiga, isegi kui see kehtestatud õigusakt ei ole veel jõustunud; kohtuasi R (Miller) *vs.* Secretary of State for Exiting the European Union [2017] UKSC 5, kus kohus kinnitas õigusakti võimet kohandada ja tühistada eesõiguslikke volitusi. Üldise ülevaate saamiseks kuninglike eesõiguste ja seadusõigusest või üldisest õigusest tulenevate volituste vahekorra kohta vt alamkoja infodokument, kättesaadav aadressil https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Õiguskaitse eesmärgil andmete töötlemise juhend, „Esimene põhimõte“ („What is the first principle about?“), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) See tuleneb 2018. aasta andmekaitseseaduse asjakohase sätte sõnastusest, mille kohaselt on isikuandmete töötlemine õiguskaitse eesmärgil seaduslik vaid sel juhul ja sellises ulatuses, kui „see põhineb õigusel“ ja „a) andmesubjekt on andnud nõusoleku isikuandmete töötlemiseks sellel eesmärgil või b) isikuandmete töötlemine on vajalik pädeva asutuse poolt eesmärgi kohase ülesande täitmiseks“.

([63]) Vt direktiivi (EL) 2016/680 põhjendused 35 ja 37.

([64]) Ühendkuningriigi ametiasutused on selgitanud, et nõusolek võib olla asjakohane alus isikuandmete töötlemiseks näiteks juhul, kui politsei võtab DNA-proovi seoses teadmata kadunud isikuga, et võrrelda seda surnukeha DNAga, kui surnukeha peaks leitama. Sellistel asjaoludel oleks politseil kohatu nõuda andmesubjektilt proovi andmist; selle asemel paluks politsei isiku vabatahtlikku nõusolekut, mille võib igal ajal tagasi võtta. Kui nõusolek võetakse tagasi, ei saa andmeid enam töödelda, kui proovi töötlemise jätkamiseks ei kehtestata uut õiguslikku alust (nt andmesubjektist sai kahtlusalune). Teine asjakohane näide on see, kui politsei uurib süütegu, mille ohvrile (röövi, seksuaalsüüteo või perevägivalla ohver või tapmisohvri või muu süüteo ohvri sugulased) oleks kasulik saada abi heategevusorganisatsioonist Victim Support (toetab kuriteo- ja muu traumaatilise sündmuse ohvreid). Sellises olukorras jagab politsei ohvriabi organisatsiooniga isiklikku teavet, näiteks nimi ja kontaktandmed, vaid ohvri nõusolekul.

(37) Isiku nõusolekut eeldavatel juhtudel peab selline nõusolek olema ühemõtteline ja selgesti väljendatud ([65]). Politsei peab esitama isikuandmete kaitse teate, sealhulgas vajaliku teabe nõusoleku korrektse kasutamise kohta. Mõned jaoskonnad avaldavad ka lisateavet selle kohta, kuidas nad järgivad andmekaitsealaseid õigusakte, sealhulgas kuidas ja millal nad kasutaksid nõusolekut õigusliku alusena ([66]).

2.4.1.3. Tundlike isikuandmete töötlemine

(38) Eriliiki andmete töötlemisel tuleks kohaldada konkreetseid kaitsemeetmeid. Sarnaselt direktiivi (EL) 2016/680 artikliga 10 ette nähtuga on 2018. aasta andmekaitseseaduse 3. osas sätestatud tundliku töötlemise jaoks rangemad kaitsemeetmed ([67]).

(39) 1998. aasta andmekaitseseaduse paragrahvi 35 lõike 3 kohaselt võivad pädevad asutused töödelda tundlikke andmeid õiguskaitse eesmärkidel üksnes kahel juhul: 1) andmesubjekt on andnud õiguskaitse eesmärgil andmete töötlemiseks nõusoleku ja töötlemise ajal on vastutaval töötlejal kehtiv nõuetekohane dokument tegevuspõhimõtete kohta ([68]) või 2) andmete töötlemine on rangelt vajalik õiguskaitse eesmärgil, töötlemine vastab vähemalt ühele 2018. aasta andmekaitseseaduse 8. lisa tingimusele ja töötlemise ajal on vastutaval töötlejal kehtiv nõuetekohane dokument tegevuspõhimõtete kohta ([69]).

(40) Esimesel juhul ei peeta nõusolekule tuginemist käesolevas otsuses käsitletava isikuandmete edastamise puhul asjakohaseks, nagu on selgitatud ka põhjenduses 38 ([70]).

(41) Kui tundlike andmete töötlemine ei põhine nõusolekul, võib selle alusena kasutada üht 2018. aasta andmekaitseseaduse 8. lisas loetletud tingimustest. Need tingimused on seotud seadusjärgsetel eesmärkidel vajaliku töötlemisega; õigusemõistmisega; andmesubjekti või teise isiku eluliste huvide kaitsmisega; laste ja ohus olevate isikute kaitsega; õiguslike nõuetega; kohtute tegevusega; pettuste ennetamisega; arhiveerimisega; juhtudega, kui andmesubjekt on isikuandmed ilmselgelt avalikustanud. Kõigi 8. lisas esitatud tingimuste vajalikkust kontrollitakse rangelt, välja arvatud juhul, kui andmed on ilmselgelt avalikustatud. Teabevoliniku selgituse kohaselt „rangelt vajalik tähendab selles kontekstis, et töötlemine peab olema seotud tungiva sotsiaalse vajadusega ja seda ei ole võimalik

([65]) 2018. aasta andmekaitseseaduse 3. osa alusel toimuva isikuandmete töötlemise eesmärkidel kasutatavat nõusolekut ei ole eraldi määratletud. Teabevoliniku büroo on koostanud suunised 2018. aasta andmekaitseseaduse 3. osa kohase nõusoleku mõiste kohta, selgitades, et sellel on sama tähendus kui isikuandmete kaitse üldmääruses esitatud määratlusel ja need tuleks kooskõlla viia, täpsustades, et „nõusolek peab olema vabatahtlik, konkreetne ja teadlik ning võimalus valida, kas oma andmete töötlemisega nõustuda, peab olema tõeline“ (õiguskaitse eesmärgil andmete töötlemise juhend, „Esimene põhimõte“ („What is the first principle about?“) (vt joonealune märkus 64) ja andmekaitse suunis nõusoleku kohta, kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Vt näiteks teave Lincolnshire'i politsei veebisaidil (https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) või West Yorkshire'i politsei veebisaidil (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) 2018. aasta andmekaitseseaduse paragrahvi 35 lõige 8.

([68]) 2018. aasta andmekaitseseaduse paragrahvi 35 lõige 4.

([69]) 2018. aasta andmekaitseseaduse paragrahvi 35 lõige 5.

([70]) Täielikkuse huvides tuleb märkida, et kui andmete töötlemine põhineb nõusolekul, peab see olema vabatahtlik, konkreetne ja teadlik ning oma andmete töötlemisega nõustumiseks tuleb teha konkreetne valik. Lisaks peab vastutaval töötlejal olema andmesubjekti nõusoleku alusel andmete töötlemiseks kehtiv nõuetekohane dokument tegevuspõhimõtete kohta. 2018. aasta andmekaitseseaduse paragrahvis 42 on esitatud nõuded, millele nõuetekohane dokument tegevuspõhimõtete kohta peab vastama. Selles väljendatakse selgesti, et dokumendis tuleb selgitada vähemalt vastutava töötleja menetlusi, millega tagada andmekaitsepõhimõtete järgimine, ning selgitada vastutava töötleja põhimõtteid isikuandmete säilitamisel ja kustutamisel. 2018. aasta andmekaitseseaduse paragrahvi 42 kohaselt tähendab see, et vastutav töötleja peab koostama dokumendi, milles a) selgitatakse vastutava töötleja menetlusi andmekaitsepõhimõtete järgimise tagamiseks ning b) selgitatakse vastutava töötleja põhimõtteid isikuandmete säilitamisel ja kustutamisel, mis tuginevad andmesubjekti nõusolekule, või näidatakse, kui kaua selliseid isikuandmeid tõenäoliselt säilitatakse. Dokumendis tegevuspõhimõtete kohta nõutakse, et töötlemistoiminguid dokumenteerides peaks vastutav töötleja alati esitama punktides a ja b nimetatud andmed. Teabevoliniku büroo on avaldanud näidisdokumendi (õiguskaitse eesmärgil andmete töötlemise juhend, „Tundlike isikuandmete töötlemise tingimused“ („Conditions for sensitive processing“), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) ja võib võtta täitemeetmeid, kui vastutavad töötlejad ei täida neid nõudeid. Nõuetekohast dokumenti tegevuspõhimõtete kohta vaatavad ka kohtud 2018. aasta andmekaitseseaduse võimalike rikkumiste kaalumisel. Näiteks hiljutises kohtuasjas R (Bridges) *vs.* Chief Constable of South Wales Police vaatasid kohtud üle vastutava töötleja nõuetekohase dokumendi tegevuspõhimõtete kohta ja leidsid, et see on asjakohane, kuid võiks olla üksikasjalikum. Lõuna-Walesi politsei vaatas dokumendi üle ja ajakohastas seda kooskõlas teabevoliniku büroo uute suunistega (vt joonealune märkus 33). 2018. aasta andmekaitseseaduse paragrahvi 42 lõike 3 kohaselt peaks vastutav töötleja nõuetekohast dokumenti tegevuspõhimõtete kohta korrapäraselt ajakohastama. Täiendava kaitsemeetmena peab vastutav töötleja 2018. aasta andmekaitseseaduse paragrahvi 42 lõike 4 kohaselt töötlemistoiminguid järjepidevalt dokumenteerima, mis hõlmab lisaelemente peale 2018. aasta andmekaitseseaduse paragrahvis 61 sätestatud vastutava töötleja üldise kohustuse dokumenteerida töötlemistoiminguid.

mõistlikult saavutada vähem sekkuvate meetoditega“ ([71]). Teatavate tingimuste suhtes kohaldatakse lisapiiranguid. Näiteks seadusjärgsete eesmärkide tingimusele ja kaitse tingimusele (8. lisa punktid 1 ja 4) tuginemiseks peab olema lisaks täidetud märkimisväärse avaliku huvi kriteerium. Seoses laste turvalisuse tagamise tingimustega (8. lisa punkt 4) peab andmesubjekt olema teatavas vanuses ja olema ohus. Vastutav töötleja võib kohaldada 8. lisa punktis 4 sätestatud tingimust vaid konkreetsetel asjaoludel ([72]). Samuti kehtivad piirangud kohtute tegevuse ja pettuste ennetamise tingimuste puhul (vastavalt 8. lisa punktid 7 ja 8). Mõlemad on kohaldatavad vaid kindlatele vastutavatele töötlejatele. Kohtute tegevuse tingimust võivad kasutada ainult kohtud või muud õigusasutused ja pettuste ennetamise tingimusele võivad tugineda vaid vastutavad töötlejad, kes on pettusevastased organisatsioonid.

(42) Kui töötlemine tugineb ühele 8. lisas loetletud tingimustest ja vastavalt 2018. aasta andmekaitseseaduse paragrahvile 42 peab olema kehtiv nõuetekohane tegevuspõhimõtteid käsitlev dokument, milles selgitatakse vastutava töötleja menetlusi andmekaitsepõhimõtete järgimise tagamiseks ning vastutava töötleja põhimõtteid seoses isikuandmete säilitamise ja kustutamisega, ning kohaldatakse järjepideva dokumenteerimise kohustust.

2.4.2. *Eesmärgi piirang*

(43) Isikuandmeid tuleks töödelda konkreetsel eesmärgil ja kasutada seejärel üksnes määral, mil see on kooskõlas töötlemise eesmärgiga. See andmekaitsepõhimõte on tagatud 2018. aasta andmekaitseseaduse paragrahviga 36. Sarnaselt direktiivi (EL) 2016/680 artikli 4 lõike 1 punktiga b nõutakse selles artiklis, et a) õiguskaitse eesmärk, milleks isikuandmeid kogutakse, peab olema täpselt ja selgelt kindlaks määratud ja õiguspärane ning b) nii kogutud isikuandmeid ei tohi töödelda viisil, mis on kogumise eesmärgiga vastuolus.

(44) Kui pädevad asutused töötlevad andmeid õiguskaitse eesmärgil, võib see hõlmata arhiveerimist, teadus- või ajaloouuringuid ja statistilisi eesmärke ([73]). 2018. aasta andmekaitseseaduses täpsustatakse ka, et sellistel juhtudel ei ole arhiveerimine (või töötlemine teadus- või ajaloouuringute ja statistilistel eesmärkidel) lubatud, kui arhiveerida soovitakse otsuseid, mis on tehtud kindla andmesubjekti kohta, või on tõenäoline, et see põhjustab talle märkimisväärset kahju või märkimisväärseid kannatusi ([74]).

2.4.3. *Õigsus ja võimalikult väheste andmete kogumine*

(45) Andmed peavad olema õiged ja vajaduse korral ajakohastatud. Need peavad olema ka piisavad, asjakohased ja mitte ülemäärased seoses eesmärkidega, mille tarvis neid töödeldakse. Need põhimõtted on sarnaselt direktiivi (EL) 2016/680 artikli 4 lõike 1 punktidega c, d ja e tagatud 2018. aasta andmekaitseseaduse paragrahvidega 37 ja 38. Tuleb võtta kõik mõistlikud meetmed, millega tagatakse, et ebaõiged isikuandmed ([75]) kustutatakse

([71]) Õiguskaitse eesmärgil andmete töötlemise juhend, „Tundlike isikuandmete töötlemise tingimused“ („Conditions for sensitive processing“) (vt joonealune märkus 70).

([72]) Töötlemine toimub ilma andmesubjekti nõusolekuta, kui: a) andmesubjekt ei saa anda töötlemiseks nõusolekut; b) ei ole mõistlikku alust eeldada, et vastutav töötleja saab töötlemiseks andmesubjekti nõusoleku; c) töötlemine peab toimuma ilma andmesubjekti nõusolekuta, sest andmesubjektilt nõusoleku hankimine takistaks alapunkti 1 alapunktis a mainitud kaitse tagamist.

([73]) Vt 2018. aasta andmekaitseseaduse paragrahvi 41 lõige 1.

([74]) Vt 2018. aasta andmekaitseseaduse paragrahvi 41 lõige 2.

([75]) 2018. aasta andmekaitseseaduse paragrahvis 205 on ebatäpsed isikuandmed määratletud kui ebaõiged või eksitavad isikuandmed. Ühendkuningriigi ametiasutused on selgitanud, et on tavapärane, et kriminaaluurimistega seotud andmed on sageli mittetäielikud, kuid võivad sellest hoolimata olla õiged.

või neid parandatakse viivitamata, ([76]) võttes arvesse õiguskaitse eesmärki, mille tarvis neid töödeldakse, ([77]) ning et ebaõigeid, mittetäielikke või aegunud isikuandmeid ei edastata ega tehta kättesaadavaks ühelgi õiguskaitse eesmärgil ([78]).

(46) Sarnaselt direktiivi (EL) 2016/680 artikliga 7 näeb Ühendkuningriigi andmekaitsekord ette, et faktidel põhinevaid isikuandmeid tuleb eristada nii palju kui võimalik isiklikel hinnangutel põhinevatest isikuandmetest ([79]). Kui see on asjakohane ja võimalik, tuleb selgesti eristada isikuandmeid, mis on seotud eri andmesubjektide kategooriatega, nagu kahtlusalused, süüteos süüdimõistetud, süütegude ohvrid ja tunnistajad ([80]).

2.4.4. *Säilitamise piirang*

(47) Direktiivi (EL) 2016/680 artikli 5 kohaselt ei tohiks andmeid põhimõtteliselt säilitada kauem, kui see on vajalik isikuandmete töötlemise eesmärkide täitmiseks. 2018. aasta andmekaitseseaduse paragrahvi 39 kohaselt ja sarnaselt selle direktiivi artikliga 5 on keelatud säilitada õiguskaitse eesmärgil töödeldud isikuandmeid kauem, kui see on vajalik seoses andmete töötlemise eesmärgiga. Ühendkuningriigi õiguskord näeb ette, et tuleb kehtestada nõuetekohased ajavahemikud, mille jooksul tuleb läbi vaadata, kas isikuandmete jätkuv säilitamine õiguskaitse eesmärkidel on vajalik. Täiendavad eeskirjad isikuandmete säilitamisega seotud tavade ja kohalduvate ajapiirangute kohta on sätestatud asjakohastes õigusaktides ja suunistes, millega reguleeritakse politsei volitusi ja tegevust. Näiteks Inglismaal ja Walesis moodustavad politseikolledži politseiteabe haldamise tegevusjuhend ja kinnitatud kutsetavad politseiteabe haldamise kohta raamistiku, mis aitab tagada politsei operatiivteabe haldamises järjepidevat riskipõhist säilitamis-, läbivaatamis- ja kõrvaldamisprotsessi ([81]). Raamistikuga seatakse kogu teenistustele selged ootused selle kohta, kuidas teavet tuleks luua, jagada, kasutada ja hallata politseiasutustes ja nende vahel ning teiste asutustega ([82]). Politseilt eeldatakse tegevusjuhendi järgimist, mida kontrollib Tema Majesteedi politseiteenistuse ning tuletõrje- ja päästeteenistuse inspektoraat (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, HMICFRS) ([83]).

(48) Seadus ei nõua politseiteabe haldamise tegevusjuhendi järgimist Põhja-Iirimaa politseiteenistuselt. 2011. aastal vastu võetud politseiteabe haldamise raamistikku täiendab aga Põhja-Iirimaa politseiteenistuse käsiraamat, ([84]) milles on sätestatud põhimõtted ja kord politseiteabe haldamise tegevusjuhendi kohaldamise kohta Põhja-Iirimaal.

([76]) 2018. aasta andmekaitseseaduse paragrahvi 38 lõike 1 punkt b.

([77]) Kaitse piisavuse arutelu selgitava Ühendkuningriigi raamistiku kohaselt tagab see, et „arvesse võetakse nii andmesubjektide õigusi kui ka õiguskaitseasutuste operatiivseid vajadusi. Seda aspekti kaaluti hoolikalt andmekaitseseaduse eelnõu koostamise ajal, sest võib esineda konkreetseid ja piiratud operatiivseid põhjuseid, miks andmeid ei saa parandada. Seda juhtub kõige tõenäolisemalt siis, kui kõnealuseid ebaõigeid isikuandmeid tuleb säilitada originaalvormingus tõendamise eesmärkidel" (vt kaitse piisavuse arutelu selgitav Ühendkuningriigi raamistik, osa F: õiguskaitse, lk 21, vt joonealune märkus 9).

([78]) 2018. aasta andmekaitseseaduse paragrahvi 38 lõige 4. Lisaks tuleb 2018. aasta andmekaitseseaduse paragrahvi 38 lõike 5 kohaselt enne isikuandmete edastamist või kättesaadavaks tegemist kontrollida nende kvaliteeti, isikuandmete edastamisel tuleb alati lisada vajalik teave, mis võimaldab andmete vastuvõtjal hinnata andmete õigsust, täielikkust, usaldusväärsust ja ajakohasust, ning kui pärast isikuandmete edastamist ilmneb, et andmed ei olnud õiged või edastamine oli ebaseaduslik, tuleb viivitamata teavitada vastuvõtjat.

([79]) 2018. aasta andmekaitseseaduse paragrahvi 38 lõige 2.

([80]) 2018. aasta andmekaitseseaduse paragrahvi 38 lõige 3.

([81]) Raamistik tagab järjepidevuse hangitud isikuandmete säilitamise nõuete kohaldamisel. Läbivaatamisperiood oleneb süüteost, need on jagatud nelja rühma: 1) teatavad kodanikukaitseküsimused; 2) muud seksuaal-, vägivaldsed ja rasked süüteod; 3) kõik muud süüteod; 4) muud. Üksikasjad on kinnitatud kutsetavades politseiteabe haldamise kohta (vt joonealune märkus 26).

([82]) Ühendkuningriigi ametiasutuste antud teabe kohaselt võivad ka teised organisatsioonid soovi korral järgida politseiteabe haldamise tegevusjuhendit, näiteks Ühendkuningriigi maksu- ja tolliamet ning riiklik kriminaalamet järgivad vabatahtlikult paljusid politseiteabe haldamise tegevusjuhendi põhimõtteid, et tagada õiguskaitse järjepidevus. Üldjuhul kehtestab enamik organisatsioone oma töötajatele konkreetsed põhimõtted ja suunised isikuandmete haldamise kohta nende tööülesannete raames ja vastavalt konkreetse organisatsiooni eripärale. Tavaliselt sisaldab see ka kohustuslikku koolitust.

([83]) Politseiteabe haldamise tegevusjuhendi avaldamisel lähtuti 1996. aasta politseiseaduse alusel sätestatud volitustest, mis võimaldavad politseikolledžil avaldada politseitöö tõhususega seotud tegevusjuhendeid. Enne kui parlamendile esitatakse selle seaduse alusel avaldatav tegevusjuhend, peab selle heaks kiitma minister ja selle asjus tuleb konsulteerida riikliku kriminaalametiga. 1996. aasta politseiseaduse paragrahvi 39A lõikes 7 nõutakse, et politsei peab võtma arvesse 1996. aasta politseiseadusest tulenevaid koodekseid.

([84]) Põhja-Iirimaa politseiteenistuse käsiraamatu peatükid 1–6.

(49) Šotimaal tuginevad politseijõud andmete säilitamise standardsele töökorrale (SOP), ([85]) mis täiendab Šotimaa politseiteenistuse andmehalduse põhimõtteid ([86]). Standardses töökorras on sätestatud konkreetsed eeskirjad Šotimaa politsei valduses olevate andmete säilitamise kohta.

