KOMISIJOS ĮGYVENDINIMO SPRENDIMAS (ES) 2021/1773

2021 m. birželio 28 d.

pagal Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje

(pranešta dokumentu Nr. C(2021) 4801)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyvą (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR ([1]), ypač į jos 36 straipsnio 3 dalį,

kadangi:

1. **ĮVADAS**

(1) Direktyvoje (ES) 2016/680 nustatytos taisyklės dėl asmens duomenų perdavimo iš Sąjungos kompetentingų institucijų trečiosioms valstybėms ir tarptautinėms organizacijoms, kai toks duomenų perdavimas patenka į direktyvos taikymo sritį. Kompetentingų institucijų vykdomo tarptautinio duomenų perdavimo taisyklės yra nustatytos Direktyvos (ES) 2016/680 V skyriuje, tiksliau – 35–40 straipsniuose. Nors asmens duomenų srautas į Europos Sąjungai nepriklausančias valstybes ir iš jų yra labai svarbus veiksmingam bendradarbiavimui teisėsaugos srityje, būtina garantuoti, kad Europos Sąjungoje užtikrinamas asmens duomenų apsaugos lygis dėl tokio duomenų perdavimo nesumažėtų ([2]).

(2) Pagal Direktyvos (ES) 2016/680 36 straipsnio 3 dalį Komisija, priimdama įgyvendinimo aktą, gali nuspręsti, kad trečioji valstybė, teritorija arba vienas ar daugiau nurodytų sektorių toje trečiojoje valstybėje, arba tarptautinė organizacija užtikrina tinkamo lygio apsaugą. Tokiu atveju perduodant asmens duomenis trečiajai valstybei jokio papildomo leidimo gauti nereikia (išskyrus tuos atvejus, kai kita valstybė narė, iš kurios gauti duomenys, turi duoti leidimą perduoti duomenis), kaip nurodyta Direktyvos (ES) 2016/680 35 straipsnio 1 dalyje ir 66 konstatuojamojoje dalyje.

(3) Kaip nurodyta Direktyvos (ES) 2016/680 36 straipsnio 2 dalyje, sprendimas dėl duomenų apsaugos tinkamumo turi būti priimamas nuodugniai išnagrinėjus trečiosios valstybės teisinę sistemą. Atlikdama vertinimą Komisija turi nustatyti, ar atitinkama valstybė garantuoja tokio lygio apsaugą, kuri yra „iš esmės lygiavertė“ Europos Sąjungoje užtikrinamai apsaugai (Direktyvos (ES) 2016/680 67 konstatuojamoji dalis). Standartas, kuriuo remiantis vertinamas „esminis lygiavertiškumas“, yra nustatytas ES teisės aktuose, visų pirma Direktyvoje (ES) 2016/680, ir Europos Sąjungos Teisingumo Teismo jurisprudencijoje ([3]). Šiuo atžvilgiu taip pat svarbią reikšmę turi Europos duomenų apsaugos valdybos tinkamumo pavyzdžiai ([4]).

(4) Kaip išaiškino Europos Sąjungos Teisingumo Teismas, pagal šią nuostatą nereikalaujama, kad apsauga būtų tokio paties lygio ([5]). Visų pirma, priemonės, kurių gali imtis atitinkama trečioji valstybė, siekdama apsaugoti asmens duomenis, gali skirtis nuo Europos Sąjungoje taikomų priemonių, jeigu šios priemonės padeda veiksmingai užtikrinti praktinę tinkamo lygio apsaugą ([6]). Todėl pagal tinkamumo kriterijų nėra reikalaujama Sąjungos taisykles atkartoti papunkčiui. Veikiau pagal šį kriterijų turi būti patikrinta, ar visoje užsienio valstybės sistemoje užtikrinamas reikiamas apsaugos lygis – teisių į privatumą esmė, veiksmingas jų įgyvendinimas, priežiūra ir įgyvendinimo užtikrinimas ([7]).

([1]) OL L 119, 2016 5 4, p. 89.
([2]) Žr. Direktyvos (ES) 2016/680 64 konstatuojamąją dalį.
([3]) Žr. naujausią Sprendimą *Maximilian Schrems / Data Protection Commissioner,* C-311/18 (toliau – Sprendimas *Schrems II*), ECLI:EU:C:2020:559.
([4]) Žr. 2021 m. vasario mėn. priimtas rekomendacijas 01/2021 dėl tinkamumo pavyzdžių pagal Teisėtvarkos direktyvą. Jas galima rasti šiuo adresu: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_en.
([5]) Sprendimas *Maximilian Schrems / Data Protection Commissioner* (toliau – Sprendimas *Schrems*), C-362/14, ECLI:EU:C:2015:650, 73 punktas.
([6]) *Schrems*, 74 punktas.
([7]) 2017 m. sausio 10 d. Komisijos komunikato Europos Parlamentui ir Tarybai „Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje“ COM(2017) 7, 3.1 skirsnis, p. 6–7; galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

(5) Komisija atidžiai išanalizavo atitinkamą Jungtinės Karalystės teisę ir praktiką. Remdamasi toliau išdėstytais nustatytais faktais, Komisija daro išvadą, kad Jungtinė Karalystė užtikrina tinkamą kompetentingų Sąjungos institucijų, kurios patenka į Direktyvos (ES) 2016/680 taikymo sritį, Jungtinės Karalystės kompetentingoms institucijoms, kurios patenka į 2018 m. Duomenų apsaugos akto (toliau – 2018 m. DAA) ([8]) 3 dalies taikymo sritį, perduodamų asmens duomenų apsaugos lygį.

(6) Pagal šį sprendimą, nepažeidžiant Direktyvos (ES) 2016/680 35 straipsnyje išdėstytų sąlygų, duomenis bus galima perduoti be reikalavimo gauti papildomą leidimą ketverius metus (su galimybe terminą pratęsti).

2. TAISYKLĖS, TAIKOMOS KOMPETENTINGOMS INSTITUCIJOMS TVARKANT ASMENS DUOMENIS BAUDŽIAMOSIOS TEISĖSAUGOS TIKSLAIS

2.1. Konstitucinė sistema

(7) Jungtinė Karalystė yra parlamentinės demokratijos valstybė. Joje veikia suverenus parlamentas – viršiausias iš visų kitų Vyriausybės institucijų, iš parlamento narių renkama ir parlamentui atskaitinga vykdomoji valdžia ir nepriklausoma teisminė valdžia. Vykdomosios valdžios įgaliojimai grindžiami išrinktų Bendruomenių rūmų pasitikėjimu ir ji yra atskaitinga abiem Parlamento rūmams (Bendruomenių rūmams ir Lordų rūmams), kurie prižiūri Vyriausybės veiklą ir svarsto bei priima įstatymus. Jungtinės Karalystės Parlamentas atsakomybę priimti teisės aktus tam tikrais Škotijos, Velso ir Šiaurės Airijos vidaus klausimais yra perdavęs Škotijos parlamentui, Velso parlamentui (*Senedd Cymru*) ir Šiaurės Airijos asamblėjai. Nors duomenų apsauga priklauso Jungtinės Karalystės parlamento kompetencijai, t. y. visoje šalyje taikomi tie patys teisės aktai, kitos su šiuo sprendimu susijusios politikos sritys yra deleguotos. Pavyzdžiui, Škotijos ir Šiaurės Airijos baudžiamosios teisėsaugos sistemų, įskaitant policijos veiklą (policijos pajėgų vykdomą veiklą), klausimai yra perduoti spręsti atitinkamai Škotijos parlamentui ir Šiaurės Airijos asamblėjai ([9]).

(8) Jungtinė Karalystė neturi kodifikuotos konstitucijos, kuri būtų įtvirtinta konstituciniame dokumente, jos konstituciniai principai vystėsi ilgą laiką ir yra kildinami iš teismų praktikos, ypač papročių. Teismai pripažino konstitucinę tam tikrų įstatymų, pvz., *Magna Carta*, 1689 m. Teisių bilio ir 1998 m. Žmogaus teisių akto, svarbą. Pagrindinės asmenų teisės, kurios yra sudedamoji konstitucijos dalis, plėtotos bendrojoje teisėje, įstatymuose ir tarptautinėse sutartyse, visų pirma, Europos žmogaus teisių konvencijoje (toliau – EŽTK), kurią Jungtinė Karalystė ratifikavo 1951 m. 1987 m. Jungtinė Karalystė taip pat yra ratifikavusi Europos Tarybos konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – 108-oji konvencija) ([10]).

(9) 1998 m. Žmogaus teisių aktu EŽTK įtvirtintos teisės perkeltos į Jungtinės Karalystės teisę. Šiuo aktu bet kuriam asmeniui suteikiamos EŽTK 2–12 ir 14 straipsniuose, jos Pirmojo protokolo 1–3 straipsniuose ir jos Tryliktojo protokolo 1 straipsnyje (skaitant juos kartu su tos EŽTK 16–18 straipsniais) nustatytos pagrindinės teisės ir laisvės. Prie šių teisių ir laisvių taip pat priskiriama teisė į privatų ir šeimos gyvenimą, kuri apima teisę į duomenų apsaugą, ir teisė į teisingą bylos nagrinėjimą ([11]). Svarbu pažymėti, kad pagal EŽTK 8 straipsnį valdžios institucija teisę į privatumą pagal įstatymą gali apriboti tik tada, kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės apsaugos ar šalies ekonominės gerovės interesams, siekiant užkirsti kelią viešosios tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti.

([8]) 2018 m. Duomenų apsaugos aktas; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([9]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento (angl. *Explanatory Framework for Adequacy Discussion*) F skirsnis „Teisėsauga“ (angl. *Law enforcement*); galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) 108-osios konvencijos principai į Jungtinės Karalystės teisę pirmą kartą perkelti 1984 m. Duomenų apsaugos aktu, vietoj kurio vėliau įsigaliojo 1998 m. DAA, o dar vėliau – 2018 m. DAA (taikomas kartu su Jungtinės Karalystės BDAR). Jungtinė Karalystė 2018 m. taip pat pasirašė Protokolą, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (dar vadinama „108+ konvencija“), o šiuo metu vykdomos Konvencijai ratifikuoti reikalingos procedūros.

([11]) EŽTK 6 ir 8 straipsniai (taip pat žr. 1998 m. Žmogaus teisių akto 1 priedą).

(10) Pagal 1998 m. Žmogaus teisių aktą bet koks valdžios institucijų veiksmas turi būti suderinamas su pagal EŽTK garantuojama teise ([12]). Be to, pirminės teisės aktai ir poįstatyminiai aktai turi būti aiškinami ir įgyvendinami su tomis teisėmis suderinamu būdu ([13]). Jeigu asmuo mano, kad valdžios institucijos pažeidė jo teises, įskaitant teises į privatumą ir duomenų apsaugą, pagal 1998 m. Žmogaus teisių aktą jis gali ginti savo teises Jungtinės Karalystės teismuose, o išnaudojęs visas nacionalines teisių gynimo priemones, dėl EŽTK garantuojamų teisių pažeidimo kreiptis į Europos žmogaus teisių teismą.

2.2. **Jungtinės Karalystės duomenų apsaugos sistema**

(11) 2020 m. sausio 31 d. Jungtinė Karalystė išstojo iš Sąjungos. Pagal Susitarimą dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės išstojimo iš Europos Sąjungos ir Europos atominės energijos bendrijos ([14]), pereinamuoju laikotarpiu iki 2020 m. gruodžio 31 d. Jungtinei Karalystei toliau taikyta Sąjungos teisė. Iki išstojimo ir pereinamuoju laikotarpiu asmens duomenų apsaugos teisės normas, kuriomis buvo reglamentuojamas asmens duomenų tvarkymas Jungtinės Karalystės kompetentingose institucijose nusikalstamų veikų prevencijos, tyrimo, atskleidimo arba baudžiamojo persekiojimo už jas tikslais, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir tų grėsmių prevenciją, Jungtinėje Karalystėje sudarė atitinkamos 2018 m. Duomenų apsaugos akto nuostatos, kuriomis į nacionalinę teisę perkelta Direktyva (ES) 2016/680.

(12) Rengdamasi išstojimui iš ES, Jungtinės Karalystės Vyriausybė priėmė 2018 m. Išstojimo iš Europos Sąjungos aktą ([15]) (toliau – Išstojimo iš ES aktas), kuriuo tiesiogiai taikytini Sąjungos teisės aktai buvo perkelti į Jungtinės Karalystės teisę ir buvo nustatyta, kad pagal ES teisę priimtos vidaus teisės normos galios ir pereinamajam laikotarpiui pasibaigus. 2018 m. DAA ([16]), kuriuo į nacionalinę teisę perkelta Direktyva (ES) 2016/680, 3 dalis pagal Išstojimo iš ES aktą yra laikoma pagal ES teisę priimtomis vidaus teisės normomis. Remiantis Išstojimo iš ES aktu, pagal ES teisę priimtas ir nepakeistas vidaus teisės normas Jungtinės Karalystės teismai privalo aiškinti atsižvelgdami į atitinkamą Europos Sąjungos Teisingumo Teismo (toliau – Teisingumo Teismas) jurisprudenciją ir bendruosius Sąjungos teisės principus, kurie galiojo prieš pat pereinamojo laikotarpio pabaigą (atitinkamai vadinama „palikta galioti ES jurisprudencija“ ir „palikti galioti bendrieji ES teisės principai“) ([17]).

(13) Pagal Išstojimo iš ES aktą Jungtinės Karalystės ministrai turi įgaliojimus įstatyminiais dokumentais priimti antrinės teisės aktus ir jais, atsižvelgdami į Jungtinės Karalystės išstojimo iš Sąjungos pasekmes, atlikti būtinus paliktos galioti ES teisės pakeitimus. Šiais įgaliojimais jie naudojasi pagal 2019 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (su pakeitimais) (išstojimo iš ES) taisykles (toliau – DAPER taisyklės) ([18]). Jomis Jungtinės Karalystės duomenų apsaugos teisės aktai, įskaitant 2018 m. DAA, buvo iš dalies pakeisti, kad atitiktų šalies vidaus aplinkybes ([19]).

([12]) 1998 m. Žmogaus teisių akto 6 straipsnis.

([13]) 1998 m. Žmogaus teisių akto 3 straipsnis.

([14]) Susitarimas dėl Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės išstojimo iš Europos Sąjungos ir Europos atominės energijos bendrijos 2019/C 384 I/01, XT/21054/2019/INIT (OL C 384 I, 2019 11 12, p. 1) (toliau – Susitarimas dėl išstojimo); galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=LT.

([15]) 2018 m. Išstojimo iš Europos Sąjungos aktas; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/16/contents.

([16]) 2018 m. Duomenų apsaugos aktas; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/12/contents.

([17]) 2018 m. Išstojimo iš ES akto 6 straipsnis.

([18]) 2019 m. Duomenų apsaugos, privatumo ir elektroninių ryšių (su pakeitimais) (išstojimo iš ES) taisyklės (galima rasti šiuo adresu: https://www.legislation.gov.uk/uksi/2019/419/contents/made), iš dalies pakeistos 2020 m. DAPER taisyklėmis, kurias galima rasti šiuo adresu: https://www.legislation.gov.uk/ukdsi/2020/9780348213522.