(50) Kogu Ühendkuningriigis kohaldatavat andmete läbivaatamise üldnõuet täiendavad üksikasjad on esitatud kohalikes eeskirjades. Näiteks Inglismaal ja Walesis on 2012. aasta vabaduste kaitse seadusega muudetud politsei- ja kriminaaltõendite seaduses ette nähtud sõrmejälgede ja DNA-profiilide säilitamine ning erikord seoses süüdimõistmata isikutega ([87]). Vabaduste kaitse seadusega loodi ka biomeetriliste andmete säilitamise ja kasutamise voliniku ametikoht (edaspidi „biomeetriavolinik“) ([88]). Vahistamisfotode 2017. aasta läbivaatamist käsitlevas dokumendis ([89]) on sätestatud vahistamisfotodega seotud erieeskirjad. Šotimaal on sõrmejälgede ja bioloogiliste proovide võtmise ja säilitamise eeskirjad sätestatud 1995. aasta kriminaalmenetluse seaduses ([90]). Nagu Inglismaal ja Walesiski reguleeritakse õigusaktiga biomeetriliste andmete säilitamist erinevatel juhtudel ([91]).

2.4.5. *Andmete turvalisus*

(51) Isikuandmeid tuleb töödelda viisil, mis tagab nende turvalisuse, sealhulgas kaitse loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahju eest. Sellel eesmärgil peavad avaliku sektori asutused võtma asjakohaseid tehnilisi ja korralduslikke meetmeid, et kaitsta isikuandmeid võimalike ohtude eest. Neid meetmeid tuleb hinnata, võttes arvesse tehnika taset ja seonduvaid kulusid.

(52) Neid põhimõtteid kajastatakse direktiivi (EL) 2016/680 artikli 4 lõike 1 punktiga f sarnaselt 2018. aasta andmekaitseseaduse paragrahvis 40, mille kohaselt tuleb isikuandmeid töödelda õiguskaitse eesmärkidel viisil, mis tagab isikuandmete asjakohase turvalisuse, ja kasutada tuleb asjakohaseid tehnilisi või korralduslikke meetmeid. See

([85]) Andmete säilitamise standardne töökord (Record Retention Standard Operating Procedure, SOP), kättesaadav aadressil https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Andmehalduse kohta lisateabe saamiseks vt Šotimaa riikliku registriga (National Records of Scotland) seotud teavet, mis on kättesaadav aadressil https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Säilitamistähtaeg oleneb sellest, kas isik on süüdi mõistetud või mitte (1984. aasta politsei- ja kriminaaltõendite seaduse (PACE) paragrahvid 63I–63KI). Näiteks kui täiskasvanu mõistetakse süüdi süüteos (*recordable offence*), võib tema sõrmejälgi ja DNA-profiili säilitada määramata aja jooksul (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahvi 63I lõige 2), kuid säilitamine on ajaliselt piiratud, kui süüdimõistetu on noorem kui 18-aastane, tegemist on väärteoga (*minor recordable offence*) ja isikut ei ole varem süüdi mõistetud (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahv 63K). Kui isik on vahistatud või talle on esitatud süüdistus, kuid teda ei ole süüdi mõistetud, võib andmeid säilitada kolm aastat (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahv 63F). Säilitamistähtaja pikendamiseks on vajalik õigusasutuse heakskiit (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahvi 63F lõige 7). Andmeid ei ole võimalik säilitada juhul, kui isik on vahistatud väärteo eest või talle on esitatud selle eest süüdistus, kuid teda ei ole väärteos süüdi mõistetud (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahvid 63D ja 63H).

([88]) Biomeetriavoliniku ametikoht loodi 2012. aasta vabaduste kaitse seaduse paragrahviga 20. Peale muude ülesannete täitmise otsustab biomeetriavolinik, kas politsei tohib säilitada selliste isikute DNA-profiilide andmeid ja sõrmejälgi, kes on vahistatud, kuid kellele ei ole esitatud kuriteo (*qualifying offence*) süüdistust (1984. aasta politsei- ja kriminaaltõendite seaduse paragrahv 63G). Biomeetriavolinikul on ka üldine kohustus jälgida DNA ja sõrmejälgede säilitamist ja kasutamist ning säilitamist riigi julgeoleku kaalutlustel (2012. aasta vabaduste kaitse seaduse paragrahvi 20 lõige 2). Biomeetriavolinik nimetatakse ametisse ametnike ametitesse nimetamise eeskirjade (Code for Public Appointments) kohaselt (eeskirjad on kättesaadavad aadressil Governance Code for Public Appointments - GOV.UK (www.gov.uk)) ning tema ametisse nimetamise tingimustes on selgelt sätestatud, et ametist tagandada saab teda ainult siseminister kitsalt kindlaks määratud asjaolude korral, nagu kohustuste täitmata jätmine kolme kuu jooksul, kuriteos süüdi mõistmine või ametisse nimetamise tingimuste rikkumine.

([89]) Vahistamisfotode kasutamise ja säilitamise läbivaatamist käsitlev dokument „Review of the Use and Retention of Custody Images“, kättesaadav aadressil https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Šotimaa 1995. aasta kriminaalmenetluse seaduse paragrahv 18 jj.

([91]) Säilitamistähtajad olenevad sellest, kas isik on süüdi mõistetud (Šotimaa 1995. aasta kriminaalmenetluse seaduse paragrahvi 18 lõige 3) või kas ta on alaealine. Viimasel juhul on säilitamistähtaeg kolm aastat alates lapse süüdimõistmisest kohtuistungil (Šotimaa 1995. aasta kriminaalmenetluse seaduse paragrahvi 18E lõige 8). Vahistatud, kuid süüdi mõistmata isikute andmeid ei tohi säilitada (Šotimaa 1995. aasta kriminaalmenetluse seaduse paragrahvi 18 lõige 3), välja arvatud erijuhtudel ja olenevalt süüteo raskusest (Šotimaa 1995. aasta kriminaalmenetluse seaduse paragrahv 18A). 2020. aasta Šotimaa biomeetriavoliniku seadusega (Scottish Biometrics Commissioner Act 2020) (vt https://www.legislation.gov.uk/asp/2020/8/contents) loodi Šotimaa biomeetriavoliniku ametikoht. Volinik peab koostama ja läbi vaatama tegevusjuhendid (mille on heaks kiitnud Šotimaa parlament) biomeetriliste andmete hankimise, säilitamise, kasutamise ja hävitamise kohta kriminaalõiguse ja politseitöö eesmärkidel (2020. aasta Šotimaa biomeetriavoliniku seaduse paragrahv 7).

hõlmab andmete kaitset loata või ebaseadusliku töötlemise ning juhusliku kaotsimineku, hävimise või kahju eest ([92]). 2018. aasta andmekaitseseaduse paragrahvis 66 on täpsustatud, et iga vastutav töötleja ja volitatud töötleja peab rakendama asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada isikuandmete töötlemisest tulenevatele riskidele vastaval tasemel turvalisus. Selgitavate märkuste kohaselt peab vastutav töötleja hindama riske ja rakendama sellel hinnangul põhinevaid asjakohaseid turvameetmeid, näiteks krüpteerimine või eri tasemete turvaload andmeid töötlevatele töötajatele ([93]). Hindamisel tuleb arvesse võtta ka näiteks töödeldavate andmete laadi ja muid asjakohaseid tegureid või asjaolusid, mis võivad mõjutada töötlemise turvalisust.

(53) Andmeturbe põhimõtete järgimise kord on väga sarnane direktiivi (EL) 2016/680 artiklitega 29–31 kehtestatud korraga. Vastutava töötleja vastutusalasse kuuluvate isikuandmetega seotud rikkumise korral peab vastutav töötleja 2018. aasta andmekaitseseaduse paragrahvi 67 lõike 1 kohaselt eelkõige teavitama teabevolinikku põhjendamatu viivituseta ja võimaluse korral 72 tunni jooksul pärast rikkumisest teada saamist ([94]). Teavitamiskohustust ei kohaldata, kui isikuandmete rikkumine ei ohusta tõenäoliselt isikute õigusi ega vabadusi ([95]). Vastutav töötleja peab dokumenteerima isikuandmete rikkumise asjaolud, rikkumise mõju ja võetud parandusmeetmed viisil, mis võimaldab teabevolinikul kontrollida andmekaitseseaduse järgimist ([96]). Kui volitatud töötleja saab teadlikuks turvarikkumisest, peab ta põhjendamatu viivituseta teavitama vastutavat töötlejat ([97]).

(54) 2018. aasta andmekaitseseaduse paragrahvi 68 lõikes 1 on sedastatud, et kui isikuandmetega seotud rikkumine põhjustab tõenäoliselt suurt ohtu isikute õigustele ja vabadustele, peab vastutav töötleja rikkumisest põhjendamatu viivituseta teavitama andmesubjekti ([98]). Teade peab sisaldama sama teavet nagu põhjenduses 53 kirjeldatud teavitus teabevolinikule. Kohustust ei kohaldata, kui vastutav töötleja on rakendanud asjakohaseid tehnilisi ja korralduslikke kaitsemeetmeid, mida kohaldati rikkumisest mõjutatud isikuandmetele. Seda ei kohaldata ka siis, kui vastutav töötleja on võtnud järelmeetmeid, mis tagavad, et andmesubjektide õigustele ja vabadustele ei ole enam tõenäoliselt suurt ohtu. Vastutav töötleja ei pea teavitama andmesubjekti, kui see eeldaks põhjendamatult suurt jõupingutust ([99]). Sellisel juhul tuleb teha teave andmesubjektile kättesaadavaks muul sama tõhusal viisil, näiteks avaliku teavitusvahendi kaudu ([100]). Kui vastutav töötleja ei ole andmesubjekti rikkumisest teavitanud, võib teabevolinik, keda on teavitatud andmekaitseseaduse paragrahvi 67 alusel ja kes on kaalunud rikkumise põhjustatava suure ohu tõenäosust, nõuda et vastutav töötleja teavitaks andmesubjekti rikkumisest ([101]).

([92]) Kooskõlas 2018. aasta andmekaitseseaduse selgitavate märkustega (vt joonealune märkus 45), peab vastutav töötleja eelkõige kavandama ja korraldama oma julgeolekut nii, et see vastaks tema valduses olevate isikuandmete laadile ja võimalikule turvarikkumisest tulenevale kahjule; määrama, kes tema organisatsioonis vastutab infoturbe tagamise eest; veenduma, et tal on õiged füüsilised ja tehnilised turvameetmed, mida toetavad ranged põhimõtted ja kord ja usaldusväärsed ja hästi koolitatud töötajad, ning olema valmis kiiresti ja tõhusalt reageerima turvarikkumistele.

([93]) 2018. aasta andmekaitseseaduse selgitavate märkuste punkt 221 (vt joonealune märkus 45).

([94]) 2018. aasta andmekaitseseaduse paragrahvi 67 lõikes 4 on ette nähtud, et teavitus peab hõlmama isikuandmetega seotud rikkumise laadi kirjeldust (sealhulgas võimaluse korral asjaomaste andmesubjektide kategooriad ja ligikaudne arv ning asjakohaste isikuandmete kirjete kategooriad ja ligikaudne arv), kontaktasutuse nime ja kontaktandmeid, isikuandmetega seotud rikkumise tõenäoliste tagajärgede kirjeldust ning isikuandmetega seotud rikkumise kõrvaldamiseks vastutava töötleja võetud või kavandatud meetmete kirjeldust (sealhulgas asjakohasel juhul rikkumise võimaliku negatiivse mõju leevendamise meetmed).

([95]) 2018. aasta andmekaitseseaduse paragrahvi 67 lõige 2.

([96]) 2018. aasta andmekaitseseaduse paragrahvi 67 lõige 6.

([97]) 2018. aasta andmekaitseseaduse paragrahvi 67 lõige 9.

([98]) 2018. aasta andmekaitseseaduse paragrahvi 68 lõike 7 alusel võib vastutav töötleja piirata täielikult või osaliselt teabe andmist andmesubjektile sellises ulatuses ja seni, kuni piirang on andmesubjekti põhiõiguste ja õigustatud huvi seisukohast vajalik ja proportsionaalne meede a) ametliku või õigusliku päringu, uurimise või menetluse takistamise vältimiseks; b) süütegude tõkestamise, avastamise, uurimise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise kahjustamise vältimiseks; c) avaliku julgeoleku kaitseks; d) riigi julgeoleku kaitseks; e) teiste isikute õiguste ja vabaduste kaitseks.

([99]) 2018. aasta andmekaitseseaduse paragrahvi 68 lõige 3.

([100]) 2018. aasta andmekaitseseaduse paragrahvi 68 lõige 5.

([101]) 2018. aasta andmekaitseseaduse paragrahvi 68 lõige 6 vastavalt 2018. aasta andmekaitseseaduse paragrahvi 68 lõikes 8 ette nähtud piirangule.

2.4.6. *Läbipaistvus*

(55) Andmesubjekte tuleb teavitada nende isikuandmete töötlemise põhitunnustest. Seda andmekaitsepõhimõtet kajastatakse 2018. aasta andmekaitseseaduse paragrahvis 44, milles on sarnaselt direktiivi (EL) 2016/680 artiklile 13 ette nähtud, et vastutaval töötlejal on üldine kohustus teha andmesubjektidele kättesaadavaks teave nende isikuandmete töötlemise kohta (tehes teabe üldsusele kättesaadavaks või muul viisil) ([102]). Teave, mis tuleb teha kättesaadavaks, on a) vastutava töötleja nimi ja kontaktandmed; b) kui kohaldatav, siis andmekaitseametniku kontaktandmed; c) vastutava töötleja eesmärgid isikuandmete töötlemisel; d) andmesubjektide õigused taotleda vastutavalt töötlejalt isikuandmetega tutvumist, isikuandmete parandamist ja isikuandmete kustutamist või nende töötlemise piiramist ning e) õigus esitada kaebus teabevolinikule ja voliniku kontaktandmed ([103]).

(56) Lisaks peab vastutav töötleja erijuhtudel (nt kui töödeldavad isikuandmed koguti andmesubjekti teadmata) andma 2018. aasta andmekaitseseadusest tulenevate andmesubjekti õiguste teostamise võimaldamiseks andmesubjektile a) teavet töötlemise õigusliku aluse kohta; b) teavet isikuandmete säilitamise tähtaja kohta või, kui see ei ole võimalik, siis kõnealuse tähtaja määramise kriteeriumite kohta; c) asjakohasel juhul teavet isikuandmete vastuvõtjate kategooriate kohta (sealhulgas kolmandates riikides või rahvusvahelistes organisatsioonides); d) sellist lisateavet, mis on vajalik, et võimaldada andmesubjektil teostada 2018. aasta andmekaitseseaduse 3. osast tulenevaid õigusi ([104]).

2.4.7. *Üksikisiku õigused*

(57) Andmesubjektidele tuleb anda kohtulikult kaitstavad õigused. 2018. aasta andmekaitseseaduse 3. osa 3. peatükis on üksikisikutele ette nähtud õigus tutvuda andmetega, andmete parandamise õigus, andmete kustutamise õigus ning andmete töötlemise piiramise õigus, ([105]) mis on võrreldavad direktiivi (EL) 2016/680 III peatükis ette nähtud õigustega.

(58) Õigus tutvuda andmetega on sätestatud 2018. aasta andmekaitseseaduse paragrahvis 45. Esiteks on üksikisikul õigus saada vastutavalt töötlejalt kinnitus selle kohta, kas tema isikuandmeid töödeldakse või mitte ([106]). Kui isikuandmeid töödeldakse, siis teiseks on andmesubjektil õigus nende andmetega tutvuda ja saada töötlemise kohta järgmist teavet: a) töötlemise eesmärgid ja õiguslikud alused; b) asjakohaste andmete liigid; c) vastuvõtja, kellele andmeid on avalikustatud; d) isikuandmete säilitamise tähtaeg; e) andmesubjekti õigus isikuandmete parandamisele ja kustutamisele; f) õigus esitada kaebus ning g) asjakohaste isikuandmete päritolu ([107]).

(59) 2018. aasta andmekaitseseaduse paragrahvi 46 kohaselt on andmesubjektil õigus nõuda, et vastutav töötleja parandaks temaga seotud ebaõigeid isikuandmeid. Vastutav töötleja peab andmeid parandama (või täiendama ebatäielikke ja seega ebaõigeid andmeid) põhjendamatu viivituseta. Kui isikuandmeid tuleb säilitada tõendamise eesmärgil, peab vastutav töötleja piirama nende töötlemist (mitte isikuandmeid parandama) ([108]).

([102]) Õiguskaitse eesmärgil andmete töötlemise juhendis on esitatud järgmine näide: „Teie veebisaidil on üldine isikuandmete kaitse teade, mis puudutab põhiteavet organisatsiooni kohta, isikuandmete töötlemise eesmärki, andmesubjekti õigusi ja tema õigust esitada kaebus teabevolinikule. Olete saanud teavet, et ühe süüteo toimepanemise juures viibis keegi. Selle isiku esmakordsel küsitlemisel peate andma üldist teavet ja lisateavet, et võimaldada tal teostada oma õigusi. Võite piirata õiglase andmete töötlemise teabe andmist vaid siis, kui see kahjustab teie läbiviidavat uurimist." (õiguskaitse eesmärgil andmete töötlemise juhend, „Isikutele antav teave" („What information should we supply to an individual?"), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Õiguskaitse eesmärgil andmete töötlemise juhendis on sedastatud, et isikuandmete töötlemise kohta jagatav teave peab olema täpne, arusaadav ja kergesti kättesaadav, kirjutatud selges ja lihtsas keeles, kohandatud haavatavate isikute, näiteks laste vajadustega ning tasuta (õiguskaitse eesmärgil andmete töötlemise juhend, „Teabe jagamise viisid" („How should we provide this information?"), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) 2018. aasta andmekaitseseaduse paragrahvi 44 lõige 2.

([105]) Andmesubjekti õiguste üksikasjalik analüüs vt õiguskaitse eesmärgil andmete töötlemise juhend, „Üksikisiku õigused" („Individual rights"), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) 2018. aasta andmekaitseseaduse paragrahvi 45 lõige 1.

([107]) 2018. aasta andmekaitseseaduse paragrahvi 45 lõige 2.

([108]) 2018. aasta andmekaitseseaduse paragrahvi 46 lõige 4.

(60) 2018. aasta andmekaitseseaduse paragrahvis 47 on üksikisikutele ette nähtud andmete kustutamise õigus ja õigus piirata andmete töötlemist. Vastutav töötleja peab ([109]) kustutama isikuandmed põhjendamatu viivituseta, kui isikuandmete töötlemine oleks vastuolus andmekaitsepõhimõtetega, andmete töötlemise õiguslike alustega või arhiveerimise ja tundlike andmete töötlemisega seotud kaitsemeetmetega. Vastutav töötleja peab andmed kustutama ka juhul, kui tal on juriidiline kohustus seda teha. Kui isikuandmeid tuleb säilitada tõendamise eesmärgil, peab vastutav töötleja piirama nende töötlemist (mitte isikuandmeid kustutama) ([110]). Vastutav töötleja peab piirama isikuandmete töötlemist, kui andmesubjekt vaidlustab isikuandmete õigsuse, kuid ei ole võimalik kindlaks teha, kas andmed on õiged või mitte ([111]).

(61) Kui andmesubjekt taotleb isikuandmete parandamist või kustutamist või nende töötlemise piiramist, peab vastutav töötleja teavitama andmesubjekti kirjalikult sellest, kas taotlus on rahuldatud. Kui taotluse rahuldamisest on keeldutud, peab vastutav töötleja teavitama andmesubjekti keeldumise põhjustest ja õiguskaitsevõimalustest (andmesubjekti õigus taotleda teabevolinikult piirangu kohaldamise seaduslikkuse uurimist, õigus esitada teabevolinikule kaebus ja õigus taotleda kohtult täitmiskorraldust) ([112]).

(62) Kui vastutav töötleja parandab teiselt pädevalt asutuselt saadud isikuandmeid, peab ta teist asutust teavitama ([113]). Kui vastutav töötleja parandab või kustutab vastutava töötleja avaldatud isikuandmeid või piirab nende töötlemist, peab vastutav töötleja teavitama andmete vastuvõtjaid ning vastuvõtjad peavad samuti isikuandmeid parandama või kustutama või piirama nende töötlemist (sedavõrd kui nad nende eest vastutavad) ([114]).

(63) Andmesubjektil on ka õigus saada vastutavalt töötlejalt põhjendamatu viivituseta teada isikuandmetega seotud rikkumisest, kui see toob tõenäoliselt kaasa suure ohu isikute õigustele ja vabadustele ([115]).

(64) Seoses kõigi nende andmesubjekti õigustega ja sarnaselt direktiivi (EL) 2016/680 artiklis 12 ette nähtuga on vastutaval töötlejal kohustus tagada, et andmesubjektile antav teave esitatakse täpses, arusaadavas ja kergesti kättesaadavas vormis ([116]) ning võimaluse korral tuleks see esitada taotlusega samas vormis ([117]). Vastutav töötleja peab rahuldama andmesubjekti taotluse põhjendamatu viivituseta või igal juhul põhimõtteliselt enne ühe kuu möödumist taotluse esitamisest ([118]). Kui vastutaval töötlejal on mõistlik alus kahelda isiku isikusamasuses, võib ta nõuda lisateavet ja oodata taotluse rahuldamisega kuni isikusamasuse kinnitamiseni. Kui vastutav töötleja peab taotlust ilmselgelt põhjendamatuks, võib ta küsida mõistlikku tasu või keelduda tegutsemast ([119]). Teabevoliniku büroo on esitanud suunised selle kohta, millal peetakse taotlust ilmselgelt põhjendamatuks või ülemääraseks ja millal võib küsida tasu ([120]).

(65) 2018. aasta andmekaitseseaduse paragrahvi 53 lõike 4 alusel võib minister kehtestada määruses tasu maksimaalse summa.

([109]) Andmesubjekt võib taotleda, et vastutav töötleja kustutaks isikuandmed või piiraks nende töötlemist (kuid vastutaval töötlejal on kohustus kustutada andmed või piirata nende töötlemist hoolimata sellest, kas selline nõue on esitatud).

([110]) 2018. aasta andmekaitseseaduse paragrahvi 46 lõige 4 ja paragrahvi 47 lõige 2.

([111]) 2018. aasta andmekaitseseaduse paragrahvi 47 lõige 3.

([112]) 2018. aasta andmekaitseseaduse paragrahvi 48 lõige 1.

([113]) 2018. aasta andmekaitseseaduse paragrahvi 48 lõige 7.

([114]) 2018. aasta andmekaitseseaduse paragrahvi 48 lõige 9.

([115]) 2018. aasta andmekaitseseaduse paragrahv 68.

([116]) 2018. aasta andmekaitseseaduse paragrahvi 52 lõige 1.

([117]) 2018. aasta andmekaitseseaduse paragrahvi 52 lõige 3.

([118]) 2018. aasta andmekaitseseaduse paragrahvis 54 on määratletud mõiste „kohaldatav ajavahemik“ kui ühekuuline ajavahemik või õigusaktides sätestatud pikem ajavahemik, mis algab asjakohasel ajal, kui vastutav töötleja saab kõnealuse taotluse; kui vastutav töötleja saab andmekaitseseaduse paragrahvi 52 lõike 4 kohase taotluse kohta küsitud teabe (kui asjakohane) või kui makstakse andmekaitseseaduse paragrahvi 53 kohase taotlusega seoses võetav tasu (kui asjakohane).

([119]) 2018. aasta andmekaitseseaduse paragrahvi 53 lõige 1.

([120]) Teabevoliniku büroo suuniste kohaselt võib vastutav töötleja otsustada võtta andmesubjektilt tasu, kui viimase taotlus on ilmselgelt põhjendamatu või ülemäärane, kuid vastutav töötleja otsustab sellele siiski vastata. Tasu peab olema mõistlik ja vastama põhjendatud kuludele. Õiguskaitse eesmärgil andmete töötlemise juhend, „Ilmselgelt põhjendamatud ja ülemäärased taotlused“ („Manifestly unfounded and excessive requests“), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

2.4.7.1. Andmesubjekti õiguste piirangud ja läbipaistvuskohustused

(66) Teatud tingimustel võib pädev asutus piirata andmesubjekti teatavaid õigusi: õigus tutvuda isikuandmetega, ([121]) õigus olla teavitatud, ([122]) õigus saada teada isikuandmetega seotud rikkumistest ([123]) ja õigus olla teavitatud andmete parandamise või kustutamise taotluse rahuldamisest keeldumise põhjusest ([124]). Sarnaselt direktiivi (EL) 2016/680 III peatükis esitatud korraga võib pädev asutus kohaldada piirangut vaid siis, kui see on andmesubjekti põhiõigusi ja õigustatud huve arvestades vajalik ja proportsionaalne a) ametliku või õigusliku päringu, uurimise või menetluse takistamise vältimiseks; b) süütegude tõkestamise, avastamise, uurimise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise kahjustamise vältimiseks; c) avaliku julgeoleku kaitseks; d) riigi julgeoleku kaitseks; e) teiste isikute õiguste ja vabaduste kaitseks.

(67) Teabevoliniku büroo on esitanud nende piirangute kohaldamise suunised. Nende suuniste kohaselt peavad vastutavad töötlejad analüüsima iga juhtumit, et leida õige tasakaal üksikisiku õiguste ja avalikustamisest tuleneva kahju vahel. Eelkõige peavad nad põhjendama kohaldatud piirangu vajalikkust ja proportsionaalsust ning võivad piirata andmete esitamist vaid siis, kui nende esitamine seaks ohtu eespool nimetatud eesmärgid ([125]).

(68) Ka mitmes muus pädevate asutuste avaldatud suunises antakse üksikasjalikku teavet andmekaitsealaste õigusaktide kõigi aspektide kohta, sealhulgas andmesubjektide õiguste piirangute kohta ([126]). Näiteks seoses paragrahvi 45 lõikega 4 märgitakse riikliku kõrgemate politseiametnike nõukogu andmekaitse käsiraamatus järgmist: „Tuleb meeles pidada, et piiranguid tohib kohaldada vaid vajalikul määral ja vajaliku aja jooksul. Järelikult ei ole lubatud kohaldada piirangut üldiselt kõigile taotleja isikuandmetele ega kohaldada piirangut püsivalt. Viimase küsimuse puhul on sageli nii, et uurimises kahtlusaluseks oleva andmesubjekti teadmata kogutud isikuandmeid tuleb alguses kaitsta andmesubjektile avaldamise eest, et vältida uurimise kahjustamist uurimise ajal, kuid hiljem isikule küsitluse käigus isikuandmete avaldamine ei oleks kahjulik. Politseijõud peavad võtma kasutusele protsessid, mis tagavad, et neid piiranguid kohaldatakse ainult vajalikus ulatuses ja vajaliku aja jooksul“ ([127]). Nendes suunistes esitatakse ka näiteid selle kohta, millal iga piirangut tõenäoliselt kasutatakse ([128]).

(69) Seoses võimalusega piirata eespool nimetatud õigusi „riigi julgeoleku kaitseks“, võib vastutav töötleja taotleda sertifikaati, mille allkirjastab kabinetiminister või peaprokurör (Attorney General) (või valitsuse nõunik Šotimaa õiguse alal) ja mis kinnitab, et selliste õiguste piiramine on vajalik ja proportsionaalne meede riigi julgeoleku kaitsmiseks ([129]). Ühendkuningriigi valitsus on esitanud 2018. aasta andmekaitseseaduse alusel suunised riigi julgeoleku sertifikaatide kohta, milles eelkõige toonitatakse, et andmesubjektide õiguste piiramine riigi julgeoleku kaitsmise nimel peab olema proportsionaalne ja vajalik ([130]) (lisateave riigi julgeoleku sertifikaatide kohta on esitatud põhjendustes 131–134).

([121]) 2018. aasta andmekaitseseaduse paragrahvi 45 lõige 4.
([122]) 2018. aasta andmekaitseseaduse paragrahvi 44 lõige 4.
([123]) 2018. aasta andmekaitseseaduse paragrahvi 68 lõige 7.
([124]) 2018. aasta andmekaitseseaduse paragrahvi 48 lõige 3.
([125]) Vt näiteks õiguskaitse eesmärgil andmete töötlemise juhend, „Andmetega tutvumise õigus“ („The right of access“), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Vt näiteks riikliku kõrgemate politseiametnike nõukogu andmekaitse käsiraamat politsei andmekaitsespetsialistidele (vt joonealune märkus 27) või raskete pettuste ameti suunised, kättesaadavad aadressil https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Riikliku kõrgemate politseiametnike nõukogu andmekaitse käsiraamat, lk 140 (vt joonealune märkus 27).
([128]) Riikliku kõrgemate politseiametnike nõukogu andmekaitse käsiraamatus on märgitud, et „ametliku või õigusliku päringu, uurimise või menetluse takistamise vältimiseks“ on tõenäoliselt asjakohane isikuandmete puhul, mida töödeldakse seoses uurimiste, perekonnaasjade kohtu menetluste, kuritegevusega mitteseotud sisediskipliinijuurdluste ja selliste juurdlustega nagu laste seksuaalse kuritarvitamise sõltumatu juurdlus (Independent Inquiry into Child Sexual Abuse); „teiste isikute õiguste ja vabaduste kaitseks“ on aga seotud isikuandmetega, mis puudutavad lisaks taotlejale ka teisi isikuid (riikliku kõrgemate politseiametnike nõukogu andmekaitse käsiraamat, lk 140, vt joonealune märkus 27).
([129]) 2018. aasta andmekaitseseaduse paragrahv 79.
([130]) Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta (UK Government Guidance on National Security Certificates), 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.

(70) Kui andmesubjekti õigust piiratakse, peab pädev asutus teavitama andmesubjekti põhjendamatu viivituseta sellest, et tema õigusi on piiratud, piiramise põhjustest ja õiguskaitse võimalustest, välja arvatud juhul, kui selle teabe esitamine oleks vastuolus piirangu kohaldamise põhjusega ([131]). Piirangute kuritarvitamise vastase täiendava kaitsemeetmena peab vastutav töötleja dokumenteerima teabe piiramise põhjused ja tegema need teabevolinikule tema nõudmisel kättesaadavaks ([132]).

(71) Kui vastutav töötleja keeldub andmast täiendavat läbipaistvusalast teavet või võimalust andmetega tutvuda või rahuldamast andmete parandamise või kustutamise või töötlemise piiramise taotlust, võib isik taotleda, et teabevolinik uuriks, kas vastutav töötleja on kasutanud piirangut seaduslikult ([133]). Asjaomane isik võib ka esitada kaebuse teabevolinikule või paluda kohtul nõuda vastutavalt töötlejalt taotluse rahuldamist ([134]).

2.4.7.2. Automatiseeritud töötlusel põhinevate otsuste tegemine

(72) 2018. aasta andmekaitseseaduse paragrahvid 49 ja 50 hõlmavad vastavalt automatiseeritud töötlusel põhinevate otsuste tegemisega seotud õigusi ja kohaldatavaid kaitsemeetmeid ([135]). Sarnaselt direktiivi (EL) 2016/680 artikliga 11 võib vastutav töötleja teha ainult isikuandmete automatiseeritud töötlusel põhineva kaaluka otsuse vaid juhul, kui seda nõuab või lubab seadus ([136]). Otsus on kaalukas, kui see tekitaks andmesubjektiga seoses kahjuliku õigusliku mõju või kahjustaks andmesubjekti märkimisväärselt ([137]).

(73) 2018. aasta andmekaitseseaduse paragrahvis 50 on sätestatud kaitsemeetmed, mida kohaldatakse kaaluka otsuse suhtes, kui seadus nõuab või lubab, et vastutav töötleja teeks sellise otsuse (*qualifying significant decision*). Vastutav töötleja peab nii kiiresti kui mõistlikult võimalik teatama andmesubjektile, et selline otsus on tehtud. Seejärel võib andmesubjekt ühe kuu jooksul taotleda, et vastutav töötleja vaataks otsuse uuesti läbi või teeks uue otsuse, mis ei põhine ainult automatiseeritud töötlemisel. Vastutav töötleja peab taotlust kaaluma ja teavitama andmesubjekti selle kaalumise tulemusest. 2018. aasta andmekaitseseadusega volitatakse ministrit vastu võtma määrust täiendavate kaitsemeetmete kohta ([138]). Sellist määrust ei ole veel vastu võetud.

2.4.8. *Andmete edasisaatmine*

(74) Liikmesriigi õiguskaitseasutustelt Ühendkuningriigi õiguskaitseasutusele edastatavatele isikuandmetele pakutava kaitse taset ei tohi vähendada selliste andmete edasisaatmine kolmanda riigi vastuvõtjale. Sellist edasisaatmist, mis tähendab Ühendkuningriigi õiguskaitseasutuse seisukohast rahvusvahelist edastamist Ühendkuningriigist, tuleks lubada üksnes juhul, kui järgmine saaja väljaspool Ühendkuningriiki järgib ise eeskirju, mis tagavad sarnase kaitse kui see, mis on tagatud Ühendkuningriigi õiguskorraga.

([131]) 2018. aasta andmekaitseseaduse paragrahvi 44 lõiked 5 ja 6, paragrahvi 45 lõiked 5 ja 6 ning paragrahvi 48 lõige 4.

([132]) 2018. aasta andmekaitseseaduse paragrahvi 44 lõige 7, paragrahvi 45 lõige 7 ja paragrahvi 48 lõige 6.

([133]) 2018. aasta andmekaitseseaduse paragrahv 51.

([134]) 2018. aasta andmekaitseseaduse paragrahv 167.

([135]) Automatiseeritud töötluse ulatuse kohta märgitakse 2018. aasta andmekaitseseaduse selgitavates märkustes, et „need sätted on seotud täielikult automatiseeritud otsuste tegemisega, mitte automatiseeritud töötlemisega. Automatiseeritud töötlemisega (sealhulgas profiilianalüüs) on tegemist siis, kui andmetega tehtavatesse toimingutesse ei pea sekkuma inimesed. Seda kasutatakse sageli õiguskaitses, et filtreerida suuri andmekogumeid hallatavateks osadeks, mida saavad kasutada inimesed. Automatiseeritud töötlusel põhinevate otsuste tegemine on automatiseeritud töötlemise vorm ja tähendab, et lõplik otsus tehakse ilma inimeste sekkumiseta.“ (Andmekaitseseaduse selgitavad märkused, punkt 204, vt joonealune märkus 45).

([136]) Lisaks andmekaitseseadusega ettenähtud kaitsele on Ühendkuningriigi õigusraamistikus sätestatud muud õiguskaitseasutuste suhtes kohaldatavad õiguslikud piirangud, mis takistaksid automatiseeritud töötlust (sealhulgas profiilianalüüsi), mille tulemuseks on ebaseaduslik diskrimineerimine. 1998. aasta inimõiguste seadusega inkorporeeritakse Ühendkuningriigi õigusesse õigused, mis on tagatud Euroopa inimõiguste konventsiooniga, sealhulgas konventsiooni artikliga 14, kus on sätestatud diskrimineerimiskeeld. Samuti keelatakse 2010. aasta võrdõiguslikkuse seadusega diskrimineerida kaitstud tunnustega (nende hulka kuuluvad sugu, rass, puue jne) inimesi.

([137]) 2018. aasta andmekaitseseaduse paragrahvi 49 lõige 2.

([138]) 2018. aasta andmekaitseseaduse paragrahvi 50 lõige 4.

(75) Ühendkuningriigi andmete rahvusvahelise edastamise korda reguleeritakse 2018. aasta andmekaitseseaduse 3. osa 5. peatükiga ([139]) ja see sarnaneb direktiivi (EL) 2016/680 V peatükis kasutatud lähenemisviisile. Nimelt peab pädev asutus isikuandmete edastamiseks kolmandale riigile täitma kolm tingimust: a) edastamine peab olema vajalik õiguskaitse eesmärgil; b) edastamine peab põhinema i) kolmandat riiki käsitleval kaitse piisavuse määrusel; ii) kui see ei põhine kaitse piisavuse määrusel, peavad olema võetud asjakohased kaitsemeetmed, või iii) kui see ei põhine kaitse piisavuse otsusel või asjakohastel kaitsemeetmetel, peab see põhinema erilistel asjaoludel ning c) edastatavate andmete saaja peab olema i) kolmanda riigi asjaomane asutus (st pädeva asutusega samaväärne asutus); ii) „asjaomane rahvusvaheline organisatsioon“, näiteks rahvusvaheline organ, mis täidab õiguskaitse eesmärkidele vastavaid ülesandeid, või iii) muu isik kui asjaomane asutus, kuid ainult juhul, kui edastamine on rangelt vajalik õiguskaitse eesmärgi täitmiseks; ükski asjaomase andmesubjekti põhiõigus ega -vabadus ei kaalu üles avalikku huvi, mis teeb edastamise vajalikuks; isikuandmete edastamine kolmandas riigis asuvale asjaomasele asutusele ei oleks tõhus või kohane ning andmete saajat teavitatakse eesmärkidest, mille tarvis andmeid võidakse töödelda ([140]).

(76) Minister võtab vastu kaitse piisavuse määruse seoses kolmanda riigiga, kolmanda riigi territooriumi või sektoriga või rahvusvahelise organisatsiooniga või sellise riigi, territooriumi, sektori või organisatsiooni kirjelduse ([141]). Täidetavate nõuetega seoses peab minister hindama, kas selline territoorium/sektor/organisatsioon tagab isikuandmete kaitse piisava taseme. 2018. aasta andmekaitseseaduse paragrahvi 74A lõikes 4 on märgitud, et selleks peab minister kaaluma mitut aspekti, mis sarnanevad direktiivi (EL) 2016/680 artiklis 36 loetletud elementidega ([142]). Pärast üleminekuperioodi lõppu sai 2018. aasta andmekaitseseaduse 3. osast ELi õigusel põhinev siseriiklik õigusakt, mida, nagu selgitatud, tõlgendavad Ühendkuningriigi kohtud kooskõlas Euroopa Kohtu asjakohase praktikaga, mis pärineb ajast enne Ühendkuningriigi lahkumist liidust, ja kooskõlas liidu õiguse üldiste põhimõtetega, mis kehtisid vahetult enne üleminekuperioodi lõppu. See hõlmab sisulise vastavuse standardit, mida kohaldatakse Ühendkuningriigi ametiasutuste tehtavatele kaitse piisavuse hindamistele.

(77) Määruse suhtes kohaldatakse 2018. aasta andmekaitseseaduse paragrahvis 182 ette nähtud üldisi menetlusnõudeid. Kui minister kavatseb teha tulevikus Ühendkuningriigi kaitse piisavuse määruse ettepaneku, peab ta selle menetluse

([139]) Seda uut raamistikku, sealhulgas ministri volitust anda välja kaitse piisavuse määrus, kohaldatakse alates üleminekuperioodi lõpust. Andmekaitse, eraelu puutumatuse ja elektroonilise side määruses (eriti 21. lisa punktides 10–12, mis lisatakse selle määrusega 2018. aasta andmekaitseseadusesse) on aga ette nähtud, et teatavat isikuandmete edastamist üleminekuperioodil ja pärast selle lõppu käsitletakse nii, nagu see põhineks kaitse piisavuse määrusel. Selline edastamine hõlmab edastamist kolmandatele riikidele, mille suhtes kohaldatakse üleminekuperioodi lõpus ELi kaitse piisavuse otsust, ning ELi liikmesriikidele, EFTA riikidele ja Gibraltari territooriumile, sest nad kohaldavad õiguskaitsega seotud andmete töötlemisele õiguskaitsedirektiivi (EFTA riigid kohaldavad direktiivi (EL) 2016/680 tulenevalt nende kohustustest Schengeni *acquis*' raames). See tähendab, et üleminekuperioodi lõpus võib edastamine nendesse riikidesse jätkuda nagu enne EList väljaastumist. Pärast üleminekuperioodi lõppu peab minister vaatama kaitse piisavuse otsused läbi nelja aasta jooksul.

([140]) 2018. aasta andmekaitseseaduse paragrahvid 73 ja 77.

([141]) Ühendkuningriigi ametiasutused on selgitanud, et riigi või rahvusvahelise organisatsiooni kirjeldust kasutatakse olukorras, kus on vaja piisavus konkreetselt ja osaliselt kindlaks määrata, kohaldades sihipäraseid piiranguid (näiteks kaitse piisavuse määrus seoses ainult teatavat liiki andmete edastamisega).

([142]) Vt 2018. aasta andmekaitseseaduse paragrahvi 74A lõige 4, milles on ette nähtud, et isikuandmete kaitse taseme piisavuse hindamisel peab minister eelkõige arvesse võtma järgmisi asjaolusid: „a) õigusriigi põhimõte, inimõiguste ja põhivabaduste austamine, asjaomased õigusaktid, nii üldised kui ka valdkondlikud, sealhulgas õigusaktid, mis käsitlevad avalikku julgeolekut, riigikaitset, riigi julgeolekut, kriminaalõigust ja riigiasutuste juurdepääsu isikuandmetele, ning kõnealuste õigusaktide, andmekaitsenormide, ametieeskirjade ja turvameetmete (sealhulgas eeskirjad isikuandmete edasisaatmise kohta teisele kolmandale riigile või rahvusvahelisele organisatsioonile, mida kõnealune kolmas riik või rahvusvaheline organisatsioon täidab) rakendamine, kohtupraktika ning tõhusate ja kohtulikult kaitstavate õiguste ja tõhusa haldus- ja õiguskaitse olemasolu andmesubjektide jaoks, kelle isikuandmeid edastatakse; b) ühe või mitme sellise sõltumatu järelevalveasutuse olemasolu ja tõhus toimimine asjaomases kolmandas riigis või kellele rahvusvaheline organisatsioon allub, kes vastutab andmekaitsenormide järgimise ja täitmise tagamise eest, sealhulgas piisavate täidesaatvate volituste eest, ning andmesubjektide abistamise ja nõustamise eest nende õiguste teostamisel ning volinikuga tehtava koostöö eest, ja c) asjaomase kolmanda riigi või rahvusvahelise organisatsiooni rahvusvahelised kohustused või muud kohustused, mis tulenevad õiguslikult siduvatest konventsioonidest või õigusaktidest või kõnealuse kolmanda riigi või rahvusvahelise organisatsiooni osalemisest mitmepoolsetes või piirkondlikes süsteemides, eelkõige seoses isikuandmete kaitsega“.

raames konsulteerima teabevolinikuga ([143]). Kui minister on määruse vastu võtnud, esitatakse see parlamendile negatiivse resolutsiooni menetluse (*negative resolution procedure*) raames, mille alusel võivad mõlemad parlamendikojad määrust kontrollida ja neil on õigus võtta vastu ettepanek määrus 40-päevase ajavahemiku jooksul tühistada ([144]).

(78) 2018. aasta andmekaitseseaduse paragrahvi 74B lõike 1 kohaselt tuleb kaitse piisavuse määrus läbi vaadata vähemalt iga nelja aasta järel ja minister peab järjepidevalt jälgima suundumusi sellistes kolmandates riikides ja rahvusvahelistes organisatsioonides, mis võivad mõjutada kaitse piisavuse määruse koostamise, muutmise või tühistamise otsuseid. Kui minister saab teada, et mõni riik või organisatsioon ei taga enam isikuandmete kaitse piisavat taset, peab ta määrust vajalikus ulatuses muutma või selle tühistama ja alustama asjaomase kolmanda riigi või rahvusvahelise organisatsiooniga konsultatsioone piisava kaitsetaseme taastamiseks.