([19]) Išstojimo taisyklėmis padaryta keletas 2018 m. DAA 3 dalies pakeitimų. Didelė dalis šių pakeitimų yra techninio pobūdžio, pavyzdžiui, išbraukta vartota sąvoka „valstybė narė“, nuorodos į „Teisėsaugos direktyvą“ (pvz., žr. 2018 m. DAA 48 straipsnio 8 dalį arba 73 straipsnio 5 dalies a punktą dėl „vidaus teisės“), kad, pasibaigus pereinamajam laikotarpiui, 3 dalis faktiškai būtų taikoma kaip vidaus teisės aktas. Kai kur buvo reikalingi kitokio pobūdžio pakeitimai, pavyzdžiui, susiję su tuo, „kas“ Jungtinės Karalystės duomenų apsaugos teisės aktų sistemoje priima „sprendimus dėl tinkamumo“ (žr. 2018 m. DAA 74A straipsnį), t. y. juos priima ne Europos Komisija, bet valstybės sekretorius.

(14) Todėl teisiniai standartai, taikomi duomenų tvarkymui kompetentingose institucijose baudžiamųjų veikų prevencijos, tyrimo, atskleidimo, patraukimo baudžiamojon atsakomybėn už jas arba baudžiamųjų sankcijų vykdymo tikslais, įskaitant apsaugą nuo grėsmių Jungtinės Karalystės visuomenės saugumui ir tų grėsmių prevenciją, pagal Išstojimo susitarimą po pereinamojo laikotarpio bus išdėstyti atitinkamose DAPER taisyklėmis iš dalies pakeistose 2018 m. DAA dalyse, visų pirma – 3 dalyje. Jungtinės Karalystės bendrasis duomenų apsaugos reglamentas (toliau – Jungtinės Karalystės BDAR) tokiam duomenų tvarkymui netaikomas.

(15) 2018 m. DAA 3 dalyje išdėstytos asmens duomenų tvarkymo baudžiamosios teisėsaugos tikslais taisyklės, įskaitant duomenų apsaugos principus, teisinius duomenų tvarkymo pagrindus (teisėtumą), duomenų subjektų teises, kompetentingų institucijų, atliekančių duomenų valdytojų funkcijas, prievoles ir tolesnio duomenų perdavimo apribojimus. O teisėsaugos sektoriui taikytinos taisyklės dėl priežiūros, vykdymo užtikrinimo ir žalos atlyginimo yra išdėstytos 2018 m. DAA 5 ir 6 dalyse.

(16) Be to, turint galvoje atitinkamą policijos pajėgoms tenkantį vaidmenį teisėsaugos sektoriuje, reikėtų atsižvelgti į policijai taikomas taisykles. Kadangi policijos funkcijos yra deleguotos, a) Anglijos ir Velso, b) Škotijos ir c) Šiaurės Airijos policijai taikomi skirtingi teisės aktai, nors jų turinys dažnai yra panašus ([20]). Papildomi paaiškinimai, kaip turėtų būti naudojamasi policijai suteiktais įgaliojimais, išdėstyti įvairaus pobūdžio gairėse. Politikos gairės yra trijų pagrindinių formų: 1) pagal teisės aktus paskelbtos įstatyminės gairės, pavyzdžiui, Etikos kodeksas ([21]) ir Policijos informacijos valdymo praktikos kodeksas (toliau – PIV praktikos kodeksas) ([22]); paskelbti pagal 1996 m. Policijos aktą ([23]), arba kodeksai ([24]), paskelbti pagal Policijos ir baudžiamųjų įrodymų aktą ([25]); 2) Policijos koledžo paskelbtas Policijos informacijos valdymo leistinos profesinės praktikos aprašas (Policijos informacijos valdymo LPP aprašas) ([26]) ir 3) operatyvinės gairės (jas skelbia pati policija). Nacionalinė policijos vadovų taryba (visų Jungtinės Karalystės policijos pajėgų koordinavimo institucija) skelbia operatyvines gaires, kurias visos policijos pajėgos turi patvirtinti, todėl jos yra taikomos nacionaliniu lygiu ([27]). Šių gairių paskirtis – užtikrinti, kad visose pajėgose informacija būtų valdoma vienodai ([28]).

(17) PIV praktikos kodeksą 2005 m. paskelbė valstybės sekretorius, naudodamasis pagal 1996 m. Policijos akto ([29]) 39A straipsnį suteiktais įgaliojimais. Bet kurį pagal Policijos aktą skelbiamą kodeksą turi tvirtinti valstybės sekretorius, o prieš teikiant jį Parlamentui, dėl jo turi būti konsultuojamasi su Nacionaline nusikaltimų agentūra.

([20]) Daugiau informacijos apie Jungtinės Karalystės policijos pajėgas ir jų įgaliojimus galima rasti diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento F skirsnyje „Teisėsauga“ (žr. 9 išnašą).

([21]) Anglijos ir Velso Policijos profesinio elgesio principų ir standartų praktikos kodeksas, kurį galima rasti šiuo adresu: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf, Šiaurės Airijos policijos tarnybos etikos kodeksas, kurį galima rasti šiuo adresu: https://www.nipolicingboard.org.uk/psni-code-ethics; Škotijos policijos etikos kodeksas, kurį galima rasti šiuo adresu: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Policijos informacijos valdymo praktikos kodeksas; galima rasti šiuo adresu: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) 1996 m. Policijos aktas, kurį galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Pagal 1984 m. Policijos ir baudžiamųjų įrodymų aktą paskelbti praktikos kodeksai; galima rasti šiuo adresu: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) 1984 m. Policijos ir baudžiamųjų įrodymų aktas; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Policijos informacijos valdymo leistinos profesinės praktikos aprašas; galima rasti šiuo adresu: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Policijos duomenų apsaugos specialistams skirtas duomenų apsaugos vadovas; galima rasti adresu: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Pavyzdžiui, PIV praktikos kodeksas (žr. 22 išnašą) yra taikomas policijos informacijos saugojimui operatyviniais tikslais (žr. šio sprendimo 47 konstatuojamąją dalį).

([29]) Remiantis Jungtinės Karalystės institucijų pateikta informacija, derybų dėl tinkamumo laikotarpiu Policijos koledžas rengė Įrašų valdymo praktikos kodeksą, kuris turėtų įsigalioti vietoj Policijos informacijos valdymo praktikos kodekso. Kodekso projektas viešoms konsultacijoms paskelbtas 2021 m. sausio 25 d., jį galima rasti šiuo adresu: https://www.college.police.uk/article/information-records-management-consultation.

Policijos akto 39A straipsnio 7 dalyje reikalaujama, kad policija deramai laikytųsi pagal šį aktą paskelbtų kodeksų, todėl policija turėtų šio kodekso laikytis ([30]). Be to, neįstatyminės gairės (Policijos informacijos valdymo LPP aprašas) visais atvejais privalo atitikti teisiškai viršesnį PIV praktikos kodeksą ([31]). Bet kuriuo atveju, nors tam tikrų operatyvinių atvejų, kai policijos pareigūnams reikės nukrypti nuo šių gairių, gali pasitaikyti, policijos pareigūnai vis tiek turi laikytis 2018 m. DAA 3 dalies ([32]).

(18) Išsamesnes gaires dėl Jungtinės Karalystės duomenų apsaugos teisės aktų, pagal kuriuos duomenys yra tvarkomi teisėsaugos sektoriuje, yra parengęs informacijos komisaras ([33]) (daugiau informacijos apie informacijos komisarą pateikta 93–109 konstatuojamosiose dalyse). Nors gairės nėra teisiškai privalomos, teismai turėtų atsižvelgti į visus jų pažeidimus, nes tam tenka aiškinamasis vaidmuo ir tai parodo, kaip komisaras aiškina duomenų apsaugos gaires ir užtikrina jų vykdymą praktiškai ([34]).

(19) Galiausiai pažymėtina, kad, kaip nurodyta 8–10 konstatuojamosiose dalyse, Jungtinės Karalystės teisėsaugos agentūros privalo užtikrinti, kad būtų laikomasi (EŽTK) ir 108-osios konvencijos.

(20) Pagal struktūrą ir pagrindines sudedamąsias dalis duomenų tvarkymą Jungtinės Karalystės baudžiamosios teisėsaugos institucijose reglamentuojantys teisės aktai yra labai panašūs į taikomus ES. Taip pat pažymėtina, kad šią teisinę sistemą sudaro ne tik pagal ES teisę suformuotos vidaus teisės normos, bet ir tarptautinėje teisėje nustatyti įpareigojimai, kurių Jungtinė Karalystė laikosi, visų pirma, pagal EŽTK ir 108-ąją konvenciją bei paklusdama Europos Žmogaus Teisių Teismo jurisdikcijai. Tad šie įpareigojimai, kylantys iš teisiškai privalomų tarptautinių dokumentų, visų pirma susijusių su asmens duomenų apsauga, yra ypač svarbus šiame sprendime vertinamos teisinės sistemos aspektas.

2.3. **Materialinė ir teritorinė taikymo sritis**

(21) 2018 m. DAA 3 dalies materialinė taikymo sritis sutampa su Direktyvos (ES) 2016/680 2 straipsnio 2 dalyje nurodyta taikymo sritimi. 3 dalis taikoma kompetentingos institucijos vykdomam asmens duomenų tvarkymui visiškai arba iš dalies automatizuotomis priemonėmis ir kompetentingos institucijos vykdomam asmens duomenų, kurie sudaro arba yra skirti sudaryti susisteminto rinkinio dalį, tvarkymui neautomatizuotomis priemonėmis.

(22) Be to, tam, kad duomenų tvarkymas patektų į 3 dalies taikymo sritį, duomenų valdytojas turi būti „kompetentinga institucija“, o duomenys turi būti tvarkomi „teisėsaugos tikslu“. Todėl šiame sprendime vertinama duomenų apsaugos tvarka taikoma visai šių kompetentingų institucijų veiklai teisėsaugos srityje.

(23) Pagal DAA 30 straipsnyje pateiktą apibrėžtį „kompetentinga institucija“ yra laikomas 2018 m. DAA 7 priede nurodytas asmuo ir bet kuris kitas asmuo, kuris vykdo įstatymuose nustatytas funkcijas bet kuriuo iš teisėsaugos tikslų. Prie 7 priede išvardytų kompetentingų institucijų priskiriamos ne tik policijos pajėgos, bet ir visi Jungtinės Karalystės Vyriausybės ministerijų departamentai ir kitos tyrimų funkcijas vykdančios institucijos (pvz., Jos Didenybės mokesčių ir muitų komisaras, Velso mokesčių institucija, Konkurencijos ir rinkų institucija, Jos Didenybės žemės registras ir Nacionalinė nusikaltimų agentūra), prokuratūros tarnybos, kitos baudžiamojo

([30]) Sprendime *R* / *Commission of Police of the Metropolis* [2014] EWCA Civ 585, buvo patvirtintas Policijos informacijos valymo praktikos kodekso teisinis statutas, o lordas teisėjas konstatavo, kad pagal 1996 m. Policijos akto 39A straipsnį Londono policijos komisaras privalo laikytis Policijos informacijos valdymo kodekso ir Policijos informacijos valdymo LPP.

([31]) Tai, kaip policija laikosi PIV praktikos kodekso, tikrina Jos Didenybės konsteblių inspekcija ir priešgaisrinė bei gelbėjimo tarnyba).

([32]) Šiuo atžvilgiu žr. Policijos koledžo poziciją dėl LPP gairių visais policijos veiklos aspektais laikymosi, kurioje paaiškinama, kad „LPP parengė profesinė policijos institucija (Policijos koledžas) ir tai yra oficialus policijos profesinės praktikos dokumentas. Policijos pareigūnai ir darbuotojai vykdydami savo pareigas turėtų laikytis LPP. Tačiau gali susiklostyti aplinkybių, kai Pajėgos dėl teisėtų operatyvinių priežasčių, kai tam bus akivaizdus pagrindas, turės nukrypti nuo LPP. Pajėgos turėtų prisiimti atsakomybę už visą vietos ir nacionalinę riziką, kuri kyla, kai veikla vykdoma ne pagal nacionaliniu lygiu suderintas gaires, o jei dėl to kyla incidentų arba pradedamas tyrimas (pavyzdžiui, jį atlieka Nepriklausoma policijos valdymo tarnyba), už visą riziką atsako Pajėgos.“; galima rasti adresu https://www.app.college.police.uk/faq-page/.

([33]) Duomenų tvarkymo teisėsaugos srityje gairės; galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Žr. Sprendimą *Bridges* / *Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), kuriame Aukštasis teismas pripažino, kad Komisaro gairės neturi įstatymo galios, tačiau konstatavo, kad „nagrinėdamas, ar duomenų valdytojas laikėsi 64 straipsnyje nustatytos pareigos [atlikti poveikio duomenų apsaugai vertinimą, kai duomenų tvarkymas yra susiję su didele rizika], Teismas atsižvelgs į informacijos komisaro paskelbtas gaires dėl poveikio duomenų apsaugai vertinimų“.

teisingumo tarnybos ir kitos teisėsaugos veiklą vykdančios įstaigos ar organizacijos ([35]). 2018 m. DAA 3 dalis taip pat yra taikoma teismams ir specialiesiems teismams, kai šie vykdo teismines funkcijas, išskyrus nuostatas dėl duomenų subjekto teisių ir dėl informacijos komisaro priežiūros ([36]). 7 priede pateiktas kompetentingų institucijų sąrašas nėra baigtinis; valstybės sekretorius, atsižvelgdamas į valstybės institucijų organizacinės struktūros pokyčius, gali jį papildyti priimdamas taisykles ([37]).

(24) Taip pat pažymėtina, kad atitinkamas duomenų tvarkymas turi būti atliekamas „teisėsaugos tikslu“, kuris apibrėžiamas kaip nusikalstamų veikų prevencija, tyrimas, atskleidimas, baudžiamasis persekiojimas už jas arba baudžiamųjų sankcijų vykdymas, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją ([38]). Kompetentingų institucijų ne teisėsaugos tikslais vykdomo duomenų tvarkymo 2018 m. DAA 3 dalis nereglamentuoja. Pavyzdžiui, ši dalis netaikoma, kai Konkurencijos ir rinkų institucija tiria bylas, kurios nėra laikomos baudžiamosiomis (pvz. įmonių susijungimo bylas). Tais atvejais, kai kompetentingos institucijos asmens duomenis tvarko kitais, ne teisėsaugos, tikslais, taikomas Jungtinės Karalystės BDAR kartu su 2018 m. DAA 2 dalimi. Norėdama nustatyti, kurios duomenų apsaugos nuostatos (2018 m. DAA 3 ar 2 dalis) yra taikomos konkrečiu atveju tvarkant asmens duomenis, kompetentinga institucija, t. y. duomenų valdytojas, privalo atsižvelgti į tai, ar „pagrindinis“ duomenų tvarkymo tikslas yra vienas iš 2018 m. DAA nurodytų teisėsaugos tikslų.