(79) Sarnaselt direktiivi (EL) 2016/680 artiklis 37 ette nähtuga on kaitse piisavuse määruse puudumise korral isikuandmete edastamine õiguskaitse kontekstis võimalik, kui on võetud asjakohased kaitsemeetmed. Sellised kaitsemeetmed tagatakse kas a) õiguslikult siduva aktiga, mis sisaldab isikuandmete kaitseks võetud asjakohaseid kaitsemeetmeid, või b) hindamisega, mille viib läbi vastutav töötleja, kes pärast kõikide isikuandmete edastamisega seotud asjaolude hindamist järeldab, et võetud on andmete kaitseks asjakohased kaitsemeetmed ([145]). 2018. aasta andmekaitseseaduses on ette nähtud, et kui isikuandmete edastamine põhineb asjakohastel kaitsemeetmetel, siis lisaks teabevoliniku büroo tavapärasele järelevalvele peavad pädevad asutused esitama teabevoliniku büroole andmete edastamise kohta konkreetse teabe ([146]).

(80) Kui andmete edastamine ei põhine kaitse piisavuse otsusel ega asjakohastel kaitsemeetmetel, võib see toimuda ainult teatavatel kindlaksmääratud asjaoludel, millele viidatakse kui erilistele asjaoludele ([147]). Asjaolud on erilised, kui edastamine on vajalik a) andmesubjekti või teise isiku eluliste huvide kaitsmiseks; b) andmesubjekti õigustatud huvide kaitsmiseks; c) kolmanda riigi avalikku julgeolekut ähvardava vahetu ja tõsise ohu ennetamiseks; d) üksikjuhtumite korral õiguskaitse eesmärkidel või e) üksikjuhtumite korral õiguslikul eesmärgil (näiteks seoses kohtumenetlustega või õigusliku nõu saamiseks) ([148]). Punkte d ja e ei kohaldata, kui andmesubjekti õigused ja vabadused kaaluvad üles avaliku huvi andmete edastamiseks ([149]). Need asjaolud vastavad eriolukordadele ja tingimustele, mis on direktiivi (EL) 2016/680 artiklis 38 liigitatud eranditeks.

(81) Selliste asjaolude esinemise korral tuleb dokumenteerida edastamise kuupäev, kellaaeg ja selgitus, vastuvõtja nimi ja muu asjakohane teave tema kohta ja edastatud isikuandmete kirjeldus ning esitada taotluse korral teabevolinikule ([150]).

(82) 2018. aasta andmekaitseseaduse paragrahviga 78 reguleeritakse andmete edasisaatmist ehk olukordi, kui Ühendkuningriigilt kolmandale riigile edastatud isikuandmed saadetakse hiljem edasi muule kolmandale riigile või rahvusvahelisele organisatsioonile. Paragrahvi 78 lõike 1 kohaselt peab andmeid edastav Ühendkuningriigi vastutav töötleja kehtestama edastamise tingimusena, et andmeid ei tohi kolmandale riigile edasi saata ilma andmeid edastava vastutava töötleja loata. Lisaks kohaldatakse juhul, kui nõutakse kõnealust luba, paragrahvi 78 lõike 3 kohaselt ja sarnaselt direktiivi (EL) 2016/680 artikli 35 lõike 1 punktis e sätestatuga mitut sisulist nõuet. Kui pädev

([143]) Vt digi-, kultuuri-, meedia- ja spordiministri ning teabevoliniku büroo vaheline vastastikuse mõistmise memorandum teabevoliniku büroo osa kohta seoses Ühendkuningriigi kaitse piisavuse uue hindamisega https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Selle 40-päevase ajavahemiku jooksul on mõlemal parlamendikojal võimalus hääletada määruse vastu; kui määruse vastu antakse piisavalt hääli, ei ole määrusel enam õiguslikku mõju.

([145]) 2018. aasta andmekaitseseaduse paragrahv 75.

([146]) Kui andmete edastamisel tuginetakse asjakohastele kaitsemeetmetele, siis tuleb 2018. aasta andmekaitseseaduse paragrahvi 75 lõike 3 kohaselt a) edastamine dokumenteerida, b) dokumendid tuleb esitada taotluse korral volinikule ja c) dokumendid peavad sisaldama eelkõige i) edastamise kuupäeva ja kellaaega, ii) vastuvõtja nime ja muud asjakohast teavet tema kohta, iii) edastamise selgitust ning iv) edastatud isikuandmete kirjeldust.

([147]) Õiguskaitse eesmärgil andmete töötlemise juhend, „Erilised asjaolud“ („Are there any special circumstances?“), kättesaadav aadressil https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) 2018. aasta andmekaitseseaduse paragrahv 76.

([149]) 2018. aasta andmekaitseseaduse paragrahv 76.

([150]) 2018. aasta andmekaitseseaduse paragrahvi 76 lõige 3.

asutus otsustab, kas edasisaatmist lubada või mitte, peab ta veenduma, et edasisaatmine on vajalik õiguskaitse eesmärgil, ning peaks arvesse võtma muu hulgas järgmisi tegureid: a) loataotluse aluseks olnud asjaolude raskus; b) isikuandmete algse edastamise eesmärk ja c) isikuandmete kaitse standardid, mida kohaldatakse selles kolmandas riigis või rahvusvahelises organisatsioonis, kuhu isikuandmed edasi saadetakse.

(83) Kui Ühendkuningriigist edasisaadetavad andmed saadeti algselt Euroopa Liidust, kohaldatakse täiendavaid kaitsemeetmeid.

(84) Sarnaselt direktiivi (EL) 2016/680 artikli 35 lõike 1 punktiga c on 2018. aasta andmekaitseseaduse paragrahvi 73 lõike 1 punktis b ette nähtud, et kui liikmesriik edastas vastutavale töötlejale või muule pädevale asutusele isikuandmed või tegi need talle muul viisil kättesaadavaks, siis see liikmesriik või selles liikmesriigis asuv isik, kes on direktiivi (EL) 2016/680 eesmärkidel pädev asutus, on andnud loa andmete edastamiseks kooskõlas liikmesriigi õigusega.

(85) Sarnaselt direktiivi (EL) 2016/680 artikli 35 lõikega 2 ei ole aga selline luba vajalik, kui a) isikuandmete edastamine on vajalik liikmesriigi või kolmanda riigi avalikku julgeolekut ähvardava vahetu ja tõsise ohu ennetamiseks või liikmesriigi olulise huvi seisukohast ning b) luba ei ole võimalik õigeaegselt saada. Sellisel juhul tuleb viivitamata teavitada selle liikmesriigi asutust, mis oleks pidanud otsustama, kas lubada andmete edastamist ([151]).

(86) Sama lähenemisviisi kohaldatakse andmete suhtes, mis on algselt saadetud Euroopa Liidust Ühendkuningriiki ja siis on Ühendkuningriik need omakorda saatnud kolmandasse riiki, kes saadab need seejärel edasi kolmandasse riiki. Sellisel juhul ei tohi Ühendkuningriigi pädev asutus vastavalt paragrahvi 78 lõikele 4 anda viimati nimetatud edastamiseks luba paragrahvi 78 lõike 1 kohaselt, välja arvatud juhul, kui „liikmesriik [kes algselt kõnealused andmed edastas] või selles liikmesriigis asuv isik, kes on õiguskaitsedirektiivi kohaldamisel pädev asutus, on andnud loa andmete edastamiseks kooskõlas liikmesriigi õigusega“. Need kaitsemeetmed on olulised, sest need võimaldavad liikmesriikide ametiasutustel tagada kaitse järjepidevuse kooskõlas ELi andmekaitseõigusega kogu edastamise ajal.

(87) Seda andmete rahvusvahelise edastamise uut raamistikku kohaldatakse alates üleminekuperioodi lõpust ([152]). Andmekaitse, eraelu puutumatuse ja elektroonilise side määrusega kehtestatud 21. lisa punktides 10–12 on aga ette nähtud, et pärast üleminekuperioodi lõppu käsitletakse teatavate isikuandmete edastamist nii, nagu see põhineks kaitse piisavuse määrustel. Selline edastamine hõlmab edastamist liikmesriigile, EFTA riigile, kolmandatele riikidele, mille suhtes kohaldatakse üleminekuperioodi lõpus ELi kaitse piisavuse otsust, ja Gibraltari territooriumile. Järelikult võib andmete edastamine nendele riikidele jätkuda nii, nagu see toimus enne Ühendkuningriigi väljaastumist liidust. Pärast üleminekuperioodi lõppu peab minister vaatama need kaitse piisavuse otsused läbi nelja aasta jooksul, s.o 2024. aasta detsembri lõpuks. Kuigi minister peab sellise läbivaatamise lõpule viima 2024. aasta detsembri lõpuks, ei hõlma üleminekusätted Ühendkuningriigi ametiasutuste antud selgituse kohaselt aegumisklausli sätet ja asjakohased üleminekusätted ei muutu automaatselt kehtetuks, kui läbivaatamist 2024. aasta detsembri lõpuks läbi ei viida.

2.4.9. *Aruandekohustus*

(88) Vastutuse põhimõtte kohaselt peavad andmeid töötlevad avaliku sektori asutused kehtestama asjakohased tehnilised ja korralduslikud meetmed, et täita tõhusalt oma andmekaitsekohustusi ja suuta nende täitmist tõendada, eriti pädevale järelevalveasutusele.

(89) Seda põhimõtet kajastatakse 2018. aasta andmekaitseseaduse paragrahvis 56, millega kehtestatakse vastutavale töötlejale üldine aruandekohustus, s.o kohustus rakendada asjakohaseid tehnilisi ja korralduslikke meetmeid, et tagada ja suuta tõendada, et isikuandmete töötlemine vastab 2018. aasta andmekaitseseaduse 3. osa nõuetele. Rakendatud meetmed tuleb läbi vaadata ja neid vajaduse korral ajakohastada ning kui see on töötlemisega seoses proportsionaalne, peavad need sisaldama asjakohaseid andmekaitsepõhimõtteid.

([151]) 2018. aasta andmekaitseseaduse paragrahvi 73 lõige 5.

([152]) Uue raamistiku kohaldatavust tuleb käsitleda koos ühelt poolt Euroopa Liidu ja Euroopa Aatomienergiaühenduse ning teiselt poolt Suurbritannia ja Põhja-Iiri Ühendkuningriigi vahelise kaubandus- ja koostöölepingu (ELT L 444, 31.12.2020, lk 14) (edaspidi „ELi ja Ühendkuningriigi kaubandus- ja koostööleping“) artikliga 782 Leping on kättesaadav aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:22020A1231(01)&from=ET.

(90) Kooskõlas direktiivi (EL) 2016/680 IV peatükiga on 2018. aasta andmekaitseseaduse paragrahvides 55–71 ette nähtud erinevad mehhanismid, et tagada aruandekohustus ning võimaldada vastutavatel töötlejatel ja volitatud töötlejatel nõuetele vastavust tõendada. Eelkõige nõutakse, et vastutav töötleja rakendaks lõimitud andmekaitse ja vaikimisi andmekaitse meetmeid, et tagada andmekaitsepõhimõtete tõhus rakendamine, dokumenteeriks kõik töötlemistoimingute liigid, mille eest ta vastutab (sealhulgas teave vastutava töötleja identiteedi kohta, andmekaitseametniku kontaktandmed, töötlemise eesmärgid, avalikustatavate andmete saajate kategooriad, kirjeldus andmesubjektide kategooriate kohta ja isikuandmed), ning teeks need dokumendid teabevolinikule taotluse korral kättesaadavaks. Lisaks peavad vastutav töötleja ja volitatud töötleja pidama teatavate töötlemistoimingute kohta logisid ja tegema need teabevolinikule kättesaadavaks ([153]). Vastutavalt töötlejalt nõutakse ka teabevoliniku ülesannete täitmise käigus volinikuga koostöö tegemist.

(91) 2018. aasta andmekaitseseaduses on sätestatud lisanõuded töötlemisele, mis põhjustab tõenäoliselt suurt ohtu isikute õigustele ja vabadustele. Nende hulka kuulub kohustus viia ellu andmekaitsealased mõjuhindamised ja konsulteerida enne töötlemist teabevolinikuga, kui sellisest hindamisest nähtub, et töötlemise tulemusena tekiks suur oht isikute õigustele ja vabadustele (kui puuduvad ohu leevendamise meetmed).

(92) Vastutav töötleja peab ka määrama andmekaitseametniku, välja arvatud juhul, kui vastutav töötleja on kohus või muu õigusasutus, mis täidab õigusemõistja funktsiooni ([154]). Vastutav töötleja peab tagama, et andmekaitseametnik on kaasatud kõikidesse isikuandmete kaitsega seotud küsimustesse, tal on vajalikud vahendid ja juurdepääs isikuandmetele ja nende töötlemise toimingutele ning ta suudab täita oma ülesandeid sõltumatult. Andmekaitseametniku ülesanded on sätestatud 2018. aasta andmekaitseseaduse paragrahvis 71; nende hulka kuulub teavitamine ja nõustamine, nõuete täitmise jälgimine, koostöö teabevolinikuga ning tegutsemine tema kontaktpunktina. Oma ülesannete täitmisel peab andmekaitseametnik võtma arvesse töötlemistoimingutega seotud ohte ning arvestama töötlemise laadi, ulatust, konteksti ja eesmärke.

2.5. **Järelevalve ja täitmise tagamine**

2.5.1. *Sõltumatu järelevalve*

(93) Et tagada andmekaitse piisav tase ka praktikas, peab olema loodud sõltumatu järelevalveasutus, millele on antud volitused jälgida andmekaitse-eeskirjadele vastavust ja tagada nende täitmine. See asutus peab tegutsema oma ülesandeid täites ja volitusi kasutades täiesti sõltumatult ja erapooletult.

(94) Ühendkuningriigis jälgib Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseseaduse täitmist ja tagab selle teabevolinik ([155]). Teabevolinik jälgib ka 2018. aasta andmekaitseseaduse 3. osa kohaldamisalasse kuuluvate isikuandmete töötlemist pädevate asutuste poolt ([156]). Teabevolinik on ühest füüsilisest isikust koosnev eraldiseisev juriidiline isik (*Corporation Sole*). Teabevolinikku toetab tema töös büroo. 31. märtsil 2020 oli teabevoliniku büroos 768 alalist töötajat ([157]). Teabevolinikku toetav ministeerium on digi-, kultuuri-, meedia- ja spordiministeerium ([158]).

([153]) 2018. aasta andmekaitseseaduse paragrahv 62.
([154]) 2018. aasta andmekaitseseaduse paragrahv 69.
([155]) Direktiivi (EL) 2016/680 artikli 36 lõike 2 punkt b.
([156]) 2018. aasta andmekaitseseaduse paragrahv 116.
([157]) Teabevoliniku 2019.–2020. aasta aruanne ja finantsaruanded, kättesaadavad aadressil https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.
([158]) Nende kahe suhteid reguleeritakse halduslepinguga. Digi-, kultuuri-, meedia- ja spordiministeeriumi peamised kohustused on järgmised: teabevoliniku büroole piisavate rahaliste ja muude vahendite tagamine; teabevoliniku büroo huvide esindamine parlamendis ja teistes ministeeriumites; range riikliku andmekaitseraamistiku tagamine ning teabevoliniku büroo nõustamine ja toetamine äriühingutega seotud küsimustes, nagu kinnisasjad, rendilepingud ja hanked (2018.–2021. aasta halduslepping, kättesaadav aadressil https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Voliniku sõltumatus on sõnaselgelt kehtestatud Ühendkuningriigi isikuandmete kaitse üldmääruse artiklis 52, milles kajastatakse Euroopa Parlamendi ja nõukogu määruse (EL) 2016/679 ([159]) artikli 52 lõigetes 1–3 sätestatud nõudeid. Volinik peab tegutsema talle kooskõlas Ühendkuningriigi isikuandmete kaitse üldmäärusega antud ülesannete täitmisel ja volituste kasutamisel täiesti sõltumatult, jääma nende ülesannete ja volitustega seoses vabaks nii otsestest kui ka kaudsetest välistest mõjutustest ning ei tohi küsida ega võtta vastu juhiseid mitte kelleltki. Volinik peab ka hoiduma oma kohustustega kokkusobimatust tegevusest ega tööta oma ametiaja jooksul ühelgi muul sobimatul tasustatud või tasustamata ametikohal.

(96) Teabevoliniku ametisse nimetamise ja ametist tagandamise tingimused on sätestatud 2018. aasta andmekaitseseaduse 12. lisas. Teabevoliniku nimetab ametisse kuninganna valitsuse soovitusel ausa ja avatud konkurentsi tingimustel. Kandidaadil peavad olema asjakohane kvalifikatsioon, oskused ja pädevus. Nõuandev hindamiskomisjon koostab sobivate kandidaatide nimekirja kooskõlas avalikesse ametitesse nimetamise koodeksiga (Governance Code on Public Appointments) ([160]). Enne kui digi-, kultuuri-, meedia- ja spordiminister teeb lõpliku otsuse, peab asjaomane parlamendi erikomisjon läbi viima ametisse nimetamise eelse kontrolli. Erikomisjoni seisukoht avalikustatakse ([161]).

(97) Teabevoliniku ametiaeg on kuni seitse aastat. Tema Majesteet võib teabevoliniku ametist tagandada pärast mõlema parlamendikoja sellekohast pöördumist ([162]). Teabevoliniku ametist tagandamise taotlust ei tohi tuua kummagi parlamendikoja ette, kui minister ei ole esitanud sellele kojale aruannet, milles sedastatakse, et ta on veendunud, et teabevolinik on süüdi raskes teenistuskohustuste rikkumises ja/või volinik ei vasta enam voliniku ülesannete täitmiseks vajalikele tingimustele ([163]).

(98) Teabevolinikku rahastatakse kolmest allikast: i) vastutavate töötlejate makstavad andmekaitsetasud, mis on sätestatud ministri määrusega ([164]) ja moodustavad 85–90 % büroo aastaeelarvest; ([165]) ii) teabevolinikule makstav valitsuse võimalik toetus, mida kasutatakse peamiselt teabevoliniku muude kui andmekaitsega seotud tegevuskulude rahastamiseks; ([166]) iii) teenuste eest võetavad tasud ([167]). Praegu selliseid tasusid ei võeta.

(99) Teabevoliniku üldised ülesanded 2018. aasta andmekaitseseaduse 3. osa kohaldamisalasse kuuluvate isikuandmete töötlemisel on sätestatud 2018. aasta andmekaitseseaduse 13. lisas. Ülesannete hulka kuuluvad 2018. aasta andmekaitseseaduse 3. osa täitmise seire ja tagamine, üldsuse teadlikkuse suurendamine, parlamendi, valitsuse ja teiste institutsioonide nõustamine seadusandlike ja haldusmeetmete valdkonnas, vastutavate töötlejate ja volitatud töötlejate teadlikkuse suurendamine nende kohustuste valdkonnas, andmesubjektidele teabe jagamine nende õiguste

([159]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (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) (ELT L 119, 4.5.2016, lk 1).

([160]) Avalikesse ametitesse nimetamise koodeks (Governance Code on Public Appointments), kättesaadav aadressil https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Alamkoja kultuuri-, meedia- ja spordikomisjoni 2015.–2016. aasta istungjärgu teine aruanne, kättesaadav aadressil https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) Pöördumine (*address*) on parlamendile esitatav ettepanek, mille eesmärk on teavitada monarhi parlamendi arvamustest konkreetses küsimuses.

([163]) 2018. aasta andmekaitseseaduse 12. lisa punkt 3.

([164]) 2018. aasta andmekaitseseaduse paragrahv 137.

([165]) 2018. aasta andmekaitseseaduse paragrahvides 137 ja 138 on mitu kaitsemeedet, millega tagada, et tasud oleksid sätestatud asjakohasel tasemel. 2018. aasta andmekaitseseaduse paragrahvi 137 lõikes 4 on loetletud aspektid, millele minister peab tähelepanu pöörama, kui ta koostab määrust, milles täpsustatakse eri organisatsioonide makstav summa. 2018. aasta andmekaitseseaduse paragrahvi 138 lõikes 1 ja paragrahvis 182 on ka õigusnõue, et minister peab enne määruse koostamist konsulteerima teabevolinikuga ja selliste isikute muude esindajatega, keda määrus tõenäoliselt mõjutab, et nende seisukohti oleks võimalik arvesse võtta. 2018. aasta andmekaitseseaduse paragrahvi 138 lõike 2 alusel peab teabevolinik korrapäraselt jälgima tasude määruse toimimist ja võib esitada ministrile ettepanekuid määruse muutmise kohta. Määruse vastuvõtmiseks kasutatakse kinnitava resolutsiooni menetlust (*affirmative resolution procedure*) ja määruseid ei tohi anda enne, kui need on heaks kiidetud mõlema parlamendikoja resolutsiooniga, välja arvatud juhul, kui määrus antakse vaid tarbijahinnaindeksi tõusu arvesse võtmiseks (siis kohaldatakse negatiivse resolutsiooni menetlust (*negative resolution procedure*)).

([166]) Halduslepingus selgitatakse, et „Minister võib 2018. aasta andmekaitseseaduse 12. lisa punkti 9 alusel teha teabevolinikule makseid parlamendi eraldatud rahast. Pärast teabevolinikuga konsulteerimist maksab digi-, kultuuri-, meedia- ja spordiministeerium teabevolinikule asjakohased summad (toetus), et katta teabevoliniku büroo halduskulud ja teabevoliniku mitme eriülesande, sealhulgas teabevabaduse tagamise kulud“ (2018.–2021. aasta halduslepingu punkt 1.12, vt joonealune märkus 158).