(25) Dėl 2018 m. DAA 3 dalies teritorinės taikymo srities pažymėtina, kad 207 straipsnio 2 dalyje yra nurodyta, jog DAA yra taikomas asmens duomenų tvarkymui, susijusiam su verslo vietą turinčio asmens veikla, visoje Jungtinės Karalystės teritorijoje. Tai yra, minėtos dalies nuostatos taikomos visoms Anglijos, Velso, Škotijos ir Šiaurės Airijos institucijoms, kurios patenka į 2018 m. DAA 3 dalies materialinę taikymo sritį ([39]).

2.3.1. *Asmens duomenų apibrėžtis ir asmens duomenų tvarkymas*

(26) Pagrindinės asmens duomenų ir jų tvarkymo sąvokos yra apibrėžtos 2018 m. DAA 3 straipsnyje ir yra vartojamos visame DAA. Šių sąvokų apibrėžtys yra labai panašios į atitinkamas Direktyvos (ES) 2016/680 3 straipsnyje pateiktas apibrėžtis. Pagal 2018 m. DAA asmens duomenys yra bet kokia informacija apie gyvą fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti ([40]). Pagal 2018 m. DAA 3 straipsnio 3 dalį yra laikoma, kad asmens tapatybę galima nustatyti, jeigu jo tapatybę tiesiogiai arba netiesiogiai galima nustatyti iš turimos informacijos, visų pirma pagal vardą, pavardę, identifikatorių arba pagal vieną ar kelis to asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius. Pagal apibrėžtį „duomenų tvarkymas“ yra bet kokia su informacija ar informacijos rinkiniu atliekama operacija arba operacijų grupė, pavyzdžiui, a) rinkimas, įrašymas, rūšiavimas, sisteminimas ar saugojimas; b) adaptavimas ar keitimas; c) išgavimas, susipažinimas ar naudojimas; d) atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę naudotis informacija; e) sugretinimas ar sujungimas arba f) apribojimas, ištrynimas arba sunaikinimas. Akte taip pat apibrėžiama, kad „neskelbtinų duomenų tvarkymas“ yra „a) asmens duomenų, kuriais atskleidžiama rasė arba etninė kilmė, politinės pažiūros, religiniai ar filosofiniai įsitikinimai ar narystė profesinėje sąjungoje, tvarkymas; b) genetinių arba biometrinių duomenų tvarkymas asmens tapatybei tiksliai nustatyti; c) sveikatos duomenų tvarkymas; d) asmens seksualinio gyvenimo arba seksualinės orientacijos duomenų tvarkymas“ ([41]). Šiuo tikslu 2018 m. DAA 205 straipsnyje pateiktos sąvokų „biometriniai duomenys ([42])“, „sveikatos duomenys“ ([43]) ir „genetiniai duomenys“ ([44]) apibrėžtys.

([35]) 2018 m. DAA 7 priede pateiktą sąrašą, be kitų subjektų, įtraukti Prokuratūrų direktoriai, Šiaurės Airijos prokuratūrų direktorius ir informacijos komisaras.

([36]) 2018 m. DAA 43 straipsnio 3 dalis.

([37]) 2018 m. DAA 30 straipsnio 3 dalis. Žvalgybos tarnybos (Slaptoji žvalgybos tarnyba, Saugumo tarnyba ir Vyriausybės komunikacijos centras) nelaikomos kompetentingomis institucijomis (žr. DAA 30 straipsnio 2 dalį), todėl 2018 m. DAA 3 dalis jokiai jų veiklai netaikoma. Jų veiklai taikoma 2018 m. DAA 4 dalis.

([38]) 2018 m. DAA 31 straipsnis.

([39]) Tai reiškia, kad 2018 m. DAA, taigi ir šis sprendimas, netaikomi Jungtinės Karalystės Karūnos priklausiniams ir kitoms Jungtinės Karalystės užjūrio teritorijoms, pavyzdžiui, Folklando saloms ir Gibraltaro teritorijai.

([40]) Mirusio asmens duomenys nepatenka į 2018 m. DAA taikymo sritį.

([41]) 2018 m. DAA 35 straipsnio 8 dalis.

([42]) Biometriniai duomenys – po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, pvz., veido atvaizdai arba daktiloskopiniai duomenys.

([43]) Sveikatos duomenys – asmens duomenys, susiję su fizine ar psichine fizinio asmens sveikata, įskaitant duomenis apie sveikatos priežiūros paslaugų teikimą, atskleidžiantys informaciją apie to fizinio asmens sveikatos būklę.

([44]) Genetiniai duomenys – asmens duomenys, susiję su paveldėtomis ar įgytomis fizinio asmens genetinėmis savybėmis, suteikiančiomis unikalios informacijos apie to fizinio asmens fiziologiją ar sveikatą, ir kurie gauti visų pirma analizuojant biologinį atitinkamo fizinio asmens mėginį.

(27) 2018 m. DAA 32 straipsnyje paaiškinta, ką tvarkant asmens duomenis teisėsaugos tikslais reiškia sąvokos „duomenų valdytojas“ ir „duomenų tvarkytojas“ ir šie paaiškinimai yra labai panašūs į atitinkamas Direktyvoje (ES) 2016/680 pateiktas apibrėžtis. Duomenų valdytojas – tai kompetentinga institucija, kuri nustato asmens duomenų tvarkymo tikslus ir priemones. Jeigu duomenų tvarkymas yra reikalaujamas pagal įstatymą, duomenų valdytojas yra kompetentinga institucija, kuriai pavesta tai daryti pagal tą įstatymą. Duomenų tvarkytojas yra bet kuris asmuo, tvarkantis asmens duomenis duomenų valdytojo vardu (išskyrus asmenį, kuris yra duomenų valdytojo darbuotojas).

2.4. **Apsaugos priemonės, teisės ir prievolės**

2.4.1. *Duomenų tvarkymo teisėtumas ir sąžiningumas*

(28) Pagal 2018 m. DAA 35 straipsnį, panašiai kaip pagal Direktyvos (ES) 2016/680 4 straipsnio 1 dalies a punktą, yra reikalaujama, kad asmens duomenys būtų tvarkomi teisėtai ir sąžiningai. Pagal 2018 m. DAA 35 straipsnio 2 dalį asmens duomenų tvarkymas bet kuriuo teisėsaugos tikslu yra teisėtas tik tada, jeigu yra grindžiamas įstatymu ir jeigu duomenų subjektas sutiko, kad jo duomenys būtų tvarkomi tuo tikslu, arba duomenis tvarkyti būtina tam, kad kompetentinga institucija galėtų atlikti tuo tikslu vykdomą užduotį.

2.4.1.1. Įstatymu grindžiamas duomenų tvarkymas

(29) Panašiai kaip pagal Direktyvos (ES) 2016/680 8 straipsnį, tam, kad duomenų tvarkymas, patenkantis į 2018 m. DAA 3 dalies taikymo sritį, būtų teisėtas, jis turi būti grindžiamas įstatymu. Teisėtas duomenų tvarkymas – duomenų tvarkymas, kuris yra leidžiamas pagal įstatymą, bendrąją teisę arba karališkąsias prerogatyvas ([45]).

(30) Kompetentingų institucijų įgaliojimai dažniausiai reglamentuojami įstatymais, taigi, yra aišku, kad jų funkcijos ir įgaliojimai yra nustatomi Parlamento priimamuose teisės aktuose ([46]). Tam tikrais atvejais policija ir kitos 2018 m. DAA 7 priede nurodytos kompetentingos institucijos gali tvarkyti duomenis pagal bendrosios teisės normas ([47]). Bendrosios teisės pagrindą sudaro teismų sprendimais sukurti precedentai. Bendroji teisė yra svarbi, kai kalbama apie policijos įgaliojimus, kuriais ji naudojasi vykdydama pagrindinę šiame teisės šaltinyje įtvirtintą policijos pareigą ginti visuomenę aiškinantis nusikaltimus ir užkertant jiems kelią ([48]). Tačiau, vykdydama šią pareigą, policija vadovaujasi tiek bendrojoje

([45]) 2018 m. DAA aiškinamųjų pastabų 181 dalis; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Pavyzdžiui, Nacionalinės nusikaltimų agentūros įgaliojimai įtvirtinti 2013 m. Nusikaltimų ir teismų akte; jį galima rasti adresu https://www.legislation.gov.uk/ukpga/2013/22/contents. Atitinkamai Maisto standartų agentūros įgaliojimai yra nustatyti 1999 m. maisto standartų akte; jį galima rasti šiuo adresu https://www.legislation.gov.uk/ukpga/1999/28/contents. Kiti pavyzdžiai – 1985 m. Nusikaltėlių traukimo baudžiamojon atsakomybėn aktas, pagal kurį įsteigta Karališkoji prokuratūra (žr. https://www.legislation.gov.uk/ukpga/1985/23/contents), 2005 m. Mokesčių ir muitų komisarų aktas, pagal kurį įsteigta Jos Didenybės mokesčių ir muitų tarnyba (žr. https://www.legislation.gov.uk/ukpga/2005/11/contents), 1995 m. Baudžiamojo proceso (Škotija) aktas, pagal kurį įsteigta Škotijos baudžiamųjų bylų peržiūros komisija (žr. https://www.legislation.gov.uk/ukpga/1995/46/contents), 2002 m. Teisingumo (Šiaurės Airija) aktas, pagal kurį įsteigta Šiaurės Airijos prokuratūra (žr. Https://www.legislation.gov.uk/ukpga/2002/26/contents)), pagal 1987 m. Baudžiamojo teisingumo aktą įsteigtas Sunkių sukčiavimo nusikaltimų biuras ir šiam biurui suteikti įgaliojimai (žr. https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Pavyzdžiui, remiantis Jungtinės Karalystės institucijų pateikta informacija, Karališkojoje prokuratūroje ir prokurorų tarnyboje, atsakingoje už Škotijoje iškeltų bylų tyrimą, Škotijos prokuratūros sistemai vadovaujančio Lordo advokato įgaliojimai tirti mirtis ir vykdyti baudžiamąjį persekiojimą už nusikaltimus yra įtvirtinti bendrojoje teisėje, o kai kurios funkcijos nustatytos įstatyme. Be to, Karūnos ir pagal analogiją įvairių Vyriausybės įstaigų, departamentų ir ministrų įgaliojimai kyla tiek iš teisės aktų, tiek iš bendrosios teisės, tiek iš karališkųjų prerogatyvų (tai – Karūnai pagal bendrąją teisę suteikti įgaliojimai, kuriuos vykdo ministrai).

([48]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento F skirsnis „Teisėsauga“, p. 8 (žr. 9 išnašą).

teisėje, tiek kituose teisės aktuose nustatytais įgaliojimais ([49]). Pagal įstatymą suteikti policijos įgaliojimai yra viršesni už bendrojoje teisėje įtvirtintus įgaliojimus ([50]).

(31) Teismai pripažino, kad bendrojoje teisėje įtvirtinti policijos pareigūno įgaliojimai ir pareigos apima „visus veiksmus, kurie jam atrodo reikalingi, kad būtų išsaugota taika, nusikaltimų prevencija ir turto apsauga nuo žalos dėl nusikalstamos veikos“ ([51]). Bendrojoje teisėje nustatyti įgaliojimai nėra besąlyginiai. Jiems taikomi įvairūs apribojimai, tarp jų – teismų ([52]) ir teisės aktuose, visų pirma 1998 m. Žmogaus teisių akte ir 2010 m. Lygybės akte ([53]), nustatyti apribojimai. Be to, tais atvejais, kai kompetentingos institucijos tvarko duomenis pagal 2018 m. DAA 3 dalį, vykdant bendrojoje teisėje įtvirtintus įgaliojimus būtina nuosekliai laikytis 2018 m. DAA nustatytų reikalavimų ([54]). Priimant sprendimą vykdyti kokio nors pobūdžio duomenų tvarkymo operacijas, būtina atsižvelgti į taikytinose gairėse, pavyzdžiui, PIV praktikos kodekse ir konkrečiai kuriai nors iš Jungtinės Karalystės šalių taikomose gairėse nustatytus reikalavimus ([55]). Vyriausybės ir operatyvinės policijos tarnybos yra parengusios įvairių gairių, kuriomis siekiama užtikrinti, kad vykdydami savo įgaliojimus policijos pareigūnai laikytųsi bendrojoje teisėje arba atitinkamuose įstatymuose nustatytų apribojimų ([56]).

(32) Karališkosios prerogatyvos yra dar viena teisės sudedamoji dalis; tai – tam tikri Karūnai suteikti įgaliojimai, kuriuos vykdo vykdomosios valdžios institucijos, ir kurie yra grindžiami ne įstatymu, bet kyla iš monarcho suverenumo ([57]). Prerogatyvinių įgaliojimų, kurie būtų aktualūs teisėsaugos požiūriu, pavyzdžių yra labai nedaug. Prie jų galima priskirti, pavyzdžiui, savitarpio teisinės pagalbos sistemą, pagal kurią valstybės sekretoriui yra leidžiama keistis

([49]) Pagrindiniai teisės aktai, kuriuose nustatyta pagrindinių policijos įgaliojimų (arešto, kratų, leidimo pratęsti sulaikymo terminą, pirštų antspaudų paėmimo, intymių mėginių paėmimo, orderio perėmimo, prieigos prie ryšių duomenų) vykdymo tvarka: i) Anglijoje ir Velse – 1984 m. Policijos ir baudžiamųjų įrodymų aktas, kurį galima rasti šiuo adresu https://www.legislation.gov.uk/ukpga/1984/60/contents (su pakeitimais, padarytais 2012 m. Laisvių apsaugos aktu, kurį galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2012/9/contents) ir 2016 m. Tyrimo įgaliojimų aktas; galia rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2016/25/contents); ii) Škotijoje – 2016 m. Baudžiamojo teisingumo (Škotija) aktas, kurį galima rasti šiuo adresu: https://www.legislation.gov.uk/asp/2016/1/contents ir 1995 m. Baudžiamojo proceso (Škotija) aktas, kurį galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/1995/46/contents); iii) Šiaurės Airija – 1989 m. Policijos ir baudžiamųjų įrodymų įsakymas, kurį galima rasti šiuo adresu: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Jungtinės Karalystės institucijos paaiškino, kad įstatymų normų viršenybės principas Jungtinėje Karalystėje nustatytas dar Sprendime *Entick / Carrington* [1765] EWHC KB J98, kuriame pripažinta, kad vykdomoji valdžia savo įgaliojimais naudojasi su tam tikrais apribojimais, bei įtvirtintas principas, kad bendrojoje teisėje ir prerogatyvose įtvirtinti monarcho ir Vyriausybės įgaliojimai priklauso žemesnei teisinei hierarchijai negu šalies įstatymai.

([51]) Žr. Sprendimą *Rice / Connolly* [1966] 2 QB 414.

([52]) Žr. Sprendimą *R(Catt) / Association of Chief police Officers* [2015] AC 1065, kuriame, nagrinėdamas policijos įgaliojimą gauti ir saugoti informaciją apie asmenį (įvykdžiusį nusikaltimą), Lordas J. Sumption konstatavo, kad pagal bendrąją teisę policija turi teisę gauti ir saugoti informaciją policijos veiklos tikslais, t. y. bendrai tariant, viešosios tvarkos palaikymo ir nusikaltimų prevencijos bei atskleidimo tikslais. Naudojantis šiais įgaliojimais nėra leidžiama taikyti intervencinių metodų informacijai gauti, pavyzdžiui, neleidžiama įeiti į privačią teritoriją ar imtis veiksmų (išskyrus areštą pagal bendrojoje teisėje įtvirtintus įgaliojimus), kurie prilygtų užpuolimui. Teisėjas konstatavo, kad šiuo atveju bendrojoje teisėje įtvirtintų įgaliojimų visiškai pakanka tam, kad būtų galima gauti ir saugoti atitinkamą skunduose nurodytą viešą informaciją.

([53]) 2010 m. Lygybės aktas; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Bylos, kurioje vertinami bendrojoje teisėje įtvirtinti policijos įgaliojimai, pagal 1998 m. DAA pavyzdys – Aukštojo teismo sprendimas *Bridges / the Chief Constable of South Wales Police* (žr. 33 išnašą). Taip pat žr. Sprendimus *Vidal-Hall / Google Inc* [2015] EWCA Civ 311 ir *Richard / BBC* [2018] EWHC 1837 (Ch).

([55]) Pavyzdžiui, žr. Šiaurės Airijos policijos tarnybos gaires dėl įrašų valdymo tarnybinių instrukcijų; galima rasti šiuo adresu: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Bendruomenių rūmai paskelbė informacinį dokumentą, kuriame išdėstė pagrindinius bendrojoje teisėje ir įstatymuose įtvirtintus Anglijos ir Velso policijos įgaliojimus (žr. https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Pavyzdžiui, remiantis šiuo dokumentu, įgaliojimas „saugoti Karūnos taiką“ yra įtvirtintas bendrojoje teisėje, o įgaliojimai „panaudoti jėgą“, „sustabdyti ir apieškoti“ visada kyla iš įstatymų. Škotijos Vyriausybė savo interneto svetainėje taip pat pateikia informaciją apie policijos įgaliojimus vykdyti areštus, sustabdyti ir apieškoti asmenis (žr. https://www.gov.scot/policies/police/police-powers/).

([57]) Remiantis Jungtinės Karalystės institucijų pateikta informacija, prie prerogatyvinių Vyriausybės vykdomų įgaliojimų priskiriami, pavyzdžiui, įgaliojimai sudaryti ir ratifikuoti sutartis, vykdyti diplomatinį darbą, panaudoti ginkluotąsias pajėgas Jungtinės Karalystės teritorijoje siekiant išsaugoti taiką ir padėti policijai.

duomenimis su trečiosiomis valstybėmis teisėsaugos tikslais. Įgaliojimas tokiu būdu teikti duomenis ne visada būna įtvirtintas įstatyme ([58]). Karališkosioms prerogatyvoms galioja bendrosios teisės principai ([59]) ir jie priklauso žemesniam teisinės hierarchijos lygmeniui negu įstatymai, todėl jiems taikomi 1998 m. Žmogaus teisių akte ir 2018 m. DAA nustatyti apribojimai ([60]).

(33) Panašiai kaip pagal Direktyvos (ES) 2016/680 8 straipsnį, pagal Jungtinėje Karalystėje galiojančią tvarką yra reikalaujama, jog tam, kad būtų laikomasi teisėtumo principo, kompetentingos institucijos turėtų užtikrinti, kad tais atvejais, kai duomenys yra tvarkomi remiantis įstatymu, duomenų tvarkymas tai pat būtų „reikalingas“ teisėsaugos tikslu vykdomai užduočiai atlikti. Informacijos komisaras gairėse dėl šio aspekto paaiškina, kad „tai turi būti tikslingas ir proporcingas būdas tikslui pasiekti. Įstatyminis pagrindas nebus taikomas, jeigu tikslą pagrįstai galima pasiekti kitomis mažiau intervencinėmis priemonėmis. Nurodyti, kad duomenų tvarkymas yra reikalingas, nes nusprendėte savo veiklą vykti kuriuo nors konkrečiu būdu, nepakanka. Klausimas keliamas apie tai, ar duomenų tvarkymas yra būtinas nurodytam tikslui“ ([61]).

2.4.1.2. Duomenų tvarkymas, remiantis duomenų subjekto sutikimu

(34) Kaip nurodyta 28 konstatuojamojoje dalyje, 2018 m. DAA 35 straipsnio 2 dalyje yra numatyta galimybė asmens duomenis tvarkyti remiantis asmens „sutikimu“.

(35) Tačiau sutikimas nesudaro teisinio pagrindo duomenų tvarkymo operacijoms, dėl kurių priimamas šis sprendimas, vykdyti. Iš tiesų duomenų tvarkymo operacijos, dėl kurių priimamas šis sprendimas, visada bus susijusios su duomenimis, kuriuos pagal Direktyvą (ES) 2016/680 kurios nors valstybės narės kompetentinga institucija perdavė Jungtinės karalystės kompetentingai institucijai. Todėl paprastai šios operacijos neapims tiesioginių valdžios institucijos ir duomenų subjektų santykių (duomenų rinkimo), kurių pagrindą pagal 2018 m. DAA 35 straipsnio 2 dalies a punktą gali sudaryti sutikimas.

(36) Nors pagal šį sprendimą atliekamam vertinimui atvejai, kai remiamasi sutikimu, nėra aktualūs, dėl išsamumo derėtų paminėti, kad teisėsaugos tikslais vykdomas duomenų tvarkymas niekada nebūna grindžiamas vien sutikimu, nes kompetentinga institucija visada turi turėti atitinkamus įgaliojimus, leidžiančius jai tvarkyti duomenis ([62]). Taksliau, panašiai kaip pagal Direktyvą (ES) 2016/680 ([63]), tai reiškia, kad sutikimas yra papildoma sąlyga, leidžianti atlikti kai kurias ribotas ir specialias duomenų tvarkymo operacijas, kurių kitu atveju nebūtų galima atlikti, pavyzdžiui, paimti asmens, kuris nėra įtariamasis, DNR mėginius ir tvarkyti jo duomenis. Tokiu atveju, jeigu sutikimas nebūtų duotas arba būtų atšauktas, duomenys nebūtų tvarkomi ([64]).

([58]) Šiuo atžvilgiu žr. Jungtinės Karalystės tolesnio informacijos perdavimo tvarką, aptartą 74–87 konstatuojamosiose dalyse.

([59]) Žr. bylą *Bancoult / Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61, kurioje teismai konstatavo, kad prerogatyviniam įgaliojimui priimti Tarybos įsakymus taip pat taikomi bendrieji teisminės peržiūros pagrindai.

([60]) Žr. bylą *Attorney-General / De Keyser's Royal Hotel Ltd* [1920] [1920] AC 508, kurioje teismas konstatavo, kad prerogatyviniais įgaliojimais negalima naudotis, kai vietoj jų galioja įstatyme įtvirtinti įgaliojimai; Sprendimą *Laker Airways Ltd / Department of Trade* 1977] QB 643,], kuriame teismas konstatavo, kad prerogatyviniais įgaliojimais negalima naudotis, jei taip būtų pažeistos įstatymo normos; Sprendimą *R / Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3, kuriame teismas konstatavo, kad prerogatyviniais įgaliojimais naudotis negalima, jeigu jie prieštarauja priimtiems teisės aktams, net jeigu priimtas teisės aktas dar nėra įsigalioję; Sprendimą *R (Miller) / Secretary of State for Exiting the European Union* [2017] UKSC 5, kuriame teismas patvirtino, kad įstatymo normomis galima koreguoti ir panaikinti prerogatyvinius įgaliojimus. Bendra Karališkųjų prerogatyvų ir įstatymuose arba bendrojoje teisėje įtvirtintų įgaliojimų tarpusavio ryšių apžvalga pateikta Bendruomenių rūmų informaciniame dokumente, kurį galima rasti šiuo adresu: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Duomenų tvarkymo teisėsaugos tikslais gairė „Koks yra pirmasis principas?“; galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Tokia išvada darytina pagal atitinkamos 2018 m. DAA nuostatos formuluotę, kad asmens duomenų tvarkymas bet kuriuo teisėsaugos tikslu yra teisėtas tik tada, jeigu yra grindžiamas įstatymu ir jeigu duomenų subjektas sutiko, kad jo duomenys būtų tvarkomi tuo tikslu, arba duomenis tvarkyti būtina tam, kad kompetentinga institucija galėtų atlikti tuo tikslu vykdomą užduotį.

([63]) Žr. Reglamento (ES) 2016/680 35–26 konstatuojamąsias dalis.

([64]) Jungtinės Karalystės institucijos paaiškino, kad sutikimas gali būti tinkamas duomenų tvarkymo pagrindas, jei, pavyzdžiui, policijai reikėtų paimti DNR mėginį, kad dingusio asmens DNR galėtų palyginti su rasto kūno, jei jis būtų rastas, DNR. Tokiomis aplinkybėmis policijai būtų netinkama versti domenų subjektą duoti mėginį ir policija veikiau prašytų asmens sutikimo, o jį asmuo galėtų duoti laisva valia ir bet kuriuo metu atšaukti. Jeigu sutikimas būtų atšauktas, duomenų toliau tvarkyti nebebūtų galima, nebent būtų nustatytas naujas teisinis pagrindas mėginiui tvarkyti (pvz. duomenų subjektas taptų įtariamuoju). Kitas pavyzdys būtų atvejis, kai policijos pajėgos tiria nusikaltimą, kurio aukai (pavyzdžiui, apiplėšimo, seksualinio nusikaltimo, smurto artimoje aplinkoje aukai, nužudyto asmens artimiesiems arba kitai nusikaltimo aukai) būtų naudinga kreiptis į Pagalbos nukentėjusiems asmenims tarnybą (nepriklausomą labdaros tarnybą, teikiančią paramą dėl nusikaltimų ir traumuojančių incidentų nukentėjusiems asmenims). Tokiomis aplinkybėmis policija Pagalbos nukentėjusiems asmenims tarnybai asmens duomenis, pavyzdžiui, vardą, pavardę, kontaktinius duomenis, suteiktų tik tada, jei būtų gavusi nukentėjusio asmens sutikimą.

(37) Tais atvejais, kai reikalingas asmens sutikimas, šis sutikimas turi būti aiškus ir duotas aiškiu tai patvirtinančiu veiksmu ([65]). Policijos pajėgos privalo būti parengusios pareiškimą dėl privatumo ir, be kita ko, reikiamą informaciją apie tinkamą sutikimo naudojimą. Be to, kai kurios policijos pajėgos skelbia papildomą informaciją apie tai, kaip laikosi duomenų apsaugos teisės aktų, įskaitant tai, kaip ir kada jie remtųsi sutikimu kaip teisiniu pagrindu ([66]).

2.4.1.3. Neskelbtinų duomenų tvarkymas

(38) Kai tvarkomi „specialių kategorijų“ duomenys, turėtų būti taikomos specialios apsaugos priemonės. Šiuo atžvilgiu panašiai kaip Direktyvos (ES) 2016/680 10 straipsnyje, 2018 m. DAA 3 dalyje „neskelbtinų duomenų tvarkymo“ atvejams yra nustatytos griežtesnės apsaugos priemonės ([67]).

(39) Remiantis 1998 m. DAA 35 straipsnio 3 dalimi, neskelbtinus duomenis kompetentingos institucijos gali tvarkyti teisėsaugos tikslais tik dviem atvejais: 1) jeigu duomenų subjektas davė sutikimą dėl duomenų tvarkymo teisėsaugos tikslu ir tuo metu, kai vykdoma duomenų tvarkymo operacija, duomenų valdytojas turi atitinkamą politikos dokumentą ([68]) arba 2) jeigu duomenų tvarkymas teisėsaugos tikslu yra būtinai reikalingas, atitinka bent vieną iš 2018 m. DAA 8 priede išdėstytų sąlygų ir tuo metu, kai vykdoma duomenų tvarkymo operacija, duomenų valdytojas turi atitinkamą politikos dokumentą ([69]).

(40) Kaip paaiškina 38 konstatuojamojoje dalyje, pirmuoju atveju sutikimas kaip pagrindas nėra aktualus, jei perduodami duomenys patenka į šio sprendimo taikymo sritį ([70]).

(41) Kai sutikimas nėra neskelbtinų duomenų tvarkymo pagrindas, duomenys gali būti tvarkomi remiantis viena iš 2018 m. DAA 8 priede išdėstytų sąlygų. Šios sąlygos yra susijusios su duomenų tvarkymo reikalingumu įstatyme nustatytais tikslais: teisingumui administruoti, duomenų subjekto ar kito asmens gyvybiniams interesams apsaugoti, vaikams ir riziką patiriantiems asmenims apsaugoti, teisiniams ieškiniams, teismų veiksmams, sukčiavimo prevencijai, archyvavimui, kai asmens duomenis asmuo akivaizdžiai paviešino pats. Išskyrus atvejį, kai duomenys yra akivaizdžiai jau paviešinti, visoms 8 priede išdėstytoms sąlygoms yra taikomas „būtino reikalingumo“ kriterijus. Kaip paaiškino informacijos komisaras, „būtinas reikalingumas šiuo atžvilgiu reiškia, kad duomenų tvarkymas turi būti susijęs su aktualiu socialiniu poreikiu ir jo pagrįstai neturi būti galima patenkinti mažiau intervencinėmis

([65]) Atskiros sąvokos „sutikimas“ apibrėžties, kuri būtų taikoma tvarkant asmens duomenis pagal 2018 m. DAA 3 dalį, nėra. Informacijos komisaro gairėse dėl sąvokos „sutikimas“ pagal 2018 m. DAA 3 dalį paaiškinta, kad šios sąvokos reikšmė atitinka BDAR pateiktą apibrėžtį, tiksliau, „sutikimas turi būti duotas laisvai, remiantis visa informacija, būti konkretus ir duotas aiškiai leidus pasirinkti, ar sutikti su tuo, kad duomenys būtų tvarkomi“ (Duomenų tvarkymo teisėsaugos tikslais gairė „Koks yra pirmasis principas?“) (žr. 64 išnašą) ir Duomenų apsaugos gairių nuostatos dėl sutikimo; galima rasti adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Pvz., žr. Linkolnšyro policijos interneto svetainėje paskelbtą informaciją (žr. https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) arba Vakarų Jorkšyro policijos interneto svetainėje paskelbtą informaciją (žr. https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) 2018 m. DAA 35 straipsnio 8 dalis.

([68]) 2018 m. DAA 35 straipsnio 4 dalis.

([69]) 2018 m. DAA 35 straipsnio 5 dalis.