([167]) 2018. aasta andmekaitseseaduse paragrahv 134.

teostamise kohta ning uurimiste läbiviimine. Selleks et säiliks kohtusüsteemi sõltumatus, ei ole teabevolinikul lubatud rakendada oma volitusi isikuandmeid töötleva isiku või kohtu suhtes, kes täidab õigusemõistja funktsiooni. Kohtusüsteemi järelevalve tagavad eriorganid, seda käsitletakse allpool.

2.5.1.1. Täitmise tagamine, sealhulgas sanktsioonid

(100) Volinikul on üldised uurimis-, parandus-, loa- ja nõustamisvolitused nende isikuandmete töötlemisel, mille suhtes kohaldatakse 2018. aasta andmekaitseseaduse 3. osa. Volinikul on pädevus teavitada vastutavat töötlejat või volitatud töötlejat 3. osa väidetavast rikkumisest, esitada vastutavale töötlejale või volitatud töötlejale hoiatusi, et kavandatud töötlemistoimingud on tõenäoliselt vastuolus 3. osa normidega, ning esitada vastutavale töötlejale või volitatud töötlejale noomitusi, kui töötlemistoimingutega on rikutud 3. osa norme. Volinik võib omal algatusel või taotluse korral esitada isikuandmete kaitsega seotud teemadel arvamusi Ühendkuningriigi parlamendile, valitsusele või teistele institutsioonidele ja organitele, samuti üldsusele ([168]).

(101) Volinikul on ka järgmised volitused:

— nõuda teabenõudega vastutavalt töötlejalt ja volitatud töötlejalt (ja teatavatel asjaoludel muult isikult) vajaliku teabe esitamist (teabenõue); ([169])

— viia läbi uurimisi ja auditeid ja esitada hindamisteade, milles võib nõuda, et vastutav töötleja või volitatud töötleja lubaks volinikul siseneda kindlaksmääratud valdustesse, kontrollida või uurida dokumente või vahendeid või küsitleda vastutava töötleja nimel isikuandmeid töötlevaid isikuid (hindamisteade); ([170])

— saada muul viisil ligipääs vastutavate töötlejate ja volitatud töötlejate dokumentidele ning nende valdustele kooskõlas 2018. aasta andmekaitseseaduse paragrahviga 154 (sisenemis- ja kontrollivolitused);

— teostada parandusvolitusi, sealhulgas kasutades hoiatusi ja noomitusi, või kasutada korralduste andmiseks täitmisteateid, nõudes, et vastutavad töötlejad/volitatud töötlejad võtaksid või ei võtaks konkreetseid meetmeid (täitmisteade), ([171]) ning

— teha trahviteatega haldustrahve (trahviteade) ([172]).

(102) Teabevoliniku büroo reguleerimispõhimõtetes (Regulatory Action Policy) on sätestatud asjaolud, mille korral volinik esitab vastavalt teavitusi ning hindamis-, sundtäitmise ja trahviteateid ([173]). Täitmisteates võib esitada nõuded, mille täitmist volinik peab asjakohaseks, et kõrvaldada puudus. Karistusteate korral peab isik maksma teabevolinikule teates määratud summa. Karistusteate võib esitada, kui 2018. aasta andmekaitseseaduse teatavad nõuded on täitmata, ([174]) või esitada vastutavale töötlejale või volitatud töötlejale, kes ei ole järginud teabenõuet, hindamisteadet või täitmisteadet.

(103) Kui teabevolinik otsustab, kas esitada vastutavale töötlejale või volitatud töötlejale trahviteade, ja kui ta määrab karistussummat, peab ta konkreetsemalt võtma arvesse 2018. aasta andmekaitseseaduse paragrahvi 155 lõikes 3 loetletud küsimusi, sealhulgas rikkumise laad ja raskus, kas rikkumine pandi toime tahtlikult või hooletusest, vastutava töötleja või volitatud töötleja võetud meetmed andmesubjektide kantava kahju leevendamiseks, vastutava

([168]) 2018. aasta andmekaitseseaduse 13. lisa paragrahv 2.
([169]) 2018. aasta andmekaitseseaduse paragrahv 142 (vastavalt 2018. aasta andmekaitseseaduse paragrahvis 143 esitatud piirangutele).
([170]) 2018. aasta andmekaitseseaduse paragrahv 146 (vastavalt 2018. aasta andmekaitseseaduse paragrahvis 147 esitatud piirangutele).
([171]) 2018. aasta andmekaitseseaduse paragrahvid 149–151 (vastavalt 2018. aasta andmekaitseseaduse paragrahvis 152 esitatud piirangutele).
([172]) 2018. aasta andmekaitseseaduse paragrahv 155 (vastavalt 2018. aasta andmekaitseseaduse paragrahvis 156 esitatud piirangutele).
([173]) Reguleerimispõhimõtted (Regulatory Action Policy), kättesaadavad aadressil https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Teabevoliniku büroo võib esitada trahviteate 2018. aasta andmekaitseseaduse paragrahvi 149 lõikes 2, 3, 4 või 5 nimetatud täitmatajätmiste eest.

töötleja või volitatud töötleja vastutuse aste (võttes arvesse vastutava töötleja või volitatud töötleja võetud tehnilisi ja korralduslikke meetmeid), vastutava töötleja või volitatud töötleja eelnevad asjakohased rikkumised, rikkumisest mõjutatud isikuandmete liigid ning kas karistus on tõhus, proportsionaalne ja heidutav.

(104) Karistusteatega kehtestatav maksimaalne võimalik karistussumma on a) 17 500 000 naelsterlingit juhul, kui on rikutud andmekaitsepõhimõtteid (2018. aasta andmekaitseseaduse paragrahvid 35, 36, 37, paragrahvi 38 lõige 1, paragrahvi 39 lõige 1 ja paragrahv 40), läbipaistvuskohustusi ja üksikisiku õigusi (2018. aasta andmekaitseseaduse paragrahvid 44, 45, 46, 47, 48, 49, 52 ja 53) ja isikuandmete rahvusvahelise edastamise põhimõtteid (2018. aasta andmekaitseseaduse paragrahvid 73, 75, 76, 77 ja 78) ning b) 8 700 000 naelsterlingit muul juhul ([175]). Kui ei järgita teabenõuet, hindamisteadet või täitmisteadet, võib trahviteatega kehtestada kuni 17 500 000 naelsterlingi suuruse karistussumma.

(105) Oma viimaste aastaaruannete (2018–2019, ([176]) 2019–2020) ([177]) kohaselt on teabevolinik viinud läbi mitu uurimist seoses isikuandmete töötlemisega kriminaalõiguskaitseasutuste poolt. Näiteks 2019. aasta oktoobris viis volinik läbi uurimise ja avaldas arvamuse õiguskaitse eesmärgil näotuvastustehnoloogia kasutamise kohta avalikes kohtades. Uurimises keskenduti eriti reaalajas näotuvastuse võimekuse kasutamisele Lõuna-Walesi politseis ja Londoni politseiametis (Metropolitan Police Service). Volinik uuris ka metropoli politseiteenistuse nn jõukude maatriksit ([178]) ja avastas mitu andmekaitseõiguse rasket rikkumist, mis vähendavad tõenäoliselt maatriksi ja andmete kasutamise usaldusväärsust avalikkuse silmis.

(106) Teabevolinik esitas 2018. aasta novembris täitmisteate ja seejärel võttis metropoli politseiteenistus vajalikud meetmed, et suurendada turvalisust ja vastutust ning tagada andmete proportsionaalne kasutamine.

(107) Teine näide hiljutisest täitemeetmest on ka 325 000 naelsterlingi suurune trahv, mille volinik tegi 2018. aasta mais prokuratuurile selle eest, et asutusest läksid kaduma krüpteerimata DVD-d politseiküsitluste salvestustega. Teabevolinik on uurinud ka laiemaid küsimusi, näiteks 2020. aasta esimeses pooles uuriti mobiiltelefoni kõneeristuse väljavõtte kasutamist politseitöö eesmärgil ja ohvrite andmete töötlemist politsei poolt.

(108) Lisaks selliste täidesaatvate volituste kasutamisele võib teabevolinik kehtestada kriminaalsanktsioone teatavate andmekaitseõiguse valdkonna süütegude eest (2018. aasta andmekaitseseaduse paragrahv 196). Sellised süüteod on näiteks need, kui vastutava töötleja nõusolekuta hangitakse või avaldatakse isikuandmeid või vastutava töötleja nõusolekuta tagatakse isikuandmete avalikustamine teisele isikule; ([179]) isiku tuvastamist mittevõimaldavad isikuandmed muudetakse tuvastamist võimaldavateks andmeteks ilma selle vastutava töötleja nõusolekuta, kes vastutab andmete tuvastamist mittevõimaldavaks muutmise eest; ([180]) teabevolinikul takistatakse tahtlikult tema volituste kasutamist isikuandmete kontrollimisel rahvusvaheliste kohustuste kohaselt, ([181]) teabenõudele vastates tehakse vääraid avaldusi või hävitatakse teabenõude ja hindamisteatega seotud teavet ([182]).

(109) Teabevolinikul on ka 2018. aasta andmekaitseseaduse paragrahvist 139 tulenev kohustus esitada mõlemale parlamendikojale üldaruanne volinikule andmekaitseseadusest tulenevate funktsioonide täitmise kohta ([183]).

([175]) 2018. aasta andmekaitseseaduse paragrahv 157.

([176]) Teabevoliniku 2018.-2019. aasta aruanne ja finantsaruanded, kättesaadavad aadressil https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Teabevoliniku 2019.–2020. aasta aruanne (vt joonealune märkus 157).

([178]) Andmebaas, kus dokumenteeriti politseiteave väidetavate jõuguliikmete ja jõukudega seotud süütegude ohvrite kohta.

([179]) 2018. aasta andmekaitseseaduse paragrahv 170.

([180]) 2018. aasta andmekaitseseaduse paragrahv 171.

([181]) 2018. aasta andmekaitseseaduse paragrahv 119.

([182]) 2018. aasta andmekaitseseaduse paragrahvid 144 ja 148.

([183]) Halduslepingu kohaselt peab aastaaruanne: i) hõlmama teabevoliniku büroo kontrolli alla kuuluvaid äriühinguid, tütarettevõtteid või ühisettevõtteid; ii) vastama rahandusministeeriumi finantsaruandluse käsiraamatule (Financial Reporting Manual); iii) sisaldama juhtimisaruannet, milles on esitatud viisid, kuidas peaarvepidaja on hallanud ja kontrollinud organisatsioonis aasta jooksul kasutatud vahendeid, ja milles näidatakse, kui hästi organisatsioon haldab oma eesmärkide täitmisega kaasnevaid riske, iv) sisaldama ülevaadet eelmise eelarveaasta põhitegevusest ja tulemuslikkusest ning kokkuvõtet tulevastest plaanidest (2018.–2021. aasta halduslepingu punkt 3.26, vt joonealune märkus 158).

2.5.2. *Järelevalve kohtusüsteemi üle*

(110) Kohtutes ja kohtusüsteemis toimuva isikuandmete töötlemise järelevalvel on kaks osa. Kui kohtunik või kohus ei täida õigusemõistja funktsiooni, teostab järelevalvet teabevolinik. Kui vastutav töötleja täidab õigusemõistja funktsiooni, ei saa teabevoliniku büroo täita järelevalve ülesandeid ([184]) ja järelevalvet teostavad eriorganid. See sarnaneb direktiivi (EL) 2016/680 artiklis 32 esitatud lähenemisviisiga.

(111) Teise stsenaariumi korral, mis hõlmab Inglismaa ja Walesi kohtuid ning Inglismaa ja Walesi esimese astme kohtuid ja kõrgemaid kohtuid, teostab järelevalvet kohtusüsteemi andmekaitse komitee (Judicial Data Protection Panel) ([185]). Lisaks on ülemkohtunik (Lord Chief Justice) ja kohtute vanempresident (Senior President of Tribunals) avaldanud isikuandmete kaitse teate, ([186]) milles on sätestatud, kuidas Inglismaa ja Walesi kohtud töötlevad isikuandmeid õigusemõistmise eesmärgil. Sarnase teate on avaldanud Põhja-Iirimaa ([187]) ja Šotimaa kohtusüsteem ([188]).

(112) Põhja-Iirimaa ülemkohtunik on Põhja-Iirimaal nimetanud ühe kõrge kohtu kohtuniku andmete järelevalve kohtunikuks (*Data Supervisory Judge*) ([189]). Samuti on nad avaldanud Põhja-Iirimaa kohtunikele suunised selle kohta, mida teha andmete kaotsimineku või võimaliku kaotsimineku korral ja kuidas lahendada sellest tulenevaid probleeme ([190]).

(113) Šotimaal on lordpresident (*Lord President*) nimetanud ametisse andmete järelevalve kohtuniku (*Data Supervisory Judge*), kes uurib andmekaitse kaalutlustel esitatud kaebusi. See on sätestatud kohtunikke käsitlevate kaebuste eeskirjades, mis sarnanevad Inglismaal ja Walesis kehtestatud vastavate eeskirjadega ([191]).

(114) Kõrgeimas kohtus teostab andmekaitse järelevalvet üks kõrgeima kohtu kohtunikest.

([184]) 2018. aasta andmekaitseseaduse paragrahv 117.

([185]) Komitee vastutab kohtutele suuniste andmise ja koolituse eest. Samuti lahendab ta andmesubjektide kaebusi, mis puudutavad isikuandmete töötlemist kohtute ja õigusemõistja funktsiooni täitvate isikute poolt. Komitee eesmärk on tagada vahendid kaebuste lahendamiseks. Kui kaebuse esitaja ei ole rahul komitee otsusega ja esitab lisatõendeid, võib komitee oma otsuse läbi vaadata. Komitee ise ei kehtesta rahalisi sanktsioone, kuid kui ta leiab, et tegemist on 2018. aasta andmekaitseseaduse piisavalt raske rikkumisega, võib ta edastada asja kohtunike tegevuse uurimise büroole (Judicial Conduct Investigation Office), kes uurib kaebust. Kui kaebus on põhjendatud, otsustavad lordkantsler (*Lord Chancellor*) ja ülemkohtunik (*Lord Chief Justice*) (või tema nimel tegutsema määratud vanemkohtunik), milliseid meetmeid tuleb ametikandja suhtes võtta. Need võivad raskuse järjekorras olla ametlik nõustamine, ametlik hoiatus ja noomitus ning lõpuks ametist tagandamine. Kui isik ei ole rahul sellega, kuidas kohtunike tegevuse uurimise büroo on kaebust uurinud, võib ta esitada kaebuse ka kohtunike ametisse nimetamise ja kohtunike tegevuse ombudsmanile (*Judicial Appointments and Conduct Ombudsman*) (vt https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsman võib paluda kohtunike tegevuse uurimise bürool kaebust uuesti uurida ja kui ta leiab, et kaebuse esitaja on kandnud kahju haldusomavoli tõttu, võib ta teha ettepaneku maksta kaebuse esitajale hüvitist.

([186]) Ülemkohtuniku ja kohtute vanempresidendi (*Senior President of Tribunals*) isikuandmete kaitse teade on kättesaadav aadressil https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Põhja-Iirimaa ülemkohtuniku isikuandmete kaitse teade on kättesaadav aadressil https://judiciaryni.uk/data-privacy.

([188]) Šotimaa kohtute isikuandmete kaitse teade on kättesaadav aadressil https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Andmete järelevalve kohtunik annab kohtunikele suuniseid ja uurib rikkumisi ja/või kaebusi, mis puudutavad isikuandmete töötlemist kohtute või õigusemõistja funktsiooni täitvate isikute poolt.

([190]) Kui kaebust või rikkumist peetakse raskeks, edastatakse see uurimiseks kohtunikke käsitlevate kaebustega tegelevale ametnikule (*Judicial Complaints Officer*) vastavalt Põhja-Iirimaa ülemkohtuniku avaldatud kaebusi käsitlevale tegevusjuhendile (Code of Practice on Complaints). Sellise kaebuse võimalik tulemus: edasisi meetmeid ei võeta, nõustamine, koolitus või mentorlus, mitteametlik hoiatus, ametlik hoiatus, lõplik hoiatus, tegevuse piiramine või asja andmine seadusega ette nähtud kohtusse. Põhja-Iirimaa ülemkohtuniku avaldatud kaebusi käsitlev tegevusjuhend on kättesaadav aadressil https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([191]) Kõiki põhjendatud kaebusi uurib andmete järelevalve kohtunik ja need edastatakse lordpresidendile, kellel on volitus anda nõu või esitada ametlik hoiatus või noomitus, kui ta peab seda vajalikuks (eeskirjad on kättesaadavad aadressil https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Õiguskaitse*

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

(116) Andmesubjektil on kõigepealt õigus esitada kaebus teabevolinikule, kui andmesubjekt leiab, et seoses tema isikuandmetega on rikutud 2018. aasta andmekaitseseaduse 3. osa ([192]). Nagu kirjeldatud põhjendustes 100 ja 109, on teabevolinik pädev hindama vastutava töötleja ja volitatud töötleja vastavust 2018. aasta andmekaitseseadusele, nõudma neilt mittevastavuse korral vajalike meetmete võtmist või meetmete võtmata jätmist ning kehtestama trahve.

(117) Teiseks on 2018. aasta andmekaitseseaduses ette nähtud õigus õiguskaitsevahendile teabevoliniku vastu. Kui volinik ei tee andmesubjekti esitatud kaebuse menetlemisel edusamme, ([193]) on kaebuse esitajal juurdepääs õiguskaitsevahendile, sest ta võib taotleda, et esimese astme kohus ([194]) käsiks volinikul võtta asjakohased meetmed kaebusele vastamiseks või teavitada kaebuse esitajat kaebuse menetlemise edusammudest ([195]). Esimese astme kohtu poole võib pöörduda ka iga isik, kellele volinik on esitanud eespool nimetatud teavituse või teate (teavitus, hindamis-, sundtäitmise või trahviteade). Kui kohus leiab, et teabevoliniku otsus ei ole õigusega kooskõlas või ta oleks pidanud kasutama oma kaalutlusõigust teisiti, peab kohus kaebuse rahuldama või asendama teabevoliniku antud või tehtud muu teavituse või otsuse ([196]).

(118) Üksikisikud võivad kasutada ka kolmandat õiguskaitsevahendit, s.o pöörduda 2018. aasta andmekaitseseaduse paragrahvi 167 alusel vastutavate töötlejate ja volitatud töötlejate vastu otse kohtusse. Kui andmesubjekti taotluse alusel veendub kohus, et andmekaitsealaste õigusaktide kohaseid andmesubjekti õigusi on rikutud, võib kohus nõuda, et vastutav töötleja või selle vastutava töötleja nimel tegutsev volitatud töötleja võtaks asjakohase töötlemisega seoses korralduses nimetatud meetmeid või hoiduks korralduses nimetatud meetmete võtmisest. 2018. aasta andmekaitseseaduse paragrahvi 169 alusel on andmekaitsealastes õigusaktides (sealhulgas 2018. aasta andmekaitseseaduse 3. osas), välja arvatud Ühendkuningriigi isikuandmete kaitse üldmääruses sätestatud nõude rikkumise tõttu kahju kandval isikul õigus saada selle kahju eest hüvitist vastutavalt töötlejalt või volitatud töötlejalt, välja arvatud juhul, kui vastutav töötleja või volitatud töötleja tõestab, et vastutav töötleja või volitatud töötleja ei vastuta kahju tekitanud juhtumi eest. Kahju hõlmab nii rahalist kui ka mitterahalist kahju, näiteks kannatusi.

(119) Neljandaks, kui isik leiab, et avaliku sektori asutused on rikkunud tema õigusi, sealhulgas eraelu puutumatuse õigus ja andmekaitse õigus, võib ta õiguskaitse saamiseks pöörduda 1998. aasta inimõiguste seaduse (Human Rights Act) alusel Ühendkuningriigi kohtute poole. 2018. aasta andmekaitseseaduse 3. osas käsitletavad vastutavad töötlejad, s. o pädevad asutused, on alati avaliku sektori asutused 1998. aasta inimõiguste seaduse tähenduses. Isik, kes väidab, et avaliku sektori asutus on tegutsenud (või kavatseb tegutseda) viisil, mis on vastuolus konventsiooni kohase õigusega ja seega tulenevalt 1998. aasta inimõiguste seaduse paragrahvi 6 lõikest 1 ebaseaduslik, võib esitada asutuse vastu hagi asjakohasesse kohtusse või tugineda asjakohastele õigustele igas õigusmenetluses, kui ta on (või võib olla) ebaseadusliku teo ohver ([197]).

([192]) 2018. aasta andmekaitseseaduse paragrahv 165.

([193]) 2018. aasta andmekaitseseaduse paragrahvis 166 osutatakse konkreetselt järgmistele olukordadele: a) volinik ei võta asjakohaseid meetmeid kaebusele vastamiseks, b) volinik ei anna kaebuse esitajale teavet kaebuse menetlemisel tehtud edusammudest või kaebuse tulemusest enne, kui möödub kolmekuune ajavahemik, mis algas, kui volinik kaebuse sai, või c) kui volinik ei ole selle ajavahemiku jooksul kaebuse menetlemist lõpetanud, ei anna ta kaebuse esitajale sellist teavet järgmise kolme kuu jooksul.

([194]) Esimese astme kohus on pädev kohus valitsuse reguleerivate asutuste tehtud otsuste peale esitatud kaebuste menetlemisel. Teabevoliniku otsuse korral on pädev kolleegium üldkolleegium (General Regulatory Chamber), millel on pädevus kogu Ühendkuningriigis.

([195]) 2018. aasta andmekaitseseaduse paragrahv 166.

([196]) 2018. aasta andmekaitseseaduse paragrahvid 161 ja 162.

([197]) Vt 2016. aasta kohtuasi Brown *vs.* Commissioner of the Met, kus kohus hüvitas kahju hagejale, kes oli esitanud politsei vastu andmekaitsealase hagi. Kohus langetas otsuse hageja kasuks, rahuldades tema hagi, mille kohaselt on rikutud 1998. aasta andmekaitseseadusest tulenevaid kohustusi, 1998. aasta inimõiguste seadust (ja Euroopa inimõiguste konventsiooni artiklis 8 sätestatud seotud õigust) ja tekitatud õigusvastast kahju eraeluliste andmete väärkasutamisega (lõpuks tunnistas kostja, et rikkus andmekaitseseadust ja Euroopa inimõiguste konventsiooni, nii et kohtuotsuses keskenduti asjakohase hüvitise määramisele). Nende rikkumiste tulemusena määras kohus hagejale rahalise kahjuhüvitise.

(120) Kui kohus leiab, et avaliku sektori asutuse tegu on ebaseaduslik, võib ta määrata oma pädevuse piires sellise hüvitise või teha sellise korralduse, mida ta peab õiglaseks ja asjakohaseks ([198]). Samuti võib kohus otsustada, et esmase õiguse akti säte on vastuolus Euroopa inimõiguste konventsiooniga tagatud õigusega.

(121) Kui kõik riiklikud õiguskaitsevahendid on ammendatud, võib isik pöörduda Euroopa inimõiguste konventsiooniga tagatud õiguste rikkumise asjus Euroopa Inimõiguste Kohtusse.

2.6. **Andmete edasiandmine**

(122) Ühendkuningriigi õigus lubab õiguskaitseasutustel jagada andmeid teiste asutustega muudel kui andmete algse kogumise eesmärkidel (andmete edasiandmine) teatavatel tingimustel.

(123) Sarnaselt direktiivi (EL) 2016/680 artikli 4 lõikes 2 sätestatule võimaldab 2018. aasta andmekaitseseaduse paragrahvi 36 lõige 3 õiguskaitse eesmärgil pädeva asutuse kogutud isikuandmeid õiguskaitse eesmärgil täiendavalt töödelda (mida teeb kas algne või muu vastutav töötleja), tingimusel et vastutaval töötlejal on seadusjärgne volitus töödelda andmeid teisel eesmärgil ning töötlemine on vajalik ja proportsionaalne ([199]). Sellisel juhul kohaldatakse vastuvõtva asutuse tehtavale töötlemisele kõiki 2018. aasta andmekaitseseaduse 3. osaga ette nähtud ja eespool analüüsitud kaitsemeetmeid.

(124) Ühendkuningriigi õiguskorras lubatakse sõnaselgelt mitme seadusega andmete edasiandmist. Nimelt i) 2017. aasta digimajanduse seadus (Digital Economy Act 2017) võimaldab avaliku sektori asutuste vahel andmete jagamist mitmel eesmärgil, näiteks kui avaliku sektori vastu on toime pandud pettus, mis hõlmaks avaliku sektori asutusele kahju või kahju ohtu, ([200]) või kui ollakse võlgu avaliku sektori asutusele või monarhile; ([201]) ii) 2013. aasta kuritegevuse vastu võitlemise ja kohtute seadusega (Crime and Courts Act 2013) lubatakse teabe jagamist riikliku kriminaalametiga ([202]) raske ja organiseeritud kuritegevuse vastu võitlemiseks, selle uurimiseks ning selle eest vastutusele võtmiseks; iii) 2007. aasta raskeid kuritegusid käsitlev seadus (Serious Crime Act 2007) võimaldab avaliku sektori asutustel avalikustada pettustevastastele organisatsioonidele teavet pettuste ennetamise eesmärkidel ([203]).

(125) Nendes seadustes on sõnaselgelt ette nähtud, et teabe jagamine peaks olema kooskõlas 2018. aasta andmekaitseseaduses sätestatud eeskirjadega. Politseikolledž on lisaks avaldanud kinnitatud kutsetavad teabe jagamise kohta (Authorised Professional Practice on Information Sharing), ([204]) et aidata politseil täita Ühendkuningriigi isikuandmete kaitse üldmäärusest, andmekaitseseadusest ja 1998. aasta inimõiguste seadusest tulenevaid andmekaitsekohustusi. Jagamise vastavust kohaldatavale andmekaitse õigusraamistikule võib muidugi kohtulikult kontrollida ([205]).

(126) Sarnaselt direktiivi (EL) 2016/680 artiklis 9 sätestatule on 2018. aasta andmekaitseseaduses ette nähtud, et õiguskaitse eesmärgil kogutud isikuandmeid võib töödelda muul kui õiguskaitse eesmärgil, kui töötlemine on seadusega lubatud ([206]). Sellist tüüpi jagamise korral on kaks võimalust: 1) kui kriminaalõiguskaitseasutus jagab andmeid muu kui kriminaalõiguskaitseasutusega, mis ei ole luureamet (näiteks finants- või maksuasutus, konkurentsiasutus, noorte heaolu büroo); 2) kui kriminaalõiguskaitseasutus jagab andmeid luureametiga. Esimesel juhul

([198]) 1998. aasta inimõiguste seaduse paragrahvi 8 lõige 1.
([199]) 2018. aasta andmekaitseseaduse paragrahvi 36 lõige 3.
([200]) 2017. aasta digimajanduse seaduse paragrahv 56, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2017/30/contents.
([201]) 2017. aasta digimajanduse seaduse paragrahv 48.
([202]) 2013. aasta kuritegevuse vastu võitlemise ja kohtute seaduse paragrahv 7, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2013/22/contents.
([203]) 2007. aasta raskeid kuritegusid käsitleva seaduse paragrahv 68, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2007/27/contents.
([204]) Kinnitatud kutsetavad teabe jagamise kohta on kättesaadavad aadressil https://www.app.college.police.uk/app-content/information-management/sharing-police-information.
([205]) Vt näiteks kohtuasi M *vs.* the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), milles kõrgel kohtul paluti käsitleda andmete jagamist politsei ja sisenemiskeelu teate programmi haldama volitatud organisatsiooni Business Crime Reduction Partnership (ettevõtluses kuritegevuse vähendamise partnerlus) vahel. Sisenemiskeelu teate saanud isikutel keelatakse siseneda partnerlusse kuuluvate asutuste äripindadele. Kohus vaatas läbi andmete jagamise, mis toimus avalikkuse kaitse ja kuritegevuse tõkestamise eesmärgil sõlmitud lepingu alusel, ja järeldas, et enamik andmete jagamise aspekte on seaduslikud, välja arvatud teatava tundliku teabe jagamine politsei ja partnerluse vahel. Teine näide on kohtuasi Cooper *vs.* NCA [2019] EWCA Civ 16, kus apellatsioonikohus toetas andmete jagamist politsei ja raske organiseeritud kuritegevuse tõkestamise ameti (Serious Organised Crime Agency) vahel. Raske organiseeritud kuritegevuse amet on praegu riikliku kriminaalameti alla kuuluv õiguskaitseasutus.
([206]) 2018. aasta andmekaitseseaduse paragrahvi 36 lõige 4.

kuulub isikuandmete töötlemine Ühendkuningriigi isikuandmete kaitse üldmääruse ja 2018. aasta andmekaitseseaduse 2. osa kohaldamisalasse. Nagu on täpsustatud määruse (EL) 2016/679 kohaselt vastu võetud otsuses, tagavad Ühendkuningriigi isikuandmete kaitse üldmääruses ja 2018. aasta andmekaitseseaduse 2. osas sätestatud kaitsemeetmed liidus pakutavale sisuliselt vastava kaitsetaseme ([207]).

(127) Teise stsenaariumi korral on 2008. aasta terrorismivastane seadus (Counter Terrorism Act 2008) ([208]) õiguslik alus, mis lubab kriminaalõiguskaitseasutuse kogutud andmete jagamist luureametiga riigi julgeoleku eesmärkidel. 2008. aasta terrorismivastase seaduse kohaselt võib isik anda teavet luureteenistustele nende teenistuste ülesannete täitmise, sealhulgas riigi julgeoleku eesmärgil.

(128) Riigi julgeoleku eesmärkidel andmete jagamise tingimused on sätestatud luureteenistuste seaduses (Intelligence Services Act) ja julgeolekuteenistuse seaduses (Security Service Act). Neis piiratakse luureteenistuste volitusi hankida nende seadusjärgsete ülesannete täitmiseks vajalikke andmeid. 2018. aasta andmekaitseseaduse 3. osa kohaldamisalasse kuuluvad pädevad asutused, kes soovivad jagada andmeid luureteenistustega, peavad lisaks ametite seadusjärgsetele ülesannetele arvestama luureteenistuste seaduses ja julgeolekuteenistuse seaduses sätestatud mitme teguri/piiranguga ([209]). 2008. aasta terrorismivastase seaduse paragrahvis 20 on sõnaselgelt esitatud, et 2008. aasta terrorismivastase seaduse paragrahvi 19 kohane andmete jagamine peab ikkagi vastama andmekaitsealastele õigusaktidele; see tähendab, et kohaldatakse kõiki 2018. aasta andmekaitseseaduse piiranguid ja nõudeid. Pealegi on õiguskaitseasutused ja luureteenistused 1998. aasta inimõiguste seaduse tähenduses avaliku sektori asutused ning peavad seega tagama, et nad tegutsevad vastavalt Euroopa inimõiguste konventsiooniga, sealhulgas selle artikliga 8 tagatud õigustele. Teisisõnu tähendavad need nõuded, et kogu õiguskaitseasutuste ja luureteenistuste vaheline andmete jagamine vastab andmekaitsealastele õigusaktidele ja Euroopa inimõiguste konventsioonile.

(129) Õiguskaitseasutustelt saadud või hangitud isikuandmete töötlemisele luureteenistuste poolt riigi julgeoleku eesmärkidel kohaldatakse mitut tingimust ja kaitsemeedet ([210]). 2018. aasta andmekaitseseaduse 4. osa kohaldatakse igasugusele töötlemisele luureteenistuste poolt või nimel. Selles on sätestatud peamised andmekaitse-

([207]) Komisjoni rakendusotsus, mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete piisavat kaitset Ühendkuningriigis, C(2021)4800.

([208]) 2008. aasta terrorismivastase seaduse paragrahv 19, kättesaadav aadressil https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) 1994. aasta luureteenistuste seaduse (Intelligence Service Act 1994) paragrahvi 2 lõikes 2 (vt https://www.legislation.gov.uk/ukpga/1994/13/contents) on ette nähtud, et „Luureteenistuse juht vastutab selle teenistuse tõhususe eest ja tema kohustus on tagada: a) et on kehtestatud kord, mis tagab, et luureteenistus hangib teavet ainult oma ülesannete nõuetekohaseks täitmiseks vajalikus ulatuses ning et teenistus avalikustab teavet ainult vajalikus ulatuses i) sellel eesmärgil; ii) riigi julgeoleku huvides; iii) raske kuritegevuse tõkestamise või avastamise eesmärgil või iv) kriminaalmenetluste eesmärgil, ning b) et luureteenistus ei võta meetmeid ühegi Ühendkuningriigi erakonna huvides". 1989. aasta julgeolekuteenistuse seaduse paragrahvi 2 lõikes 2 (vt https://www.legislation.gov.uk/ukpga/1989/5/contents) on aga ette nähtud, et „Peadirektor vastutab teenistuse tõhususe eest ja tema kohustus on tagada: a) et on kehtestatud kord, mis tagab, et teenistus hangib teavet ainult oma ülesannete nõuetekohaseks täitmiseks vajalikus ulatuses ning avalikustab teavet ainult sellel eesmärgil või raske kuritegevuse tõkestamise või avastamise või kriminaalmenetluste eesmärgil vajalikus ulatuses, ja b) et teenistus ei võta meetmeid ühegi erakonna huvides ning c) et on kehtestatud riikliku kriminaalameti peadirektoriga kokkulepitud kord, et kooskõlastada käesoleva seaduse paragrahvi 1 lõike 4 kohane teenistuse tegevus politseijõudude, riikliku kriminaalameti ja teiste õiguskaitseasutuste tegevusega".

([210]) Luureteenistuste volitustega seotud kaitsemeetmeid ja piiranguid reguleeritakse ka 2016. aasta uurimisvolituste seadusega (Investigatory Powers Act 2016), mis moodustab selliste volituste kasutamise õigusliku aluse koos Inglismaa, Walesi ja Põhja-Iirimaa 2000. aasta uurimisvolituste reguleerimise seaduse määrusega (Regulation of Investigatory Powers Act 2000 for England, Wales and Northern Ireland) ning Šotimaa 2000. aasta uurimisvolituste reguleerimise seaduse määrusega (Regulation of Investigatory Powers (Scotland) Act 2000 for Scotland). Need volitused ei puuduta aga andmete edasiandmist jagamise eesmärgil, sest hõlmavad vaid isikuandmete otsest kogumist luureametite poolt. Uurimisvolituste seadusega luureametitele antud volituste hindamise kohta vt komisjoni rakendusotsus, mis põhineb Euroopa Parlamendi ja nõukogu määrusel (EL) 2016/679 ning käsitleb isikuandmete piisavat kaitset Ühendkuningriigis (C(2021)4800).

põhimõtted: seaduslikkus, õiglus ja läbipaistvus, ([211]) eesmärgi piirang, ([212]) võimalikult väheste andmete kogumine, ([213]) täpsus, ([214]) säilitamise piirang ([215]) ja turvalisus, ([216]) kehtestatud tingimused eriliiki andmete töötlemisele, ([217]) nähtud ette andmesubjektide õigused, ([218]) nõutud lõimitud andmekaitset ([219]) ning reguleeritud isikuandmete rahvusvahelist edastamist ([220]).

(130) Samal ajal on 2018. aasta andmekaitseseaduse paragrahvis 110 ette nähtud vabastus 2018. aasta andmekaitseseaduse 4. osa kindlatest sätetest, kui selline vabastus on nõutav riigi julgeoleku kaitsmiseks. 2018. aasta andmekaitseseaduse paragrahvi 110 lõikes 2 on loetletud sätted, mille kohaldamisest vabastamist lubatakse. Nende hulka kuuluvad andmekaitsepõhimõtted (välja arvatud seaduslikkuse põhimõte), andmesubjekti õigused, kohustus teavitada teabevolinikku andmetega seotud rikkumisest, teabevoliniku rahvusvahelistele kohustustele vastavad kontrollivolitused, teabevoliniku teatavad täidesaatvad volitused, sätted, mille alusel on teatavad andmekaitserikkumised süüteod, ning andmete töötlemise erieesmärkidega, näiteks ajakirjanduslike, akadeemiliste või kunstiliste eesmärkidega seotud sätted. Vabastuse kohaldamise võimalikkust analüüsitakse iga juhtumi puhul eraldi ([221]). Ühendkuningriigi ametiasutuste selgituste ja Ühendkuningriigi kohtute praktika kinnituse kohaselt peab vastutav töötleja „võtma arvesse, milline on tegelik tagajärg riigi julgeolekule või kaitsele, kui ta peab järgima konkreetset andmekaitsesätet ja kui ta võib mõistlikult järgida tavaeeskirja, mõjutamata seejuures riigi julgeolekut või kaitset“ ([222]). Vabastuse kasutamise asjakohasust jälgib teabevoliniku büroo ([223]).

([211]) 2018. aasta andmekaitseseaduse paragrahvi 86 lõike 6 järgi tuleb töötlemise õigluse ja läbipaistvuse kindlaksmääramiseks vaadelda, millist meetodit kasutati andmete hankimiseks. Õigluse ja läbipaistvuse nõue on täidetud, kui andmed on saadud isikult, kes on seadusjärgselt volitatud või kellel on seadusest tulenev nõue neid anda.

([212]) 2018. aasta andmekaitseseaduse paragrahvi 87 kohaselt peavad töötlemise eesmärgid olema täpsed, selged ja õiguspärased. Andmeid ei tohi töödelda viisil, mis on vastuolus nende kogumise eesmärkidega. Artikli 87 lõike 3 kohaselt võib edasist nõuetele vastavat isikuandmete töötlemist lubada vaid siis, kui vastutaval töötlejal on seadusjärgne volitus töödelda andmeid sellisel eesmärgil ning töötlemine on vajalik ja proportsionaalne kõnealuse muu eesmärgiga. Isikuandmete töötlemist tuleks pidada nõuetele vastavaks, kui see toimub avalikes huvides arhiveerimise eesmärgil, teadus- või ajaloouuringute eesmärgil või statistilisel eesmärgil ning kohaldatakse asjakohaseid kaitsemeetmeid (2018. aasta andmekaitseseaduse paragrahvi 87 lõige 4).

([213]) Isikuandmed peavad olema piisavad ja asjakohased ega tohi olla ülemäärased (2018. aasta andmekaitseseaduse paragrahv 88).

([214]) Isikuandmed peavad olema õiged ja ajakohastatud (2018. aasta andmekaitseseaduse paragrahv 89).

([215]) Isikuandmeid ei tohi säilitada kauem kui vajalik (2018. aasta andmekaitseseaduse paragrahv 90).

([216]) Kuuenda andmekaitsepõhimõtte kohaselt tuleb isikuandmeid töödelda viisil, mis hõlmab asjakohaste turvameetmete võtmist seoses isikuandmete töötlemisega kaasnevate riskidega. Riskid hõlmavad (muu hulgas) juhuslikku või loata tutvumist isikuandmetega, isikuandmete hävimist, kadumist, kasutamist, muutmist või avalikustamist (2018. aasta andmekaitseseaduse paragrahv 91). Artiklis 107 nõutakse, et 1) iga vastutav töötleja peab rakendama asjakohaseid turvameetmeid, mis vastavad isikuandmete töötlemisega kaasnevatele riskidele, ja 2) andmete automatiseeritud töötlemise puhul rakendab iga vastutav töötleja ja volitatud töötleja riskihinnangu põhjal ennetus- või leevendusmeetmeid.

([217]) 2018. aasta andmekaitseseaduse paragrahvi 86 lõike 2 punkt b ja 10. lisa.

([218]) 2018. aasta andmekaitseseaduse 4. osa 3. peatükk, eelkõige järgmised õigused: andmetega tutvumise õigus, õigus andmete parandamisele ja kustutamisele, õigus isikuandmete töötlemine vaidlustada, õigus mitte olla automatiseeritud töötlusel põhinevate otsuste subjekt, õigus sekkuda automatiseeritud töötlusel põhinevate otsuste tegemisse ja õigus olla teavitatud otsuste tegemisest. Lisaks peab vastutav töötleja andma andmesubjektile teavet tema isikuandmete töötlemise kohta.

([219]) 2018. aasta andmekaitseseaduse paragrahv 103.

([220]) 2018. aasta andmekaitseseaduse paragrahv 109. Isikuandmeid võib edastada rahvusvahelistele organisatsioonidele või riikidele väljaspool Ühendkuningriiki, kui edastamine on vajalik ja proportsionaalne meede, mis võetakse vastutava töötleja seadusjärgsete ülesannete täitmise eesmärkidel või 1989. aasta julgeolekuteenistuse seaduse ja 1994. aasta luureteenistuste seaduse konkreetsetes paragrahvides ette nähtud muudel eesmärkidel.

([221]) Vt kohtuasi Baker *vs.* Secretary of State for the Home Department [2001] UKIT NSA2 (edaspidi „Baker vs. Secretary of State“).

([222]) Kaitse piisavuse arutelu selgitav Ühendkuningriigi raamistik, osa H: Riigi julgeolekuga seotud andmekaitse- ja uurimisvolituste raamistik, lk 15–16, kättesaadav aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Vt ka Baker *vs.* Secretary of State (vt joonealune märkus 220 eespool), milles kohus tühistas siseministri välja antud riigi julgeoleku sertifikaadi ja kinnitas riigi julgeolekuga seotud vabastuse kohaldamise, leides, et ei ole põhjust ette näha ülderandit kohustusest vastata andmetega tutvumise nõuetele ja et sellise erandi lubamine kõikidel juhtudel ilma üksikjuhtumipõhise analüüsita ületab riigi julgeoleku kaitseks vajaliku ja proportsionaalse meetme.

([223]) Vt vastastikuse mõistmise memorandum teabevoliniku büroo ja Ühendkuningriigi luureasutuste (Intelligence Community) vahel, mille kohaselt: „Kui teabevoliniku büroo saab andmesubjektilt kaebuse, veendub teabevoliniku büroo, et küsimust on korrektselt käsitletud ja vajaduse korral on nõuetekohaselt kasutatud vabastusi“ (teabevoliniku büroo ja Ühendkuningriigi luureühenduse vaheline vastastikuse mõistmise memorandum, punkt 16, kättesaadav aadressil https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Seoses võimalusega piirata eespool nimetatud õigusi riigi julgeoleku kaitseks, võib vastutav töötleja 2018. aasta andmekaitseseaduse paragrahvi 79 kohaselt taotleda sertifikaati, mille allkirjastab kabinetiminister või peaprokurör (Attorney General) ja mis kinnitab, et selliste õiguste piiramine on või teataval ajal oli vajalik ja proportsionaalne meede riigi julgeoleku kaitsmiseks ([224]). Ühendkuningriigi valitsus on esitanud 2018. aasta andmekaitseseaduse alusel suunised riigi julgeoleku sertifikaatide kohta, milles eelkõige toonitatakse, et andmesubjektide õiguste piiramine riigi julgeoleku kaitsmise nimel peab olema proportsionaalne ja vajalik ([225]). Kõik riigi julgeoleku sertifikaadid tuleb avaldada teabevoliniku büroo veebisaidil ([226]).