([70]) Dėl išsamumo derėtų paminėti, kad tais atvejais, kai duomenų tvarkymo pagrindas yra sutikimas, toks sutikimas turi būti duotas laisvai, remiantis visa informacija, būti konkretus ir duotas aiškiai leidus pasirinkti, ar sutikti su tuo, kad duomenys būtų tvarkomi. Be to, kai duomenų valdytojas tvarko duomenis remdamasis duomenų subjekto sutikimu, jis turi turėti „atitinkamą politikos dokumentą“ (toliau – APD). 2018 m. DAA 42 straipsnyje išdėstyta, kokius reikalavimus turi atitikti APD. Jame nurodyta, kad tokiame dokumente turi būti bent paaiškinta, kaip duomenų valdytojas užtikrina, kad būtų laikomasi duomenų apsaugos principų, ir kokios asmens duomenų saugojimo ir ištrynimo politikos jis laikosi. Remiantis 2018 m. DAA 42 straipsniu, duomenų valdytojas privalo pateikti dokumentą, kuriame būtų paaiškinta: a) kokiomis procedūromis duomenų valdytojas užtikrina, kad būtų laikomasi duomenų apsaugos principų, ir b) kokios asmens duomenų, tvarkomų remiantis duomenų subjekto sutikimu, saugojimo ir ištrynimo politikos duomenų valdytojas laikosi, arba nurodyta, kiek laiko tokie asmens duomenys greičiausiai bus saugomi. Visų pirma, Politikos dokumente turi būti reikalaujama, kad duomenų valdytojas, vykdydamas savo pareigą registruoti duomenų tvarkymo veiklą, visada nurodytų a ir b punktuose paminėtus aspektus. Informacijos komisaras yra paskelbęs pavyzdinį dokumentą (Duomenų tvarkymo teisėsaugos tikslais gairė „Neskelbtinų duomenų tvarkymo sąlygos“; galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) ir, jeigu duomenų valdytojai nevykdo šių reikalavimų, gali imtis priverstinio vykdymo veiksmų. Nagrinėdami galimus 2018 m. DAA pažeidimus teismai analizuoja ir APD. Pavyzdžiui, neseniai nagrinėtoje byloje *R (Bridges) / Chief Constable of South Wales Police* teismai peržiūrėjo duomenų valdytojo APD ir nustatė, kad jis yra pakankamas, tačiau jame galėtų būti pateikta išsamesnių duomenų. Atsižvelgdama į tai, Pietų Velso policija peržiūrėjo APD ir jį atnaujino pagal informacijos komisaro gaires (žr. 33išnašą). Be to, pagal 2018 m. DAA 42 straipsnio 3 dalį duomenų valdytojas turėtų reguliariai peržiūrėti savo APD. Galiausiai pažymėtina, kad 2018 m. DAA 42 straipsnio 4 dalyje yra nustatyta papildoma apsaugos priemonė – duomenų valdytojas privalo saugoti ir kaupti duomenų tvarkymo veiklos archyvą, įskaitant papildomus duomenis, ne tik laikytis bendros savo pareigos saugoti duomenų tvarkymo veiklos įrašus, kaip nustatyta 2018 m. DAA 61 straipsnyje.

priemonėmis“ ([71]). Be to, kai kurioms sąlygoms taikomi papildomi apribojimai. Pavyzdžiui, jeigu norima remtis „įstatyme nustatyto tikslo“ ir „apsaugos“ sąlyga (8 priedo 1 ir 4 dalys), reikia, kad būtų įvykdyta papildoma reikšmingo visuomenės intereso sąlyga. Kad būtų galima remtis vaiko apsaugos sąlygomis (8 priedo 4 dalis), duomenų subjektas taip pat turi būti sulaukęs tam tikro amžiaus ir turi būti padaryta išvada, kad jam gresia pavojus. Duomenų valdytojas gali taikyti 8 priedo 4 dalyje nustatytą sąlygą tik susiklosčius tam tikroms aplinkybėms ([72]). Panašūs apribojimai taikomi „teismų veiksmų“ ir „sukčiavimo prevencijos“ sąlygoms (atitinkamai 8 priedo 7 ir 8 dalys). Abi sąlygos yra taikomos tik konkretiems duomenų valdytojams. Teismų veiksmų sąlyga gali remtis tik teismas arba kita teisminė institucija, o sukčiavimo prevencijos sąlyga – tik duomenų valdytojas, kuris yra kovos su sukčiavimu organizacija.

(42) Galiausiai pažymėtina, kad tais atvejais, kai duomenys yra tvarkomi remiantis kuria nors iš 8 priede nustatytų sąlygų ir atitinkamai 2018 m. DAA 42 straipsniu, turi būti parengtas „atitinkamas politikos dokumentas“, kuriame būtų paaiškinta, kaip duomenų valdytojas užtikrina, kad būtų laikomasi duomenų apsaugos principų ir kokios duomenų saugojimo ir ištrynimo politikos jis laikosi; taip pat turi būti vykdoma pareiga kaupti duomenis.

2.4.2. *Tikslo apribojimas*

(43) Asmens duomenys turėtų būti tvarkomi konkrečiu tikslu ir vėliau naudojami tik tiek, kiek tai nėra nesuderinama su jų tvarkymo tikslu. Šis duomenų apsaugos principas yra įtvirtintas 2018 m. DAA 36 straipsnyje. Pagal šią nuostatą, panašiai kaip pagal Direktyvos (ES) 2016/680 4 straipsnio 1 dalies b punktą, yra reikalaujama, kad a) teisėsaugos tikslas, dėl kurio renkami asmens duomenys, bet kuriuo atveju būtų konkrečiai nustatytas, aiškiai apibrėžtas ir teisėtas, ir b) tokiu būdu renkami asmens duomenys nebūtų tvarkomi tokiu būdu, kuris būtų nesuderinamas su tikslais, kuriems duomenys buvo renkami.

(44) Kai kompetentingos institucijos tvarko duomenis teisėsaugos tikslu, duomenų tvarkymas gali apimti archyvavimą, mokslo arba istorinių tyrimų ir statistinius tikslus ([73]). 2018 m. DAA taip pat paaiškinta, kad tokiais atvejais archyvavimas (arba tvarkymas mokslo ar istorinių tyrimų bei statistikos tikslais) nėra leidžiamas, jeigu jis susijęs su sprendimais dėl konkretaus duomenų subjekto arba jeigu dėl to duomenų subjektas gali patirti didelę žalą arba stresą ([74]).

2.4.3. *Tikslumas ir duomenų kiekio mažinimas*

(45) Duomenys privalo būti tikslūs ir, jei reikia, atnaujinami. Duomenys taip pat privalo būti tinkami, aktualūs ir neperteklinai, atsižvelgiant į tikslus, kuriais yra tvarkomi. Panašiai kaip Direktyvos (ES) 2016/680 4 straipsnio 1 dalies c, d ir e punktuose, šie principai yra įtvirtinti 2018 m. DAA 37 ir 38 straipsniuose. Turi būti imtasi visų pagrįstų priemonių, kuriomis būtų užtikrinta, kad netikslūs asmens duomenys ([75]) būtų

([71]) Duomenų tvarkymo teisėsaugos tikslais gairė „Neskelbtinų duomenų tvarkymo sąlygos“ (žr. 70 išnašą).

([72]) Duomenys yra tvarkomi be duomenų subjekto sutikimo, kai: a) duomenų subjektas negali duoti sutikimo dėl duomenų tvarkymo; b) duomenų valdytojas dėl pagrįstų priežasčių negalėtų gauti duomenų subjekto sutikimo dėl duomenų tvarkymo; c) duomenis būtina tvarkyti be duomenų subjekto sutikimo, nes gaunant duomenų subjekto sutikimą, būtų pažeista 1 dalies a punkto nuostata dėl apsaugos.

([73]) Žr. 2018 m. DAA 41 straipsnio 1 dalį.

([74]) Žr. 2018 m. DAA 41 straipsnio 2 dalį.

([75]) 2018 m. DAA 205 straipsnyje apibrėžta, kad sąvoka „netikslūs“ reiškia, kad asmens duomenys yra „neteisingi arba klaidinantys“. Jungtinė Karalystė paaiškino, kad su baudžiamaisiais tyrimais susiję duomenys dažnai būna neišsamūs, tačiau nepaisant to, jie gali būti tikslūs.

nedelsiant ([76]) ištrinti arba ištaisyti, atsižvelgiant į teisėsaugos tikslą, dėl kurio jie tvarkomi ([77]), ir kad netikslūs, neišsamūs arba pasenę asmens duomenys nebūtų perduodami ar suteikiami jokiais teisėsaugos tikslais ([78]).

(46) Taip pat pažymėtina, kad panašiai kaip pagal Direktyvos (ES) 2016/680 7 straipsnį, pagal Jungtinės Karalystės duomenų apsaugos reikalavimus yra nustatyta, kad faktais pagrįsti asmens duomenys, kiek tai yra galima, turi būti atskirti nuo asmeniniu vertinimu pagrįstų asmens duomenų ([79]). Kai tai svarbu ir įmanoma, asmens duomenys, susiję su įvairių kategorijų duomenų subjektais, pavyzdžiui, įtariamaisiais, už nusikalstamą veiką nuteistais asmenimis, nuo nusikalstamos veikos nukentėjusiais asmenimis ir liudininkais, turi būti atskirti ([80]).

2.4.4. *Saugojimo apribojimas*

(47) Pagal Direktyvos (ES) 2016/680 5 straipsnį duomenys iš esmės turėtų būti laikomi ne ilgiau, negu reikia tiems tikslams, dėl kurių jie yra tvarkomi. Pagal 2018 m. DAA 39 straipsnį, panašiai kaip pagal Direktyvos 5 straipsnį, asmens duomenis, kurie buvo tvarkomi kuriais nors teisėsaugos tikslais, yra draudžiama laikyti ilgiau, negu reikia tam tikslui, kuriam jie buvo tvarkyti. Pagal Jungtinėje Karalystėje galiojančią teisinę tvarką reikalaujama nustatyti tinkamus terminus, kada turi būti atlikta periodinė peržiūra, ar asmens duomenis kuriuo nors teisėsaugos tikslu reikia saugoti toliau. Atitinkamuose teisės aktuose ir gairėse dėl policijos įgaliojimų ir veikimo išdėstytos išsamesnės taisyklės dėl asmens duomenų saugojimo praktikos ir taikytinų terminų. Pavyzdžiui, Anglijoje ir Velse galiojančiame Policijos koledžo parengtame PIV praktikos kodekse, taip pat PIV LPP gairėse yra nustatyta, kaip valdant operatyvinę policijos informaciją užtikrinti rizikos vertinimu pagrįstą nuoseklų duomenų saugojimo, peržiūros ir pašalinimo procesą ([81]). Šioje tvarkoje yra nustatyti aiškūs visai tarnybai taikomi lūkesčiai, kaip informacija turėtų būti kuriama, teikiama, naudojama ir valdoma policijos pajėgų viduje ir santykiuose su kitomis tarnybomis ([82]). Policija turėtų laikytis Praktikos kodekso, o tai, kaip jo laikomasi tikrina Jos Didenybės konsteblių inspekcija ir priešgaisrinė bei gelbėjimo tarnyba ([83]).

(48) Šiaurės Airijos policijos tarnyba (angl. *Police Service of Northern Ireland* arba PSNI) pagal įstatymą neprivalo laikytis PIV praktikos kodekso. Tačiau 2011 m. patvirtinta PIV sistema papildyta PSNI vadovu ([84]), kuriame išdėstyta politika ir procedūros, kaip PIV praktikos kodeksas yra taikomas Šiaurės Airijoje.

([76]) 2018 m. DAA 38 straipsnio 1 dalies b punktas.

([77]) Diskusijoms dėl duomenų apsaugos tinkamumo skirtame Jungtinės Karalystės aiškinamajame dokumente paaiškinta, kad taip užtikrinama, kad būtų pripažintos tiek duomenų subjektų teisės, tiek teisėsaugos tarnybų teisėsaugos operatyviniai poreikiai. Rengiant Duomenų apsaugos bilį, pirmiau nurodytas aspektas buvo kruopščiai išnagrinėtas, nes kai kuriais atvejais duomenų negalima ištaisyti dėl specifinių operatyvinių priežasčių. Dažniausiai taip nutinka, kai atitinkamus netikslius asmens duomenis reikia išsaugoti pirmine forma įrodymų tikslais“ (žr. Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento F skirsnį „Teisėsauga“, p. 21, žr. 9 išnašą).

([78]) 2018 m. DAA 38 straipsnio 4 dalis. Be to, pagal 2018 m. DAA 38 straipsnio 5 dalį prieš perduodant ar suteikiant asmens duomenis, būtina patikrinti jų kokybę, visais atvejais kartu su perduodamais asmens duomenis turi būti pateikiama reikalinga informacija, kad gavėjas galėtų įvertinti duomenų tikslumą, išsamumą ir patikimumą bei tai, kiek jie yra nauji, o jei po to, kai asmens duomenys buvo perduoti, paaiškėja, kad jie nebuvo teisingi arba kad perdavimas buvo neteisėtas, gavėjas privalo būti nedelsiant apie tai informuotas.

([79]) 2018 m. DAA 38 straipsnio 2 dalis.

([80]) 2018 m. DAA 38 straipsnio 3 dalis.

([81]) Ši tvarka užtikrina, kad surinktų asmens duomenų saugojimo reikalavimai būtų taikomi nuosekliai. Peržiūros laikotarpis priklauso nuo nusikalstamų veikų ir yra skirstomas į 4 grupes: 1) tam tikri visuomenės apsaugos reikalai; 2) kiti seksualinio smurto ir sunkūs nusikaltimai; 3) visa kita nusikalstama veika; 4) kita. Daugiau informacijos pateikta PIV LPP gairėse (žr. 26 išnašą).

([82]) Remiantis Jungtinės Karalystės institucijų pateikta informacija, kitos organizacijos gali laikytis PIV praktikos kodekso principų, jeigu to pageidauja, pavyzdžiui, Jos Didenybės mokesčių ir muitų tarnyba bei Nacionalinė nusikaltimų agentūra savarankiškai taiko daugelį PIV praktikos kodekso principų, siekdamos užtikrinti nuoseklumą teisėsaugos institucijose. Apskritai dauguma organizacijų supažindina savo darbuotojus su specialia konkrečiai organizacijai pritaikyta politika ir visiems darbuotojams skirtomis gairėmis, kaip vykdant savo pareigas tvarkyti asmens duomenis. Paprastai rengiami ir privalomi mokymai.

([83]) PIV praktikos kodeksas buvo parengtas vadovaujantis 1996 m. Policijos akte įtvirtintais įgaliojimais, pagal kuriuos Policijos koledžas gali rengti praktikos kodeksus policijos veiklos veiksmingumui užtikrinti. Bet kurį pagal Aktą skelbiamą kodeksą turi patvirtinti valstybės sekretorius, o prieš pateikiant jį Parlamentui, dėl jo turi būti konsultuojamasi su Nacionaline nusikaltimų agentūra. Policijos akto 39A straipsnio 7 dalyje reikalaujama, kad policija deramai laikytųsi pagal šį aktą paskelbtų kodeksų.

([84]) Šiaurės Airijos policijos tarnybos PIV vadovo 1–6 skyriai.

(49) Škotijos policijos pajėgos taiko Įrašų saugojimo standartinę veiklos procedūrą (angl. *Standard Operating Procedure* arba SOP) ([85]), pagal kurią įgyvendinama Škotijos policijos tarnybos įrašų valdymo politika ([86]). Standartinėje veiklos procedūroje yra nustatytos specialiosios Škotijos policijos turimų duomenų laikymo taisyklės.