(132) Sertifikaat peaks kehtima kindlaksmääratud aja, maksimaalselt viis aastat, et täitevvõim selle korrapäraselt läbi vaataks ([227]). Sertifikaadis määratakse kindlaks isikuandmed või isikuandmete liigid ja 2018. aasta andmekaitseseaduse sätted, millele vabastust kohaldatakse ([228]).

(133) On oluline märkida, et riigi julgeoleku sertifikaadiga ei anta uut alust piirata andmekaitseõigusi riigi julgeoleku kaalutlustel. Teisisõnu: vastutav töötleja või volitatud töötleja võib tugineda sertifikaadile ainult siis, kui ta on järeldanud, et riigi julgeolekuga seotud vabastusele tuginemine on vajalik, ja seda tuleb kohaldada üksikjuhtumipõhiselt. Isegi kui kõnealuses küsimuses kasutatakse riigi julgeoleku sertifikaati, võib teabevoliniku büroo uurida, kas tuginemine riigi julgeolekuga seotud vabastusele oli konkreetsel juhul põhjendatud ([229]).

(134) Sertifikaadi väljastamisest otseselt mõjutatud isik võib esitada kõrgemale kohtule ([230]) sertifikaadi ([231]) kohta kaebuse või juhul, kui sertifikaadis esitatakse üldkirjelduses isikut tuvastavaid andmeid, vaidlustada sertifikaadi kohaldamise konkreetsetele andmetele ([232]).

(135) Kohus vaatab läbi sertifikaadi väljastamise otsuse ja otsustab, kas sertifikaadi väljastamiseks oli mõistlik alus ([233]). Ta võib kaaluda mitut eri aspekti, sealhulgas vajalikkus, proportsionaalsus ja seaduslikkus, võttes arvesse andmesubjektide õigustele avalduvat mõju ja leides tasakaalu riigi julgeoleku kaitsmise vajadusega. Selle tulemusena võib kohus leida, et sertifikaat ei ole seotud kaebuse esemeks olevate konkreetsete isikuandmetega ([234]).

([224]) 2018. aasta andmekaitseseadusega tunnistati kehtetuks võimalus anda sertifikaat välja 1998. aasta andmekaitseseaduse paragrahvi 28 lõike 2 alusel. Siiski on endiselt võimalik välja anda nn vanu sertifikaate, kui andmete edastamine vaidlustatakse 1998. aasta andmekaitseseaduse kohaselt (vt 2018. aasta andmekaitseseaduse 20. lisa 5. osa paragrahv 17). Seda kasutatakse siiski väga harva ja ainult teatavatel juhtudel, kui näiteks andmesubjekt vaidlustab riigi julgeolekuga seotud erandi kasutamise siis, kui avaliku sektori asutus on töödelnud isikuandmeid 1998. aasta andmekaitseseaduse kohaselt. Tuleb märkida, et sellisel juhul kohaldatakse 1998. aasta andmekaitseseaduse paragrahvi 28 tervikuna, sealhulgas on andmesubjektil võimalus sertifikaat vaidlustada. Praegu ei ole 1998. aasta andmekaitseseaduse kohaselt välja antud riigi julgeoleku sertifikaate.

([225]) Ühendkuningriigi valitsuse suunised 2018. aasta andmekaitseseadusel põhinevate 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.

([226]) 2018. aasta andmekaitseseaduse paragrahvi 130 kohaselt võib teabevoliniku büroo otsustada, et ta ei avalda sertifikaadi teksti või teatavat osa sellest, kui see oleks vastuolus riigi julgeoleku huvidega või oleks vastuolus avaliku huviga või ohustaks mõne isiku julgeolekut. Neil juhtudel avaldab teabevoliniku büroo teate selle kohta, et sertifikaat on välja antud.

([227]) Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta, punkt 15, vt joonealune märkus 225.

([228]) Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta, punkt 5, vt joonealune märkus 224.

([229]) 2018. aasta andmekaitseseaduse paragrahvis 102 nõutakse, et vastutav töötleja peab suutma tõendada, et ta on täitnud 2018. aasta andmekaitseseaduse nõuded. See tähendab, et luureteenistus peaks tõendama teabevoliniku büroole, et vabastusele tuginedes on ta arvesse võtnud juhtumi konkreetseid asjaolusid. Teabevoliniku büroo avaldab ka riigi julgeoleku sertifikaatide loetelu, mis on kättesaadav aadressil https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Kõrgem kohus on pädev kohus madalama astme halduskohtute tehtud otsuste vastu esitatud kaebuste kuulamiseks ja sellel on eripädevus teatavate valitsusorganite tehtud otsuste vastu esitatud otseste kaebuste valdkonnas.

([231]) 2018. aasta andmekaitseseaduse paragrahvi 111 lõige 3.

([232]) 2018. aasta andmekaitseseaduse paragrahvi 111 lõige 5.

([233]) Kohtuasjas Baker *vs.* Secretary of State (vt joonealune märkus 221) tühistas teabekohus (Information Tribunal) siseministri väljastatud riigi julgeoleku sertifikaadi, leides, et ei ole põhjust ette näha ülderandit kohustusest vastata andmetega tutvumise nõuetele ja et sellise erandi lubamine kõikidel juhtudel ilma üksikjuhtumipõhise analüüsita ületab riigi julgeoleku kaitseks vajaliku ja proportsionaalse meetme.

([234]) Ühendkuningriigi valitsuse suunised riigi julgeoleku sertifikaatide kohta, punkt 25, vt joonealune märkus 224.

(136) Teisi võimalikke piiranguid kohaldatakse 2018. aasta andmekaitseseaduse 11. lisa alusel sama seaduse 4. osa teatavatele sätetele, ([235]) et kaitsta muid tähtsaid üldise avaliku huvi eesmärke või huve, nagu parlamentaarne puutumatus, kutsesaladus, kohtumenetluste läbiviimine või relvajõudude võitlusjõu tõhusus. Nende sätete kohaldamisest on vabastatud teatavad teabeliigid (teabe liigi põhine) või vabastatud sellisel määral, kuivõrd nende sätete kohaldamine ohustaks tõenäoliselt kaitstavaid huve (ohupõhine) ([236]). Ohupõhiseid vabastusi võib kasutada vaid sellisel määral, kuivõrd on tõenäoline, et loetletud andmekaitse säte seab ohtu konkreetse kõnealuse huvi. Vabastuse kasutamist tuleb seepärast alati põhjendada, viidates asjakohasele ohule, mis tõenäoliselt konkreetsel juhul tekiks. Teabe liigi põhiseid vabastusi võib kasutada ainult konkreetse, kitsalt piiritletud vabastuse saanud teabeliigi puhul. Need on eesmärgilt ja mõjult sarnased mitme erandiga Ühendkuningriigi isikuandmete kaitse üldmäärusest (2018. aasta andmekaitseseaduse 2. lisas), mis omakorda sarnanevad isikuandmete kaitse üldmääruse artiklis 23 ette nähtud eranditega.

(137) Eespool esitatust ja kohtute ja teabevoliniku büroo tõlgendusest tuleneb, et Ühendkuningriigi kohaldatavates õigusnormides on kehtestatud piirangud ja tingimused, et tagada nende vabastuste ja piirangute vajalikkus ja proportsionaalsus riigi julgeoleku kaitsmiseks.

(138) 2018. aasta andmekaitseseaduse 4. osa alusel toimuvat isikuandmete töötlemist luureteenistuste poolt jälgib teabevolinik ([237]).

(139) Teabevoliniku üldised ülesanded seoses 2018. aasta andmekaitseseaduse 4. osa kohaldamisalasse kuuluvate isikuandmete töötlemisega luureteenistuste poolt on sätestatud 2018. aasta andmekaitseseaduse 13. lisas. Ülesannete hulka kuuluvad muu hulgas eelkõige 2018. aasta andmekaitseseaduse 4. osa täitmise seire ja tagamine, üldsuse teadlikkuse suurendamine, parlamendi, valitsuse ja teiste institutsioonide nõustamine seadusandlike ja haldusmeetmete valdkonnas, vastutavate töötlejate ja volitatud töötlejate teadlikkuse suurendamine nende kohustuste valdkonnas, andmesubjektidele teabe jagamine nende õiguste teostamise kohta ning uurimiste läbiviimine.

(140) Volinikul on pädevus teavitada vastutavat töötlejat 2018. aasta andmekaitseseaduse 3. osa väidetavast rikkumisest ja esitada hoiatusi selle kohta, et töötlemistoiming on tõenäoliselt vastuolus eeskirjadega, ning kui rikkumine on kinnitust leidnud, teeb volinik noomituse. Samuti võib ta esitada seaduse teatavate sätete rikkumise eest sundtäitmise teateid ja trahviteateid ([238]). Erinevalt 2018. aasta andmekaitseseaduse teistest osadest, ei saa volinik esitada hindamisteateid riigi julgeoleku kohta ([239]).

(141) 2018. aasta andmekaitseseaduse paragrahvis 110 on ette nähtud voliniku teatavate volituste kasutamise erand, kui see on nõutav riigi julgeoleku kaitse eesmärkidel. See hõlmab voliniku pädevust esitada andmekaitseseaduse alusel (igat liiki) teateid (teavitused, hindamis-, sundtäitmise ja trahviteated), volitust viia läbi kontrolle kooskõlas

([235]) Nende hulka kuuluvad i) 4. osa andmekaitsepõhimõtted, välja arvatud esimese põhimõtte alla kuuluv töötlemise seaduslikkuse nõue ja asjaolu, et töötlemine peab vastama ühele 9. ja 10. lisas sätestatud asjakohastest tingimustest, ii) andmesubjektide õigused ja iii) teabevoliniku büroole rikkumistest teatamisega seotud kohustused.

([236]) Ühendkuningriigi piisavusarutelu selgitava raamistiku kohaselt on teabe liigi põhised erandid i) teave monarhi antavate tiitlite ja autasude kohta, ii) kutsesaladus, iii) konfidentsiaalsed töö-, koolitus- või haridusalased soovitused ning iv) eksamitööd ja hinded. Ohupõhised erandid puudutavad järgmisi küsimusi: i) kuritegevuse tõkestamine või avastamine, õigusrikkujate kinnipidamine ja vastutusele võtmine, ii) parlamentaarne puutumatus, iii) kohtumenetlused, iv) monarhi relvajõudude võitlusjõu tõhusus, v) Ühendkuningriigi majanduslik heaolu, vi) läbirääkimised andmesubjektiga, vii) teadus- või ajaloouuringud või statistilised eesmärgid, viii) avalikes huvides arhiveerimine. Kaitse piisavuse arutelu selgitav Ühendkuningriigi raamistik, osa H: riigi julgeolek, lk 13, vt joonealune märkus 222.

([237]) 2018. aasta andmekaitseseaduse paragrahv 116.

([238]) 2018. aasta andmekaitseseaduse paragrahvi 149 lõike 2 ja paragrahvi 155 tõlgendamisel koostoimes võib vastutavale töötlejale või volitatud töötlejale esitada täitmisteateid ja trahviteateid rikkumiste eest, mis on seotud 2018. aasta andmekaitseseaduse 4. osa 2. peatükiga (isikuandmete töötlemise põhimõtted), 2018. aasta andmekaitseseaduse 4. osa sättega, millega antakse andmesubjektile õigused, nõudega teavitada volinikku isikuandmetega seotud rikkumisest 2018. aasta andmekaitseseaduse paragrahvi 108 alusel ning 2018. aasta andmekaitseseaduse paragrahvis 109 viidatud kolmandatele riikidele, konventsioonivälistele riikidele ja rahvusvahelistele organisatsioonidele isikuandmete edastamise põhimõtetega. (Lisateabe saamiseks sundtäitmise teadete ja trahviteadete kohta vt põhjendused 102–103).

([239]) 2018. aasta andmekaitseseaduse paragrahvi 147 lõike 6 kohaselt ei tohi teabevolinik esitada hindamisteadet 2000. aasta teabevabaduse seaduse (Freedom of Information Act 2000) paragrahvi 23 lõikes 3 viidatud organile. Nende hulka kuuluvad julgeolekuteenistus (Security service, MI5), salaluureteenistus (Secret Intelligence Service, MI6) ja valitsusside peakorter (Government Communications Headquarter).

rahvusvaheliste kohustustega, sisenemis- ja kontrollivolitust ning eeskirju süütegude kohta ([240]). Nagu selgitatud põhjenduses 136, kohaldatakse neid erandeid vaid üksikjuhtumipõhiselt ning siis, kui see on vajalik ja proportsionaalne. Erandi kohaldamist võib kohtulikult kontrollida ([241]).

(142) Teabevoliniku büroo ja Ühendkuningriigi luureteenistused on allkirjastanud vastastikuse mõistmise memorandumi, ([242]) millega loodi mitut küsimust, sealhulgas andmetega seotud rikkumiste teavitusi ja andmesubjektide kaebuste menetlemist, hõlmav koostööraamistik. Selles nähakse eelkõige ette, et kaebuse saamisel hindab teabevoliniku büroo, kas riigi julgeolekuga seotud vabastust on nõuetekohaselt kasutatud. Vastavalt Ühendkuningriigi valitsuse suunistele riigi julgeoleku sertifikaatide kohta ja andmekaitseseadusele tuleb teabevoliniku büroo päringutele kaebuste uurimise kohta vastata 20 tööpäeva jooksul, kasutades asjakohaseid turvalisi kanaleid, kui vastus sisaldab salastatud teavet. Alates 2018. aasta aprillist kuni praeguseni on teabevoliniku büroo saanud üksikisikutelt luureteenistuste kohta 21 kaebust. Iga kaebust hinnati ja tulemus edastati andmesubjektile ([243]).

(143) Luureametite poolse andmetöötluse üle teostab parlamentaarset järelevalvet ka luure- ja julgeolekukomisjon (Intelligence and Security Committee). Komisjoni õiguslik alus on 2013. aasta kohtu- ja julgeolekuseadus (Justice and Security Act 2013) ([244]). Seadusega loodi luure- ja julgeolekukomisjon Ühendkuningriigi parlamendi komisjonina. Luure- ja julgeolekukomitee koosneb parlamendi mõlema koja liikmetest, kelle määrab peaminister pärast opositsiooni juhiga konsulteerimist ([245]). Luure- ja julgeolekukomitee on kohustatud esitama parlamendile igal aastal aruande oma ülesannete täitmise kohta ja muud aruanded, mida ta peab asjakohaseks ([246]).

(144) Alates 2013. aastast on suurendatud luure- ja julgeolekukomitee volitusi, sealhulgas on komiteele antud julgeolekuteenistuste operatiivtegevuse järelevalve ülesanne. 2013. aasta kohtu- ja julgeolekuseaduse paragrahvi 2 kohaselt on luure- ja julgeolekukomitee ülesanne teostada järelevalvet riiklike julgeolekuasutuste kulude, halduse, põhimõtete ja tegevuse üle. 2013. aasta kohtu- ja julgeolekuseaduses on sätestatud, et luure- ja julgeolekukomitee võib uurida

([240]) Sätted, mille kohaldamisest võidakse vabastada: paragrahv 108 (voliniku teavitamine isikuandmetega seotud rikkumisest), paragrahv 119 (rahvusvahelistele kohustustele vastav kontroll), paragrahvid 142–154 ja 15. lisa (voliniku teated ja sisenemis- ja kontrollivolitus) ning paragrahvid 170–173 (isikuandmetega seotud rikkumised). Lisaks seoses isikuandmete töötlemisega luureteenistuste poolt 13. lisa (voliniku muud üldised ülesanded) punkti 1 alapunktid a ja g ning punkt 2.

([241]) Vt nt kohtuasi Baker *vs.* Secretary of State (vt joonealune märkus 221)

([242]) Teabevoliniku büroo ja Ühendkuningriigi luureasutuste vaheline vastastikuse mõistmise memorandum, vt joonealune märkus 231.

([243]) Seitsmel juhul soovitas teabevoliniku büroo kaebuse esitajal pöörduda andmete vastutava töötleja poole – nii tehakse, kui isik on pöördunud teabevoliniku büroo poole, kuid oleks pidanud esmalt pöörduma andmete vastutava töötleja poole. Ühel juhul andis teabevoliniku büroo andmete vastutavale töötlejale üldist nõu – kasutatakse juhul, kui vastutava töötleja tegevus ei näi olevat õigusaktidega vastuolus, kuid paremad tavad oleksid ehk ära hoidnud pöördumise teabevoliniku büroo poole. Ülejäänud 13 juhul ei pidanud andmete vastutav töötleja meetmeid võtma – kasutatakse siis, kui isiku tõstatatud probleemid kuuluvad 2018. aasta andmekaitseseaduse kohaldamisalasse, sest puudutavad isikuandmete töötlemist, kuid esitatud teabe põhjal näib, et vastutav töötleja ei ole õigusakte rikkunud.

([244]) Ühendkuningriigi ametiasutuste selgituse kohaselt laiendati kohtu- ja julgeolekuseadusega luure- ja julgeolekukomitee pädevusala, et komitee teostaks järelevalvet rohkem kui ainult luureasutuste kolme ameti üle ja et võimaldada tagasiulatuvalt jälgida ametite operatiivtegevust märkimisväärse riikliku huviga seotud küsimustes.

([245]) 2013. aasta andmekaitseseaduse paragrahv 1. Ministrid ei saa olla komitee liikmed. Luure- ja julgeolekukomitee liikmed kuuluvad komiteesse nende nimetamise aegse parlamendi ametiaja kestel. Liikme võib tagandada ta nimetanud koja resolutsiooniga või kui liige ei ole enam parlamendiliige või saab ministriks. Komitee liige võib ka tagasi astuda.

([246]) Komisjoni aruanded ja avaldused on kättesaadavad internetis aadressil http://isc.independent.gov.uk/committee-reports. 2015. aastal avaldas luure- ja julgeolekukomitee aruande „Privacy and Security: A modern and transparent legal framework“ (Privaatsus ja julgeolek: kaasaegne ja läbipaistev õigusraamistik) (vt https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), milles komitee käsitles luureametite kasutatavate seiremeetodite õigusraamistikku ja esitas mitu soovitust, mida seejärel kaaluti ja mis kaasati uurimisvolituste seaduseelnõusse (Investigatory Powers Bill), mis võeti vastu 2016. aasta uurimisvolituste seadusena. Valitsuse vastus privaatsust ja julgeolekut käsitlevale aruandele on kättesaadav aadressil https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

operatiivküsimusi, kui need ei ole seotud käimasolevate operatsioonidega ([247]). Peaministri ja luure- ja julgeolekukomitee vahel kokku lepitud vastastikuse mõistmise memorandumis ([248]) on üksikasjalikult esitatud elemendid, mida tuleb arvesse võtta, kui kaalutakse ega tegevus ei ole käimasoleva operatsiooni osa ([249]). Peaminister võib paluda, et luure- ja julgeolekukomitee uuriks ka käimasolevaid operatsioone, ja komitee võib läbi vaadata ametite vabatahtlikult esitatud teavet.

(145) 2013. aasta kohtu- ja julgeolekuseaduse 1. lisa alusel võib luure- ja julgeolekukomitee nõuda kolme luureteenistuse juhtidelt teabe avaldamist. Amet peab tegema sellise teabe kättesaadavaks, välja arvatud juhul, kui sellele paneb veto minister ([250]). Ühendkuningriigi ametiasutused on selgitanud, et tegelikult varjatakse luure- ja julgeolekukomitee eest väga vähe teavet ([251]).

(146) Seoses õiguskaitsega võib andmesubjekt 2018. aasta andmekaitseseaduse paragrahvi 165 lõike 2 alusel esitada kaebuse esmalt teabevoliniku büroole, kui ta leiab, et tema isikuandmetega seoses on rikutud 2018. aasta andmekaitseseaduse 4. osa, sealhulgas kuritarvitatud riigi julgeolekuga seotud erandeid ja piiranguid.

(147) 2018. aasta andmekaitseseaduse 4. osa alusel on isikutel ka õigus pöörduda kõrge kohtu poole (Šotimaal kõrge tsiviilkohus), et kehtestada vastutavale töötlejale korraldus austada andmetega tutvumise õigust, ([252]) töötlemise vaidlustamise õigust ([253]) ning õigust andmete parandamisele või kustutamisele.

(148) Isikutel on ka õigus nõuda vastutavalt töötlejalt või volitatud töötlejalt hüvitist 2018. aasta andmekaitseseaduse 4. osa nõude rikkumise tõttu kantud kahju eest ([254]). Kahju hõlmab nii rahalist kui ka mitterahalist kahju, näiteks kannatusi ([255]).

(149) Viimase abinõuna võib isik esitada Ühendkuningriigi luureametite või nende nimel toimunud tegevuse kohta kaebuse uurimisvolituste kohtule (Investigatory Powers Tribunal) ([256]).Uurimisvolituste kohus on loodud Inglismaa, Walesi ja Põhja-Iirimaa 2000. aasta uurimisvolituste reguleerimise seaduse ning Šotimaa 2000. aasta uurimisvolituste reguleerimise seaduse alusel ja on täitevvõimust sõltumatu ([257]). 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 kohaselt nimetab Tema Majesteet uurimisvolituste kohtu liikmed ametisse viieks aastaks.

(150) Tema Majesteet võib kohtu liikme ametist tagandada pärast mõlema parlamendikoja pöördumist ([258]) selles küsimuses ([259]).

(151) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 alusel peab isik uurimisvolituste kohtusse hagi esitamiseks („kaebeõiguse eeldus“) uskuma, et i) 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 ([260]) ja ii) et tegevus on toimunud vaidlustatavates

([247]) 2013. aasta kohtu- ja julgeolekuseaduse paragrahv 2.
([248]) Peaministri ja luure- ja julgeolekukomitee vaheline vastastikuse mõistmise memorandum, kättesaadav aadressil http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Peaministri ja luure- ja julgeolekukomitee vaheline vastastikuse mõistmise memorandum, punkt 14, vt joonealune märkus 248.
([250]) Minister võib panna teabe avalikustamisele veto vaid kahel põhjusel: teave on tundlik ja seda ei tohiks avaldada luure- ja julgeolekukomiteele riigi julgeoleku huvides või teave on sellist laadi, et kui ministril palutaks see esitada alamkoja ministeeriumi erikomisjoni ees, peaks minister asjakohaseks seda mitte teha (ka muudel kui riigi julgeolekuga seotud põhjustel). (2013. aasta kohtu- ja julgeolekuseaduse 1. lisa punkti 4 lõige 2).
([251]) Ühendkuningriigi piisavusarutelu selgitav raamistik, osa H: riigi julgeolek, lk 43.
([252]) 2018. aasta andmekaitseseaduse paragrahvi 94 lõige 11.
([253]) 2018. aasta andmekaitseseaduse paragrahvi 99 lõige 4.
([254]) 2018. aasta andmekaitseseaduse paragrahv 169, mis lubab nõudeid esitada isikul, kes kannab kahju tulenevalt andmekaitsealastes õigusaktides sätestatud nõude rikkumisest.
([255]) 2018. aasta andmekaitseseaduse paragrahvi 169 lõige 5.
([256]) Vt uurimisvolituste reguleerimise seaduse paragrahvi 65 lõike 2 punkt b.
([257]) 2000. aasta uurimisvolituste reguleerimise seaduse 3. lisa kohaselt peab liikmetel olema kohtus töötamise kogemus ja nad võidakse uuesti ametisse nimetada.
([258]) Pöördumise mõiste kohta vt joonealune märkus 183.
([259]) 2000. aasta uurimisvolituste reguleerimise seaduse 3. lisa punkti 1 alapunkt 5.
([260]) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõige 4.

oludes ([261]) või tegevuse on ellu viinud luureteenistused või see on toimunud nende nimel ([262]). Kuna „uskumise“ nõuet on tõlgendatud üsna laialt, ([263]) ei ole kaebeõiguse eeldused uurimisvolituste kohtusse hagi esitamiseks piiravad.

(152) Esitatud kaebust arutades on 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 ([264]). Kohus peab menetluses otsuse tegemisel kohaldama samu põhimõtteid, mida kasutataks kohtuliku kontrolli taotluse korral ([265]).

(153) Kohus peab teavitama kaebuse esitajat sellest, kas tema kasuks on tehtud otsus või mitte ([266]). 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67 lõigete 6 ja 7 alusel on kohtul volitus esitada vahemääruseid ja määrata selliseid hüvitisi või muid korraldusi, mida ta peab sobivaks ([267]). 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67A kohaselt võib kohtu otsuse edasi kaevata vastavalt uurimisvolituste kohtu või asjaomase apellatsioonikohtu loale.

(154) Nimelt võivad isikud esitada uurimisvolituste kohtusse hagi ja saada õiguskaitset, kui nad leiavad, et avaliku sektori asutus on tegutsenud (või kavatseb tegutseda) viisil, mis on vastuolus Euroopa inimõiguste konventsiooni kohaste õigustega, sealhulgas eraelu puutumatuse ja andmekaitse õigus, ning on seega tulenevalt 1998. aasta inimõiguste seaduse paragrahvi 6 lõikest 1 ebaseaduslik. Uurimisvolituste kohtul on inimõiguste seadusest tulenevate kõigi luureametitega seotud nõuete valdkonnas ainupädevus. Nagu on märkinud kõrge kohus, tähendab see, et „küsimuse, kas konkreetse juhtumi puhul on rikutud inimõiguste seadust, võib põhimõtteliselt tõstatada ja selle kohta otsuse langetada sõltumatu kohus, millel on juurdepääs kogu asjakohasele teabele, sealhulgas salastatud teabele. […] Selles kontekstis peame ka meeles, et nüüd on võimalus kaevata uurimisvolituste kohtu otsus edasi asjaomasesse apellatsioonikohtusse (Inglismaal ja Walesis apellatsioonikohus); ning et kõrgeim kohus otsustas hiljuti, et uurimisvolituste kohus allub põhimõtteliselt kohtulikule kontrollile: vt R (Privacy International) *vs.* Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219“ ([268]). Kui kohus leiab, et avaliku sektori asutuse tegu on ebaseaduslik, võib ta määrata oma pädevuse piires sellise hüvitise või teha sellise korralduse, mida ta peab õiglaseks ja asjakohaseks ([269]).

([261]) Sellised olud tähendavad, et avaliku sektori asutus tegutseb loa (nt teabe hankimist lubava määruse, loa/teate jms) alusel või et (olenemata sellise loa olemasolust) ei oleks tegevus olnud asjakohane ilma selle loata või vähemalt nõuetekohase kaalumiseta, kas selline luba tuleks hankida. Kohtuvoliniku (*Judicial Commissioner*) volitatud tegevust peetakse vaidlustatavates oludes toimunuks (2000. aasta uurimisvolituste reguleerimise seaduse paragrahv 65 (7ZA)), samas kui kohtuniku loa saanud tegevust ei peeta vaidlustatavates oludes toimunuks (2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 65 lõiked 7 ja 8).

([262]) 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 statistikaaruandes märgitakse, et 2016. aastal sai kohus 209 kaebust, millest 52 % peeti põhjendamatuks või pahatahtlikuks ja 25 % kohta otsust ei tehtud. Ühendkuningriigi ametiasutused selgitasid, et see tähendab kas seda, et kaebuse esitajaga seoses ei kasutatud varjatud tegevust/volitusi või et varjatud meetodeid kasutati ja kohus otsustas, et tegevus oli seaduslik. Täiendavad 11 % kaebustest leiti mitte kuuluvat kohtu alluvusse, võeti tagasi või olid kehtetud, 5 % tunnistati aegunuks ja 7 % kaebustest rahuldati. Uurimisvolituste kohtu 2016. aasta statistikaaruanne, kättesaadav aadressil https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([263]) 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).

([264]) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67 lõige 3.

([265]) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 67 lõige 2.

([266]) 2000. aasta uurimisvolituste reguleerimise seaduse paragrahvi 68 lõige 4.

([267]) See võib hõlmata korraldust hävitada avaliku sektori asutuse säilitatav teave isiku kohta.

([268]) High Court of Justice, *Liberty*, [2019] EWHC 2057 (Admin), punkt 170.

([269]) 1998. aasta inimõiguste seaduse paragrahvi 8 lõige 1.

(155) Kui riiklikud õiguskaitsevahendid on ammendatud, võib isik pöörduda Euroopa inimõiguste konventsiooniga tagatud õiguste, sealhulgas eraelu puutumatuse ja andmekaitse õiguse rikkumise asjus Euroopa Inimõiguste Kohtusse.

(156) Esitatud analüüsist ilmneb, et Ühendkuningriigi kriminaalõiguskaitseasutuste poolt käesoleva otsuse alusel edastatavate andmete jagamisele teiste avaliku sektori asutuste, sealhulgas luureametitega, kehtivad piirangud ja tingimused, mis tagavad, et andmete edasiandmine on vajalik ja proportsionaalne ning selle suhtes kohaldatakse 2018. aasta andmekaitseseaduse kohaseid andmekaitse erimeetmeid. Lisaks teostavad asjaomaste avaliku sektori asutuste poolse andmete töötlemise üle järelevalvet sõltumatud organid ja kahju kandnud isikutel on juurdepääs tõhusatele õiguskaitsevahenditele.

3. JÄRELDUS

(157) Komisjon leiab, et 2018. aasta andmekaitseseaduse 3. osa tagab liidus asuvatelt pädevatelt asutustelt Ühendkuningriigi pädevatele asutustele kriminaalõiguskaitse eesmärkidel edastatavate isikuandmete kaitse taseme, mis vastab sisuliselt direktiiviga (EL) 2016/680 tagatud kaitsetasemega.

(158) Lisaks leiab komisjon, et Ühendkuningriigi õiguses ette nähtud järelevalvemehhanismid ja õiguskaitse võimalused võimaldavad praktikas tuvastada rikkumisi ja nende eest karistada ning pakuvad andmesubjektile õiguskaitsevahendeid temaga seotud isikuandmetele juurdepääsu saamiseks ning vajaduse korral nende parandamiseks või kustutamiseks.

(159) Lisaks leiab komisjon Ühendkuningriigi õigussüsteemi kohta kättesaadava teabe põhjal, et selliste üksikisikute põhiõiguste riivamine, kelle isikuandmeid edastavad Ühendkuningriigi avaliku sektori asutused avaliku huviga seotud eesmärkidel Euroopa Liidust Ühendkuningriiki, sealhulgas õiguskaitseasutuste ja muude avaliku sektori asutuste, nagu riiklike julgeolekuorganite vahel isikuandmete jagamise kontekstis, piirdub sellega, mis on rangelt vajalik kõnealuse õiguspärase eesmärgi saavutamiseks, ning et sellise riive vastu on olemas tõhus õiguskaitse.

(160) Seetõttu tuleks otsustada, et Ühendkuningriik tagab direktiivi (EL) 2016/680 artikli 36 lõike 2 tähenduses piisava kaitsetaseme, mida tõlgendatakse põhiõiguste hartast lähtudes.

(161) Järeldus põhineb nii Ühendkuningriigi asjakohasel riigisisesel korral kui ka riigi rahvusvahelistel kohustustel, eelkõige Euroopa inimõiguste konventsiooni järgimisel ja Euroopa Inimõiguste Kohtu jurisdiktsioonile allumisel. Selliste rahvusvaheliste kohustuste järjepidev täitmine on seetõttu eriti tähtis osa käesoleva otsuse aluseks olevast hindamisest.

4. KÄESOLEVA OTSUSE MÕJU JA ANDMEKAITSEASUTUSTE TEGEVUS

(162) Liikmesriigid ja nende organid peavad võtma liidu institutsioonide aktide järgimiseks vajalikud meetmed, sest eeldatakse nende õiguspärasust ja neil on seega õiguslikud tagajärjed seni, kuni need ei ole aegunud, neid ei ole tagasi võetud, tühistamishagi menetlemise tulemusena tühistatud ega eelotsusemenetluse tulemusel või õigusvastasuse väite alusel kehtetuks tunnistatud.

(163) Seega on direktiivi (EL) 2016/680 artikli 36 lõike 3 alusel komisjoni vastu võetud kaitse piisavuse otsus siduv kõikidele otsuse adressaadiks olevate liikmesriikide organitele, sealhulgas sõltumatutele järelevalveasutustele. Eelkõige võib käesoleva otsuse kohaldamise ajal edastada andmeid liidus asuvalt vastutavalt või volitatud töötlejalt Ühendkuningriigis asuvatele vastutavatele või volitatud töötlejatele ilma, et oleks vaja taotleda lisaluba.

(164) Vastavalt direktiivi (EL) 2016/680 artikli 47 lõikele 5 ja nagu Euroopa Kohus on selgitanud Schremsi kohtuotsuses, 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 ([270]).

([270]) Schrems, punkt 65.

5. **KÄESOLEVA OTSUSE JÄRELEVALVE, PEATAMINE, KEHTETUKS TUNNISTAMINE VÕI MUUTMINE**

(165) Direktiivi (EL) 2016/680 artikli 36 lõike 4 kohaselt peab komisjon pidevalt jälgima asjakohaseid muutusi Ühendkuningriigis pärast käesoleva otsuse vastuvõtmist, et hinnata, kas Ühendkuningriik tagab endiselt sisuliselt vastava kaitsetaseme. Selline järelevalve on käesoleval juhul eriti tähtis, sest Ühendkuningriik haldab ja kohaldab uut andmekaitsekorda ja tagab selle täitmise ning selle andmekaitsekorra suhtes ei kehti enam liidu õigus ja see võib muutuda. Sellega seoses pööratakse erilist tähelepanu selliste Ühendkuningriigi õigusnormide kohaldamisele, mis käsitlevad isikuandmete edastamist kolmandatele riikidele, sealhulgas rahvusvaheliste lepingute sõlmimise kaudu, ning selle võimalikule mõjule käesoleva otsuse kohaselt edastatud andmete kaitsetasemele ja käesoleva otsuse kohaldamisalasse kuuluvate üksikisiku õiguste kasutamise tulemuslikkusele. Selleks et teostada järelevalvet, kasutab komisjon muu hulgas kohtupraktika arengu ning teabevoliniku büroo ja teiste sõltumatute asutuste järelevalve tulemusel kogutud andmeid.

(166) Selleks peaksid Ühendkuningriigi ametiasutused kiiresti ja korrapäraselt teavitama komisjoni Ühendkuningriigi õiguskorra igast sisulisest muudatusest, mis mõjutab käesolevas otsuses käsitletavat õigusraamistikku, samuti isikuandmete töötlemisega seotud ja käesolevas otsuses hinnatud tavade muudatustest, eelkõige põhjenduses 165 nimetatud aspektide osas.

(167) 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 pädevatele asutustele. Komisjoni tuleks teavitada ka võimalikest märkidest, et süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise eest vastutavate Ühendkuningriigi avaliku sektori asutuste tegevus, samuti järelevalveasutuste tegevus ei taga nõutavat kaitsetaset.

(168) 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 teavitama sellest Ühendkuningriigi pädevaid asutusi ning nõudma, et kindlaksmääratud mõistliku tähtaja jooksul, mis ei tohi olla pikem kui kolm kuud, võetakse asjakohaseid meetmeid. Vajaduse korral võib seda tähtaega pikendada teatava ajavahemiku võrra, võttes arvesse küsimuse olemust ja/või selle lahendamiseks võetavaid meetmeid.

(169) Kui Ühendkuningriigi pädevad asutused ei ole kindlaksmääratud tähtaja möödumisel neid meetmeid võtnud või muul viisil rahuldavalt tõendanud, et käesolev otsus põhineb endiselt piisaval kaitsetasemel, algatab komisjon direktiivi (EL) 2016/680 artikli 58 lõikes 2 osutatud menetluse käesoleva otsuse osaliseks või täielikuks peatamiseks või kehtetuks tunnistamiseks.

(170) Teise võimalusena algatab komisjon menetluse otsuse muutmiseks, et eelkõige kehtestada andmete edastamise lisatingimused või piirata kaitse piisavuse otsuse kohaldamisala selliselt, et selle alla kuuluks üksnes andmeedastus, mille puhul on endiselt tagatud piisav kaitsetase.

(171) Nõuetekohaselt põhjendatud, tungivalt vajalikul ja kiireloomulisel juhul kasutab komisjon võimalust võtta kooskõlas direktiivi (EL) 2016/680 artikli 58 lõikes 3 osutatud menetlusega vastu viivitamata kohaldatavad rakendusaktid, millega otsus peatatakse või tunnistatakse kehtetuks või seda muudetakse.

6. **OTSUSE KOHALDAMISE KESTUS JA PIKENDAMINE**

(172) Tuleks arvestada, 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 Euroopa Liidu õigus. See võib hõlmata muudatusi käesolevas otsuses hinnatud andmekaitseraamistikus ja muid asjakohaseid muudatusi.

(173) Seepärast on asjakohane sätestada, et käesolevat otsust kohaldatakse nelja aasta jooksul alates selle jõustumisest.

(174) 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 kohaldamisaega põhimõtteliselt veel nelja aasta võrra. Rakendusaktid käesoleva otsuse muutmiseks võetakse vastu kooskõlas direktiivi (EL) 2016/680 artikli 58 lõikes 2 osutatud menetlusega.

7. **LÕPPMÄRKUSED**

(175) Euroopa Andmekaitsenõukogu avaldas arvamuse, ([271]) mida on käesoleva otsuse koostamisel arvesse võetud.

(176) Käesoleva määrusega ette nähtud meetmed on kooskõlas direktiivi (EL) 2016/680 artikli 58 alusel loodud komisjoni arvamusega.

(177) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 21 (Ühendkuningriigi ja Iirimaa seisukoha kohta vabadusel, turvalisusel ja õigusel rajaneva ala suhtes) artikli 6a kohaselt ei ole direktiivis (EL) 2016/680 sätestatud normid isikuandmete töötlemise kohta liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. või 5. peatüki kohaldamisalasse kuuluva tegevuse puhul Iirimaa suhtes siduvad, kui Iirimaa suhtes ei ole siduvad normid, mis käsitlevad õigusalast koostööd kriminaalasjades või politseikoostööd, mille raames tuleb järgida ELi toimimise lepingu artikli 16 alusel kehtestatud sätteid. Lähtudes nõukogu rakendusotsusest (EL) 2020/1745, ([272]) tuleb direktiiv (EL) 2016/680 Iirimaal rakendada ja seda ajutiselt kohaldada alates 1. jaanuarist 2021. Järelikult on käesolev rakendusotsus Iirimaale seoses Schengeni *acquis*'ga, milles Iirimaa osaleb, siduv samadel tingimustel nagu direktiivi (EL) 2016/680 kohaldamisel Iirimaal vastavalt rakendusotsuses (EL) 2020/1745 sätestatule.

(178) ELi lepingule ja ELi toimimise lepingule lisatud protokolli nr 22 (Taani seisukoha kohta) artiklite 2 ja 2a kohaselt ei ole direktiivis (EL) 2016/680 sätestatud normid ja seega käesolev rakendusotsus Taani suhtes siduvad ning Taani suhtes ei kohaldata norme isikuandmete töötlemise kohta liikmesriikide poolt ELi toimimise lepingu kolmanda osa V jaotise 4. või 5. peatüki kohaldamisalasse kuuluva tegevuse puhul. Võttes siiski arvesse, et direktiiv (EL) 2016/680 põhineb Schengeni *acquis*'l, teatas Taani 26. oktoobril 2016 kooskõlas nimetatud protokolli artikliga 4, et on otsustanud direktiivi (EL) 2016/680 rakendada. Seega on käesolev rakendusotsus rahvusvahelise õiguse kohaselt Taani suhtes siduv.

(179) Islandi ja Norra puhul kujutab käesolev rakendusotsus Schengeni *acquis*' sätete edasiarendamist Euroopa Liidu Nõukogu ning Islandi Vabariigi ja Norra Kuningriigi vahel sõlmitud lepingu (viimase kahe riigi osalemiseks Schengeni *acquis*' sätete rakendamises, kohaldamises ja edasiarendamises) ([273]) tähenduses.

(180) Šveitsi puhul kujutab käesolev rakendusotsus Schengeni *acquis*' sätete edasiarendamist Euroopa Liidu, Euroopa Ühenduse ja Šveitsi Konföderatsiooni vahelise lepingu (Šveitsi Konföderatsiooni ühinemise kohta Schengeni *acquis*' rakendamise, kohaldamise ja edasiarendamisega) ([274]) tähenduses.

(181) Liechtensteini puhul kujutab käesolev rakendusotsus Schengeni *acquis*' sätete edasiarendamist Euroopa Liidu, Euroopa Ühenduse, Šveitsi Konföderatsiooni ja Liechtensteini Vürstiriigi vahel allakirjutatud protokolli (mis käsitleb Liechtensteini Vürstiriigi ühinemist Euroopa Liidu, Euroopa Ühenduse ja Šveitsi Konföderatsiooni vahelise lepinguga Šveitsi Konföderatsiooni ühinemise kohta Schengeni *acquis*' rakendamise, kohaldamise ja edasiarendamisega) ([275]) tähenduses,

([271]) Arvamus 15/2021 direktiivi (EL) 2016/680 kohase Euroopa Komisjoni rakendusotsuse eelnõu kohta, mis käsitleb isikuandmete piisavat kaitset Ühendkuningriigis, kättesaadav aadressil https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) Nõukogu 18. novembri 2020. aasta rakendusotsus (EL) 2020/1745, mis käsitleb andmekaitset käsitlevate Schengeni *acquis*' sätete jõustamist ning teatavate Schengeni *acquis*' sätete ajutist jõustamist Iirimaal (ELT L 393, 23.11.2020, lk 3).

([273]) EÜT L 176, 10.7.1999, lk 36.

([274]) ELT L 53, 27.2.2008, lk 52.

([275]) ELT L 160, 18.6.2011, lk 21.

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Direktiivi (EL) 2016/680 artikli 36 kohaldamisel tagab Ühendkuningriik selliste isikuandmete kaitse piisava taseme, mis edastatakse Euroopa Liidust Ühendkuningriigi avaliku sektori asutustele, kes vastutavad süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eest.

Artikkel 2

Kui liikmesriikide pädevad järelevalveasutused kasutavad isikute kaitsmiseks seoses nende isikuandmete töötlemisega direktiivi (EL) 2016/680 artikli 47 kohaseid volitusi Ühendkuningriigi avaliku sektori asutustele artiklis 1 sätestatud kohaldamisalas toimuva andmete edastamise suhtes, teavitab asjaomane liikmesriik komisjoni viivitamata.

Artikkel 3

1. Komisjon jälgib pidevalt seda, kuidas kohaldatakse käesoleva otsuse aluseks olevat õigusraamistikku, sealhulgas andmete edasisaatmisel ja üksikisiku õiguste teostamisel kohaldatavaid tingimusi, et hinnata, kas Ühendkuningriik tagab jätkuvalt piisava kaitsetaseme artikli 1 tähenduses.

2. Liikmesriigid ja komisjon teavitavad üksteist juhtudest, mil teabevolinik või muu Ühendkuningriigi pädev asutus 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.

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

Artikkel 4

Käesolev otsus kehtib kuni 27. juunini 2025, kui selle kehtivust ei pikendata direktiivi (EL) 2016/680 artikli 58 lõikes 2 osutatud korras.

Artikkel 5

Käesolev otsus on adresseeritud liikmesriikidele.

Brüssel, 28. juuni 2021

Komisjoni nimel
komisjoni liige
Didier REYNDERS