(50) Be visuotinai visoje Jungtinėje Karalystėje taikomo įrašų peržiūros reikalavimo taikomos ir kitos išsamesnės vietos lygmens taisyklės. Pavyzdžiui, Anglijoje ir Velse galiojančiame Policijos ir baudžiamųjų įrodymų akte, iš dalies pakeistame 2012 m. Laisvių apsaugos aktu, yra išdėstytos nuostatos dėl pirštų antspaudų ir DNR profilių saugojimo, taip pat nustatyta speciali nenuteistiems asmenims taikoma tvarka ([87]). Laisvių apsaugos aktu įsteigta biometrinių duomenų saugojimo ir naudojimo komisaro (toliau – biometrinių duomenų komisaras) pareigybė ([88]). 2017 m. Laikinai sulaikytų asmenų atvaizdų peržiūros apraše nustatytos specialios taisyklės dėl laikinai sulaikytų asmenų atvaizdų ([89]). Škotijos 1995 m. Baudžiamojo proceso (Škotija) akte išdėstytos taisyklės dėl pirštų antspaudų ir biologinių mėginių paėmimo ir saugojimo ([90]). Taip, kaip Anglijoje ir Velse, šiuo teisės aktu reglamentuojamas su įvairiomis bylomis susijusių biometrinių duomenų saugojimas ([91]).

2.4.5. *Duomenų saugumas*

(51) Asmens duomenys privalo būti tvarkomi taip, kad būtų užtikrintas jų saugumas, įskaitant apsaugą nuo neleistino ar neteisėto tvarkymo ir netyčinio praradimo, sunaikinimo ar sugadinimo. Todėl valdžios institucijos turi imtis tinkamų techninių ir organizacinių priemonių, kad asmens duomenis apsaugotų nuo galimų grėsmių. Tokios priemonės turi būti įvertintos atsižvelgiant į techninių galimybių išsivystymo lygį ir su tuo susijusias sąnaudas.

(52) Šie principai įtvirtinti 2018 m. DAA 40 straipsnyje, kuriame, panašiai kaip Direktyvos (ES) 2016/680 4 straipsnio 1 dalies f punkte, yra nurodyta, kad bet kuriais teisėsaugos tikslais tvarkomi asmens duomenys turi būti tvarkomi taip, kad techninėmis arba organizacinėmis priemonėmis būtų užtikrintas reikiamas asmens duomenų saugumas. Tai reiškia, kad, be kitų dalykų, duomenys turi būti apsaugoti nuo neleistino arba neteisėto tvarkymo,

([85]) Standartinę duomenų saugojimo veiklos procedūrą galima rasti šiuo adresu: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Daugiau informacijos apie įrašų valdymą pateikta Škotijos nacionalinių įrašų apraše, kurį galima rasti šiuo adresu: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Saugojimo laikotarpiai skiriasi, priklausomai nuo to, ar asmuo buvo teistas (pagal Policijos aktą priimto 1984 m. etikos kodekso 63I–63KI straipsniai). Pavyzdžiui, jeigu suaugęs asmuo yra nuteisiamas už registruotiną nusikalstamą veiką, jo pirštų antspaudai ir DNR profilis gali būti saugomi neribotą laiką (pagal Policijos aktą priimto 1984 m. etikos kodekso 63I straipsnio 2 dalis), o jeigu asmuo yra jaunesnis nei 18 m. amžiaus, teisės pažeidimas yra „smulkus“ ir asmuo iki tol nebuvo teistas, saugojimo laikotarpis bus ribotas (pagal Policijos aktą priimto 1984 m. etikos kodekso 63K straipsnis). Jeigu asmuo yra areštuojamas arba apkaltinamas, bet nenuteisiamas, saugojimo laikotarpis yra treji metai (pagal Policijos aktą priimto 1984 m. etikos kodekso 63F straipsnis). Šio saugojimo laikotarpio pratęsimą turi patvirtinti teismo institucija (pagal Policijos aktą priimto 1984 m. etikos kodekso 63F straipsnio 7 dalis). Jeigu asmuo yra areštuojamas arba apkaltinamas, tačiau už smulkų teisės pažeidimą nėra nuteisiamas, tokių duomenų saugoti negalima (pagal Policijos aktą priimto 1984 m. etikos kodekso 63D ir 63H straipsniai).

([88]) 2012 m. Laisvių apsaugos įstatymo 20 straipsniu įsteigiama biometrinių duomenų komisaro pareigybė. Bet kitų funkcijų, biometrinių duomenų komisaras nusprendžia, kada policija gali, o kada negali saugoti DNR profilio įrašų ir pirštų antspaudų, kurie buvo paimti iš areštuotų, tačiau padarius kvalifikuotą nusikaltimą neapkaltintų asmenų (pagal Policijos aktą priimto 1984 m. etikos kodekso 63G straipsnis). Biometrinių duomenų komisaras taip pat yra bendrai atsakingas už DNR ir pirštų antspaudų saugojimą ir naudojimą bei jų saugojimą siekiant užtikrinti nacionalinį saugumą (2012 m. Laisvių apsaugos akto 20 straipsnio 2 dalis). Biometrinių duomenų komisaras skiriamas pagal Valstybės pareigūnų skyrimo kodeksą (kodeksas pateikiamas adresu: *Governance Code for Public Appointments* – GOV.UK (www.gov.uk)) ir nuostatomis dėl jo skyrimo aiškiai nurodyta, kad Vidaus reikalų sekretorius gali jį atleisti iš pareigų tik griežtai apibrėžtomis aplinkybėmis; tai, pavyzdžiui, netinkamas pareigų vykdymas tris mėnesius, nuosprendis baudžiamojoje byloje arba skyrimo sąlygų nevykdymas.

([89]) Laikinai sulaikytų asmenų atvaizdų naudojimo ir saugojimo peržiūros aprašas; galima rasti šiuo adresu: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) 1995 m. Baudžiamojo proceso (Škotija) akto 18 ir paskesni straipsniai.

([91]) Duomenų saugojimo laikotarpiai skiriasi, priklausomai nuo to, ar asmuo buvo teistas (1995 m. Baudžiamojo proceso (Škotija) akto 18 straipsnio 3 dalis) arba ar yra nepilnametis. Antruoju atveju duomenų saugojimo laikotarpis yra 3 metai nuo nuosprendžio priėmimo vaikui iškeltoje byloje (1995 m. Baudžiamojo proceso (Škotija) akto 18E straipsnio 8 dalis). Asmenų, kurie buvo areštuoti, tačiau nebuvo nuteisti, duomenys negali būti saugomi (1995 m. Baudžiamojo proceso (Škotija) akto 18 straipsnio 3 dalis), išskyrus specialius atvejus ir priklausomai nuo nusikaltimo sunkumo (1995 m. Baudžiamojo proceso (Škotija) akto 18A straipsnis). 2020 m. Škotijos biometrinių duomenų komisaro aktu (žr. https://www.legislation.gov.uk/asp/2020/8/contents) sukurta Škotijos biometrinių duomenų komisaro pareigybė, o ją užimantis asmuo privalo rengti ir peržiūrėti (Škotijos parlamento patvirtintus) praktikos kodeksus dėl baudžiamojo teisingumo ir policijos tikslams skirtų biometrinių duomenų surinkimo, saugojimo, naudojimo ir sunaikinimo (2020 m. Škotijos biometrinių duomenų komisaro akto 7 straipsnis).

netyčinio praradimo, sunaikinimo arba sugadinimo ([92]). 2018 m. DAA 66 straipsnyje taip pat nustatyta, kad kiekvienas duomenų valdytojas ir kiekvienas duomenų tvarkytojas turi įdiegti reikiamas technines ir organizacines priemones, kuriomis būtų užtikrintas su asmens duomenų tvarkymu susijusią riziką atitinkantis apsaugos lygis. Remiantis aiškinamosiomis pastabomis, duomenų valdytojas privalo įvertinti rizikas ir, atsižvelgdamas į vertinimo rezultatus, įdiegti reikiamas apsaugos priemones, pavyzdžiui, duomenis šifruoti arba duomenis tvarkantiems darbuotojams suteikti specialaus lygmens saugumo leidimus ([93]). Atliekant vertinimą, pavyzdžiui, taip pat reikia atsižvelgti į tvarkomų duomenų pobūdį ir į kitus svarbius veiksnius arba aplinkybes, kurios gali turėti įtakos duomenų tvarkymo saugumui.

(53) Tvarka, kuria yra reglamentuojamas duomenų apsaugos principų laikymasis, yra labai panaši į Direktyvos (ES) 2016/680 29–31 straipsniuose nustatytus reikalavimus. Ypač pažymėtina, kad tuo atveju, jei pažeidžiamas asmens duomenų, už kuriuos atsakingas asmens duomenų valdytojas, saugumas, pagal 2018 m. DAA 67 straipsnio 1 dalį duomenų valdytojas privalo nedelsdamas, jei įmanoma – per 72 valandas nuo tada, kai sužino apie pažeidimą, pranešti apie asmens duomenų saugumo pažeidimą informacijos komisarui ([94]). Prievolė pranešti apie pažeidimą netaikoma, jeigu dėl asmens duomenų saugumo pažeidimo neiškyla pavojaus asmenų teisėms ir laisvėms tikimybė ([95]). Duomenų valdytojas privalo dokumentuoti su kiekvienu asmens duomenų saugumo pažeidimu susijusius faktus, pažeidimo padarinius ir tai, kokių taisomųjų veiksmų buvo imtasi, taip, kad informacijos komisaras galėtų įvertinti, kaip buvo laikomasi DAA ([96]). Jeigu duomenų tvarkytojas sužino apie saugumo pažeidimą, jis privalo apie tai nedelsdamas pranešti duomenų valdytojui ([97]).

(54) Remiantis 2018 m. DAA 68 straipsnio 1 dalimi, jeigu asmens duomenų saugumo pažeidimas gali kelti didelį pavojų asmenų teisėms ir laisvėms, duomenų valdytojas privalo apie pažeidimą nedelsdamas informuoti duomenų subjektą ([98]). Pranešime turi būti pateikta tokia pati informacija kaip 53 konstatuojamojoje dalyje nurodytame pranešime informacijos komisarui. Šis įpareigojimas netaikomas, jeigu duomenų valdytojas yra įdiegęs reikiamas technines ir organizacines apsaugos priemones ir jos buvo taikomos asmenims duomenims, kurių saugumas buvo pažeistas. Jis taip pat netaikomas, jeigu duomenų valdytojas ėmėsi paskesnių priemonių, kuriomis užtikrino, kad duomenų subjektų teisėms ir laisvėms daugiau nebekiltų didelis pavojus. Galiausiai pažymėtina, kad duomenų valdytojas neprivalo informuoti duomenų subjekto, jeigu tam prireiktų neproporcingai daug pastangų ([99]). Tokiu atveju informacija turi būti suteikta duomenų subjektui kitu lygiavertiškai veiksmingu būdu, pavyzdžiui, paskelbiant viešą pranešimą ([100]). Jeigu duomenų valdytojas neinformavo duomenų subjekto apie pažeidimą, gavęs DAA 67 straipsnyje nurodytą pranešimą ir apsvarstęs, kiek yra tikėtina, kad dėl pažeidimo kils didelis pavojus, informacijos komisaras gali reikalauti, kad duomenų valdytojas praneštų duomenų subjektui apie pažeidimą ([101]).

([92]) Remiantis 2018 m. DAA aiškinamosiomis pastabomis (žr. 45 išnašą), duomenų valdytojas pirmiausia privalo: suplanuoti ir įrengti turimų asmens duomenų pobūdį ir žalą, kuri gali būti padaryta dėl saugumo pažeidimo, atitinkančią apsaugą, aiškiai nustatyti, kas organizacijoje yra atsakingas už informacijos saugumo užtikrinimą, užtikrinti, kad būtų sukurta reikiama fizinė ir techninė apsauga ir kad ji būtų taikoma pagal tvirtą politiką bei procedūras, o ją taikytų patikimi, gerai parengti darbuotojai, būti pasirengęs greitai ir veiksmingai reaguoti į bet kokį saugumo pažeidimą.

([93]) 2018 m DAA aiškinamųjų pastabų 221 dalis (žr. 45 išnašą).

([94]) 2018 m. DAA 67 straipsnio 4 dalyje nustatyta, kad pranešime turi būti aprašytas asmens duomenų saugumo pažeidimo pobūdis (jeigu įmanoma, duomenų subjektų, kuriems jis aktualus, kategorijos, apytikslis skaičius ir asmens duomenų įrašų, kurių saugumas buvo pažeistas, kategorijos ir apytikslis skaičius), nurodytas kontaktinio asmens vardas pavardė ir kontaktiniai duomenys, aprašyti tikėtinų asmens duomenų saugumo pažeidimo padariniai ir priemonės, kurių duomenų valdytojas ėmėsi arba siūlo imtis asmens duomenų saugumo pažeidimui pašalinti (įskaitant, jei tai tikslinga, priemones, kuriomis neigiami padariniai būtų sušvelninti).

([95]) 2018 m. DAA 67 straipsnio 2 dalis.

([96]) 2018 m. DAA 67 straipsnio 6 dalis.

([97]) 2018 m. DAA 67 straipsnio 9 dalis.

([98]) Pagal 2018 m. DAA 68 straipsnio 7 dalį duomenų valdytojas gali visiškai arba iš dalies uždrausti teikti informaciją duomenų subjektui tokia apimtimi ir tiek laiko, kiek toks draudimas, atsižvelgiant į duomenų subjekto pagrindines teises ir teisėtus interesus, yra būtinas ir proporcingas siekiant a) išvengti trukdymo oficialiai ar teisėtai apklausai, tyrimui ar procedūrai; b) išvengti kenkimo nusikalstamų veikų prevencijai, atskleidimui, tyrimui ir baudžiamajam persekiojimui arba baudžiamųjų sankcijų vykdymui; c) užtikrinti visuomenės saugumą; d) užtikrinti nacionalinį saugumą; e) apsaugoti kitų asmenų teises ir laisves.

([99]) 2018 m. DAA 68 straipsnio 3 dalis.

([100]) 2018 m. DAA 68 straipsnio 5 dalis.

([101]) 2018 m. DAA 68 straipsnio 6 dalis, taikoma laikantis 2018 m. DAA 68 straipsnio 8 dalyje nustatyto apribojimo.

2.4.6. *Skaidrumas*

(55) Duomenų subjektai turi būti informuoti apie pagrindinius jų asmens duomenų tvarkymo aspektus. Šis duomenų apsaugos principas yra įtvirtintas 2018 m. DAA 44 straipsnyje, o jame, panašiai kaip Direktyvos (ES) 2016/680 13 straipsnyje, yra numatyta bendra duomenų valdytojo pareiga teikti duomenų subjektams informaciją apie jų asmens duomenų tvarkymą (tokią informaciją paskelbti viešai arba kitu būdu) ([102]). Reikalaujamą pateikti informaciją sudaro: a) duomenų valdytojo tapatybė ir kontaktiniai duomenys; b) kai taikoma, duomenų apsaugos pareigūno kontaktiniai duomenys; c) tikslai, dėl kurių duomenų valdytojas tvarko asmens duomenis; d) ar duomenų subjektai turi teisę prašyti duomenų valdytojo leisti peržiūrėti asmens duomenis, juos taisyti, ištrinti arba apriboti duomenų tvarkymą ir e) ar suteikiama teisė pateikti skundą informacijos komisarui, bei informacijos komisaro kontaktiniai duomenys ([103]).

(56) Tam, kad duomenų subjektas galėtų naudotis savo teisėmis pagal 2018 m. DAA (pavyzdžiui, kai tvarkomi asmens duomenys buvo surinkti duomenų subjektui nežinant), duomenų valdytojas konkrečiais atvejais taip pat privalo suteikti duomenų subjektui informaciją apie a) teisinį duomenų tvarkymo pagrindą; b) operatyvinių asmens duomenų saugojimo terminą arba, jei tai neįmanoma, kriterijus, taikomus tam terminui nustatyti; c) jei taikytina, apie asmens duomenų gavėjų kategorijas (įskaitant trečiosiose valstybėse esančius gavėjus arba tarptautines organizacijas); d) visą kitą informaciją, kuri yra reikalinga tam, kad duomenų subjektas galėtų naudotis savo teisėmis pagal 2018 m. DAA 3 dalį ([104]).

2.4.7. *Asmens teisės*

(57) Duomenų subjektams turi būti suteiktos įvairios įstatymais garantuojamos teisės. 2018 m. DAA 3 dalies 3 skyriuje įtvirtintos asmenų teisės susipažinti su duomenimis, duomenis taisyti, ištrinti ir apriboti ([105]), panašios į Direktyvos (ES) 2016/680 3 skyriuje numatytas teises.

(58) Teisė susipažinti su duomenimis įtvirtinta 2018 m. DAA 45 straipsnyje. Pirma, asmuo turi teisę gauti iš duomenų valdytojo patvirtinimą, ar jo asmens duomenys yra ar nėra tvarkomi ([106]). Antra, jeigu asmens duomenys yra tvarkomi, duomenų subjektas turi teisę susipažinti su tais duomenimis ir gauti šią informaciją apie duomenų tvarkymą: a) duomenų tvarkymo tikslus ir teisinį pagrindą; b) tvarkomų duomenų kategorijas; c) kam duomenys buvo atskleisti; d) asmens duomenų saugojimo laikotarpį; e) tai, kad duomenų subjektas turi teisę asmens duomenis ištaisyti ir ištrinti; f) apie teisę pateikti skundą ir g) visą informaciją apie atitinkamų asmens duomenų kilmę ([107]).

(59) Remiantis 2018 m. DAA 46 straipsniu, duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas ištaisytų netikslius asmens duomenis apie jį. Duomenų valdytojas privalo nedelsdamas ištaisyti duomenis (o jeigu duomenys yra netikslūs dėl to, kad neišsamūs – duomenis papildyti). Jeigu asmens duomenis reikia saugoti įrodymų tikslais, duomenų valdytojas privalo apriboti jų tvarkymą (ir jų netaisyti) ([108]).

([102]) Duomenų tvarkymo teisėsaugos srityje gairėse pateikiamas toks pavyzdys: „Savo interneto svetainėje esate paskelbę bendro pobūdžio pareiškimą dėl privatumo, kuriame pateikiama pagrindinė informacija apie asmens duomenų tvarkymo organizavimą ir tikslą, duomenų subjektų teises ir jų teisę teikti skundus informacijos komisarui. Gavote duomenų, kad asmuo dalyvavo vykdant nusikaltimą. Per pirmąją asmens apklausą turite pateikti bendro pobūdžio informaciją ir papildomą išsamesnę informaciją, kad jis galėtų pasinaudoti savo teisėmis. Sąžiningai teikiamą informaciją apie duomenų tvarkymą galite apriboti tik tada, jei tai neigiamai paveiktų jūsų vykdomą tyrimą“ (Duomenų tvarkymo teisėsaugos tikslais gairė „Kokią informaciją reikėtų suteikti asmeniui?“; galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Duomenų tvarkymo teisėsaugos tikslais gairėse nurodyta, kad teikiama informacija apie asmens duomenų tvarkymą turi būti glausta, aiški ir lengvai prieinama, išdėstyta aiškia ir paprasta kalba, pritaikyta pagal pažeidžiamų asmenų, pavyzdžiui, vaikų poreikius ir teikiama nemokamai (Duomenų tvarkymo teisėsaugos tikslais gairė „Kaip turėtume teikti šią informaciją?“; galima rasti šiuo adresu: 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 m. DAA 44 straipsnio 2 dalis.

([105]) Subjektų teisės išsamiau išnagrinėtos Duomenų tvarkymo teisėsaugos srityje gairėje apie asmens teises; ją galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) 2018 m. DAA 45 straipsnio 1 dalis.

([107]) 2018 m. DAA 45 straipsnio 2 dalis.

([108]) 2018 m. DAA 46 straipsnio 4 dalis.

(60) 2018 m. DAA 47 straipsnyje įtvirtinta asmenų teisė ištrinti duomenis ir apriboti jų tvarkymą. Jeigu dėl duomenų tvarkymo būtų pažeisti kurie nors duomenų tvarkymo principai, duomenų tvarkymo teisiniai pagrindai arba su neskelbtinų duomenų archyvavimu ir tvarkymu susijusios apsaugos priemonės, duomenų valdytojas privalo ([109]) nedelsdamas ištrinti asmens duomenis. Duomenų valdytojas taip pat privalo ištrinti duomenis, jeigu jiems nustatyta tokia teisinė prievolė. Jeigu asmens duomenis reikia išsaugoti įrodymų tikslais, duomenų valdytojas privalo apriboti jų tvarkymą (ir jų netaisyti) ([110]). Jeigu duomenų subjektas ginčija asmens duomenų tikslumą, tačiau įsitikinti, ar duomenys yra tikslūs, ar netikslūs, neįmanoma, duomenų valdytojas privalo apriboti asmens duomenų tvarkymą ([111]).

(61) Jeigu duomenų subjektas reikalauja asmens duomenis ištaisyti, ištrinti arba apriboja jų tvarkymą, duomenų valdytojas privalo raštu informuoti duomenų subjektą, ar jo prašymas buvo patenkintas, o jei prašymas buvo atmestas – informuoti duomenų subjektą apie atmetimo priežastis ir tai, kokiomis teisių gynimo priemonėmis jis gali pasinaudoti (duomenų subjekto teisę pateikti prašymą informacijos komisarui ištirti, ar apribojimas buvo taikomas teisėtai, teisę pateikti skundą informacijos komisarui ir teisę kreiptis į teismą su prašymu priimti sprendimą dėl tam tikrų veiksmų vykdymo arba nevykdymo) ([112]).

(62) Jeigu duomenų valdytojas ištaiso iš kitos kompetentingos institucijos gautus asmens duomenis, jis privalo ją apie tai informuoti ([113]). Jeigu duomenų valdytojas ištaiso, ištrina asmens duomenų valdytojo atskleistus duomenis arba apriboja jų tvarkymą, jis privalo informuoti gavėjus, o gavėjai privalo taip pat ištaisyti, ištrinti asmens duomenis arba apriboti asmens duomenų tvarkymą (ta apimtimi, kuria yra už tai atsakingi) ([114]).

(63) Be to, duomenų subjektas turi teisę į tai, kad duomenų valdytojas nedelsdamas jį informuotų apie asmens duomenų saugumo pažeidimą, jeigu dėl tokio pažeidimo kiltų didelis pavojus asmenų teisėms ir laisvėms ([115]).

(64) Kalbant apie visas šias duomenų subjekto teises, panašai kaip pagal Direktyvos (ES) 2016/680 12 straipsnį, duomenų valdytojas privalo užtikrinti, kad bet kokia informacija duomenų subjektui būtų pateikiama glausta, suprantama ir lengvai prieinama forma ([116]) ir, jei tai įmanoma, pateikiama tokia pat forma kaip prašymas ([117]). Duomenų valdytojas privalo patenkinti duomenų subjekto prašymą nedelsdamas arba bet kuriuo atveju per vieną mėnesį nuo prašymo gavimo dienos ([118]). Jeigu duomenų valdytojas turi pagrįstų abejonių dėl asmens tapatybės, jis gali prašyti pateikti papildomos informacijos ir atidėti prašymo nagrinėjimą, kol tapatybė bus patvirtinta. Duomenų valdytojas gali prašyti sumokėti pagrįstą mokestį arba atsisakyti imtis veiksmų, jeigu mano, kad prašymas yra akivaizdžiai nepagrįstas ([119]). Informacijos komisaras yra parengęs gaires apie tai, kada prašymas yra laikomas akivaizdžiai nepagrįstu ar pertekliniu ir kada galima prašyti sumokėti mokestį ([120]).

(65) Be to, pagal 2018 m. DAA 53 straipsnio 4 dalį valstybės sekretorius gali taisyklėse nustatyti didžiausią leidžiamą mokesčio dydį.

([109]) Duomenų subjektas gali reikalauti duomenų valdytojo ištrinti asmens duomenis arba apriboti jų tvarkymą (tačiau duomenų valdytojo pareigos ištrinti duomenis arba apriboti jų tvarkymą galioja, nepriklausomai nuo to, ar toks reikalavimas pateikiamas).

([110]) 2018 m. DAA 46 straipsnio 4 dalis ir 47 straipsnio 2 dalis.

([111]) 2018 m. DAA 47 straipsnio 3 dalis.

([112]) 2018 m. DAA 48 straipsnio 1 dalis.

([113]) 2018 m. DAA 48 straipsnio 7 dalis.

([114]) 2018 m. DAA 48 straipsnio 9 dalis.

([115]) 2018 m. DAA 68 straipsnis.

([116]) 2018 m. DAA 52 straipsnio 1 dalis.

([117]) 2018 m. DAA 52 straipsnio 3 dalis.

([118]) 2018 m. DAA 54 straipsnyje pateikta sąvokos „taikytinas terminas“ apibrėžtis; pagal pateiktą apibrėžtį – tai vieno mėnesio arba ilgesnis taisyklėse nustatytas laikotarpis, pradedamas skaičiuoti nuo atitinkamo laiko momento (kai duomenų valdytojas gauna atitinkamą klausimą, kai duomenų valdytojas gauna informaciją (jei gauna), susijusią su prašymu pagal DAA 52 straipsnio 4 dalį arba kai už prašymą pagal DAA 53 straipsnį yra paimamas mokestis (jei jis imamas).

([119]) 2018 m. DAA 53 straipsnio 1 dalis.

([120]) Remiantis informacijos komisaro gairėmis, duomenų valdytojas gali nuspręsti paimti mokestį iš duomenų subjekto, jeigu duomenų subjekto prašymas yra akivaizdžiai nepagrįstas arba perteklinis, tačiau duomenų valdytojas vis tiek nusprendžia jį patenkinti. Mokestis turi būti pagrįstas ir juo turi būti galima pagrįsti išlaidas. Duomenų tvarkymo teisėsaugos tikslais gairė „Akivaizdžiai nepagrįsti ir pertekliniai prašymai“; galima rasti šiuo adresu: 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. Duomenų subjekto teisių apribojimai ir pareigos laikytis skaidrumo

(66) Kompetentinga institucija tam tikromis aplinkybėmis gali apriboti tam tikras duomenų subjekto teises: teisę susipažinti su duomenimis ([121]), teisę būti informuotam ([122]), teisę žinoti apie asmens duomenų saugumo pažeidimą ([123]) ir teisę būti informuotam apie prašymo ištaisyti arba ištrinti duomenis atmetimo priežastį ([124]). Panašiai kaip pagal Direktyvos (ES) 2016/680 III skyriuje nustatytą tvarką, kompetentinga institucija gali taikyti apribojimą tik tada, kai apribojimas, atsižvelgiant į duomenų subjekto pagrindines teises ir teisėtus interesus, yra būtinas ir proporcingas siekiant: a) netrukdyti pateikti oficialias ar teisines užklausas, atlikti tyrimus ar procedūras; b) išvengti kenkimo nusikalstamų veikų prevencijai, atskleidimui, tyrimui ir baudžiamajam persekiojimui už jas arba baudžiamųjų sankcijų vykdymui; c) užtikrinti visuomenės saugumą; d) užtikrinti nacionalinį saugumą; e) apsaugoti kitų asmenų teises ir laisves.

(67) Informacijos komisaras yra parengęs gaires dėl šių apribojimų taikymo. Remiantis šiomis gairėmis, duomenų valdytojai kiekvienu atveju turi atlikti analizę ir įvertinti asmens teises bei tai, kokią žalą gali padaryti duomenų atskleidimas. Reikėtų pabrėžti, kad duomenų valdytojai turi pagrįsti, kad visi taikyti apribojimai buvo būtini ir proporcingi, o apriboti suteikiamus dalykus gali tik tada, jei jie trukdytų siekti pirmiau nurodytų tikslų ([125]).

(68) Kompetentingos institucijos taip pat yra parengusios įvairių kitų gairių, kuriose išdėstyta išsami informacija visais duomenų apsaugos teisės aktų aspektais, įskaitant duomenų subjektų teisių apribojimų taikymą ([126]). Pavyzdžiui, dėl 45 straipsnio 4 dalies Nacionalinės policijos vadovų tarybos Duomenų apsaugos vadove yra nurodyta: „Svarbu pažymėti, kad apribojimai gali būti taikomi tik tokia apimtimi ir tik tiek laiko, kiek tai yra būtina. Todėl apribojimo taikyti visiems pareiškėjo asmens duomenims arba visą laiką, neatsižvelgiant į nieką, negalima. Dėl pastarojo aspekto pažymėtina, kad dažnai iš pradžių reikia saugoti, kad duomenų subjektui, kuris tyrime yra įtariamasis, nežinant surinkti asmens duomenys nebūtų jam atskleisti ir nebūtų pakenkta vykdomam tyrimui, tačiau vėliau, per apklausą asmens duomenis atskleidus duomenų subjektui, žalos nepadaroma. Policijos pajėgos privalo parengti procedūras kuriomis užtikrintų, kad šie apribojimai būtų taikomi tik ta apimtimi ir tik tiek laiko, kiek yra būtina“ ([127]). Šiame vadove taip pat pateikta pavyzdžių apie kiekvieną apribojimą, kada labiausiai tikėtina, kad jis bus taikomas ([128]).

(69) Kalbant apie galimybę apriboti pirmiau minėtas teises „nacionalinio saugumo“ užtikrinimo tikslais, pažymėtina, kad duomenų valdytojas gali prašyti išduoti ministrų kabineto arba generalinio prokuroro (Škotijoje – generalinio prokuroro) pasirašytą sertifikatą, kuriame būtų patvirtinta, kad teisių apribojimas yra būtina ir proporcinga priemonė nacionaliniam saugumui užtikrinti ([129]). Jungtinė Karalystė yra parengusi gaires dėl nacionalinio saugumo sertifikatų pagal 2018 m. DAA, o jose yra pabrėžiama, kad duomenų subjektų teisių apribojimas nacionaliniam saugumui užtikrinti privalo būti proporcingas ir reikalingas ([130]) (daugiau apie nacionalinio saugumo sertifikatus žr. 131–134 konstatuojamąsias dalis).

([121]) 2018 m. DAA 45 straipsnio 4 dalis.
([122]) 2018 m. DAA 44 straipsnio 4 dalis.
([123]) 2018 m. DAA 68 straipsnio 7 dalis.
([124]) 2018 m. DAA 48 straipsnio 3 dalis.
([125]) Pvz., žr. Duomenų tvarkymo teisėsaugos tikslais gairę dėl teisės susipažinti su duomenimis; galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Pvz., žr. Nacionalinės policijos vadovų tarybos Policijos duomenų apsaugos specialistams skirtą duomenų apsaugos vadovą (žr. 27 išnašą) arba Sunkių sukčiavimo nusikaltimų tarnybos gaires, kurias galima rasti šiuo adresu: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Nacionalinės policijos vadovų tarybos Duomenų apsaugos vadovas, p. 140 (žr. 27 išnašą).
([128]) Nacionalinės policijos vadovų tarybos Duomenų apsaugos vadove nurodyta, kad punktas: „vengti trukdyti oficialiai arba teisinei apklausai, tyrimui arba procedūrai“ greičiausiai bus aktualus tais atvejais, kai atitinkami asmens duomenys tvarkomi tyrimų, šeimos teismo bylų, nebaudžiamųjų vidaus drausminių tyrimų ir kitų tyrimų, pavyzdžiui, nepriklausomų vaikų lytinio išnaudojimo tyrimų tikslais, punktas „saugoti kitų teises ir laisves“ aktualus tais atvejais, kai asmens duomenys taip pat yra susiję su kitais asmenimis ir pareiškėju“ (Nacionalinės policijos vadovų tarybos Duomenų apsaugos vadovas, p. 140, žr. 27 išnašą).
([129]) 2018 m. DAA 79 straipsnis.
([130]) Jungtinės Karalystės gairės dėl nacionalinio saugumo sertifikatų; galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Be to, kai duomenų subjekto teisės apribojamos, kompetentinga institucija privalo nedelsdama informuoti duomenų subjektą apie tai, kurios jo teisės apribotos, apribojimo priežastis ir galimas teisių gynimo priemones, nebent suteikus tokią informaciją būtų pakenkta tam, dėl ko apribojimas taikytas ([131]). Duomenų valdytojas privalo taikyti dar vieną apsaugos nuo piktnaudžiavimo apribojimais apsaugos priemonę – registruoti informacijos apribojimo priežastis ir pateikti registro įrašus informacijos komisarui, jeigu to paprašoma ([132]).

(71) Jeigu duomenų valdytojas atsisako suteikti papildomą skaidrią informaciją, neleidžia susipažinti su duomenimis arba atmeta prašymą duomenis ištaisyti, ištrinti arba apriboti jų tvarkymą, asmuo gali prašyti informacijos komisaro ištirti, ar duomenų valdytojas apribojimą taikė teisėtai ([133]). Suinteresuotasis asmuo taip pat gali pateikti skundą informacijos komisarui arba kreiptis į teismą, kad jis nurodytų patenkinti prašymą ([134]).

2.4.7.2. Automatizuotas sprendimų priėmimas

(72) 2018 m. DAA 49 ir 50 straipsniais atitinkamai reglamentuojamos su automatizuotu sprendimų priėmimu ir taikytinomis apsaugos priemonėmis susijusios teisės ([135]). Panašiai kaip Direktyvos (ES) 2016/680 11 straipsnyje, duomenų valdytojas gali priimti reikšmingą sprendimą remdamasis vien tik automatizuotai tvarkytais asmens duomenimis tik tada, jei to reikalaujama arba tai leidžiama pagal įstatymą ([136]). Sprendimas yra reikšmingas, jeigu padarytų neigiamą teisinį poveikį duomenų subjektui arba reikšmingai paveiktų duomenų subjektą ([137]).

(73) Tiems atvejams, kai pagal įstatymą iš duomenų valdytojo reikalaujama arba jam leidžiama priimti reikšmingus sprendimus, 2018 m. DAA 50 straipsnyje yra nustatytos apsaugos priemonės, kurios būtų taikomos tokiam sprendimui (jis vadinamas „kriterijus atitinkantis reikšmingas sprendimas“). Duomenų valdytojas privalo, kai tik gali, pranešti duomenų subjektui, kad toks sprendimas buvo priimtas. Duomenų subjektas tuomet gali per vieną mėnesį pareikalauti, kad duomenų valdytojas persvarstytų sprendimą arba priimtų naują sprendimą, kuris nebūtų grindžiamas tik automatizuotu duomenų tvarkymu. Duomenų valdytojas privalo išnagrinėti prašymą ir pranešti duomenų subjektui apie nagrinėjimo rezultatus. Pagal 2018 m. DAA valstybės sekretoriui suteikiami įgaliojimai priimti taisykles dėl papildomų apsaugos priemonių ([138]). Kol kas tokios taisyklės dar nepriimtos.

2.4.8. *Tolesnis perdavimas*

(74) Asmens duomenims, kuriuos valstybės narės teisėsaugos institucija perduoda Jungtinės Karalystės teisėsaugos institucijai, užtikrinamas apsaugos lygis neturėtų sumažėti tokius duomenis toliau perduodant gavėjams trečiojoje valstybėje. Toks „tolesnis perdavimas“, kuris Jungtinės Karalystės teisėsaugos institucijos požiūriu laikomas tarptautiniu perdavimu iš Jungtinės Karalystės, turėtų būti leidžiamas tik tada, kai tolesniam gavėjui, esančiam už Jungtinės Karalystės ribų, taikomos taisyklės, kuriomis užtikrinama panašaus lygio apsauga kaip Jungtinės Karalystės teisinėje sistemoje.

([131]) 2018 m. DAA 44 straipsnio 5 ir 6 dalys, 45 straipsnio 5 ir 6 dalys, 48 straipsnio 4 dalis.
([132]) 2018 m. DAA 44 straipsnio 7 dalis, 45 straipsnio 7 dalis, 48 straipsnio 6 dalis.
([133]) 2018 m. DAA 51 straipsnis.
([134]) 2018 m. DAA 167 straipsnis.
([135]) Dėl automatizuoto duomenų tvarkymo apimties 2018 m. DAA aiškinamosiose pastabose yra nurodyta: „Šios nuostatos taikomos visiškai automatizuotam sprendimų priėmimui, ne automatizuotam duomenų tvarkymui. Automatizuotas duomenų tvarkymas (įskaitant profiliavimą) yra toks duomenų tvarkymas, kai operacijai su duomenimis atlikti nereikalingas žmogaus įsikišimas. Jis yra reguliariai naudojamas teisėsaugos tikslais siekiant suskirstyti didelius duomenų rinkinius į tokio dydžio rinkinius, kuriuos galėtų naudoti žmogus. Automatizuotas sprendimų priėmimas yra tam tikros formos automatizuotas duomenų tvarkymas, kai galutinis sprendimas priimamas be žmogaus įsikišimo“. (DAA aiškinamųjų pastabų 204 dalis, žr. 45 išnašą).
([136]) Be DAA numatytosios apsaugos Jungtinės Karalystės teisinėje sistemoje yra numatyta ir kitų teisėsaugos įstaigoms taikomų įstatyminių apribojimų, kuriais draudžiama vykdyti automatizuotą duomenų tvarkymą (įskaitant profiliavimą), sudarantį sąlygas diskriminavimui. 1998 m. Žmogaus teisių aktu į Jungtinės Karalystės teisę perkeltos Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje įtvirtintos teisės, įskaitant šios konvencijos 14 straipsnyje nustatytą draudimą diskriminuoti. Be to, 2010 m. Lygybės aktu uždrausta diskriminuoti tam tikrų ginamų savybių (pvz., lyties, rasės, negalios ir pan.) turinčius žmones.
([137]) 2018 m. DAA 49 straipsnio 2 dalis.
([138]) 2018 m. DAA 50 straipsnio 4 dalis.

(75) Jungtinėje Karalystėje taikoma tarptautinio duomenų perdavimo tvarka yra nustatyta 2018 m. DAA 3 dalies 5 skyriuje ([139]) ir atitinka poziciją, kurios laikomasi Direktyvos (ES) 2016/680 V skyriuje. Visų pirma pažymėtina, kad, norėdama perduoti asmens duomenis trečiajai valstybei, kompetentinga institucija turi atitikti tris sąlygas: a) duomenis perduoti turi būti būtina teisėsaugos tikslu; b) duomenys turi būti perduodami remiantis: i) dėl trečiosios valstybės priimtomis taisyklėmis dėl duomenų apsaugos tinkamumo; ii) jeigu duomenų perdavimo pagrindas yra ne taisyklės dėl duomenų apsaugos tinkamumo, turi būti įdiegtos tinkamos apsaugos priemonės; iii) jeigu duomenų perdavimo pagrindas yra ne sprendimas dėl duomenų apsaugos tinkamumo arba tinkamos apsaugos priemonės, turi būti susiklosčiusios specialios aplinkybės; c) perduodamų duomenų gavėjas turi būti: i) atitinkama trečiosios valstybės institucija (t. y. kompetentingos institucijos atitikmuo); ii) atitinkama tarptautinė organizacija, pvz., tarptautinė organizacija, vykdanti kurį nors teisėsaugos tikslą atitinkančias funkcijas; iii) kitas asmuo, ne atitinkama institucija, tačiau tik tada, kai duomenis perduoti yra būtinai reikalinga kuriam nors teisėsaugos tikslui įgyvendinti; jokios atitinkamų duomenų subjektų pagrindinės teisės ir laisvės nėra viršesnės už viešąjį interesą, dėl kurio konkrečiu atveju būtina perduoti duomenis; asmens duomenis perduoti atitinkamai trečiosios valstybės institucijai būtų neefektyvu arba netikslinga; gavėjas yra informuojamas apie tai, kokiais tikslais duomenys gali būti tvarkomi ([140]).

(76) Taisykles dėl trečiosios valstybės, trečiosios valstybės teritorijos, sektoriaus arba tarptautinės organizacijos duomenų apsaugos tinkamumo arba tos valstybės, teritorijos, sektoriaus arba organizacijos aprašą ([141]) tvirtina valstybės sekretorius. Dėl to, kokio standarto turi būti laikomasi, pažymėtina, kad valstybės sektorius turi įvertinti, ar tokia teritorija (sektorius, organizacija) užtikrina tinkamą asmens duomenų apsaugos lygį. 2018 m. DAA 74A straipsnio 4 dalyje yra nurodyta, kad šiuo tikslu valstybės sekretorius privalo atsižvelgti į daugelį aspektų, o jie yra panašūs į Direktyvos (ES) 2016/680 36 straipsnyje įtvirtintus aspektus ([142]). Šiuo atžvilgiu pažymėtina, kad pereinamajam laikotarpiui pasibaigus, 2018 m. DAA 3 dalis bus laikoma, kaip buvo paaiškinta, „pagal ES teisę priimta vidaus teisės norma“, o Jungtinės Karalystės teismai ją aiškindami remsis atitinkama Teisingumo Teismo jurisprudencija, suformuota iki Jungtinės Karalystės išstojimo iš Sąjungos, ir Sąjungos teisės bendraisiais principais, kurie galiojo prieš baigiantis pereinamajam laikotarpiui. Prie jų priskirtinas ir „esminio lygiavertiškumo“ kriterijus, tad Jungtinės Karalystės institucijos, atlikdamos vertinimus, juo vadovausis.

(77) Dėl procedūros aspektų pažymėtina, kad taisyklėms dėl duomenų apsaugos tinkamumo taikomi „bendrieji“ procedūriniai reikalavimai, nustatyti 2018 m. DAA 182 straipsnyje. Pagal šią procedūrą priimdamas Jungtinės Karalystės taisykles dėl duomenų apsaugos tinkamumo valstybės sekretorius privalo konsultuotis su informacijos

([139]) Ši nauja tvarka, įskaitant valstybės sekretoriaus įgaliojimus priimti taisykles dėl duomenų apsaugos tinkamumo, įsigalioja pereinamojo laikotarpio pabaigoje. Tačiau DAPER taisyklėse (ypač 21 priedo 10–12 dalyse, kuriomis šiomis taisyklėmis yra įterpiamos į 2018 m. DAA) nustatyta, kad tam tikras asmens duomenų perdavimas pereinamuoju laikotarpiu arba jo pabaigoje yra vykdomas taip, lyg būtų paremtas taisyklėmis dėl duomenų apsaugos tinkamumo. Prie tokio duomenų perdavimo priskiriamas duomenų perdavimas trečiosioms valstybėms, dėl kurių pereinamojo laikotarpio pabaigoje galioja sprendimas dėl duomenų apsaugos tinkamumo, ES valstybėms narėms, ELPA valstybėms ir Gibraltaro teritorijai, kurie duomenų tvarkymui teisėsaugos tikslais taiko Teisėsaugos direktyvą (ELPA valstybės taiko Direktyvą (ES) 2016/680, laikydamosi savo įsipareigojimų pagal Šengeno *acquis*. Tai reiškia, kad pereinamojo laikotarpio pabaigoje duomenys toms valstybėms gali būti toliau perduodami taip kaip iki išstojimo iš ES. Pasibaigus pereinamajam laikotarpiui, valstybės sekretorius privalo per ketverius metus peržiūrėti šias išvadas dėl duomenų apsaugos tinkamumo.

([140]) 2018 m. DAA 73 ir 77 straipsniai.

([141]) Jungtinės Karalystės institucijos paaiškino, kad valstybės arba tarptautinės organizacijos apraše nurodoma, kada būtų reikalinga priimti sprendimą dėl konkretaus arba dalinio duomenų apsaugos tinkamumo, kuriame būtų nustatyti konkretūs apribojimai (pvz., taisyklės dėl duomenų apsaugos tinkamumo, skirtos tik tam tikrų rūšių duomenų perdavimui).

([142]) Žr. 2018 m. DAA 74A straipsnio 4 dalį, kurioje nurodyta, kad vertindamas duomenų apsaugos lygio pakankamumą, „valstybės sekretorius pirmiausia turi atsižvelgti į a) teisinės valstybės principą, pagarbą žmogaus teisėms ir pagrindinėms laisvėms, atitinkamus teisės aktus – tiek bendruosius, tiek sektorinius, įskaitant teisės aktus dėl visuomenės saugumo, gynybos, nacionalinio saugumo, baudžiamosios teisės ir valstybės institucijų prieigos prie asmens duomenų, tokių teisės aktų įgyvendinimą, duomenų apsaugos taisykles, profesines taisykles ir apsaugos priemones, įskaitant taisykles dėl tolesnio asmens duomenų perdavimo kitai trečiajai valstybei arba tarptautinei organizacijai, kurių yra laikomasi toje šalyje arba tarptautinėje organizacijoje, taip pat į faktines ir įstatymais garantuotas duomenų subjekto teises ir veiksmingas administracines ir teismines duomenų subjektų, kurių duomenys buvo perduoti, teisių gynimo priemones; b) tai, ar trečiojoje valstybėje yra arba ar tarptautinę organizaciją prižiūri ir ar veiksmingai dirba viena arba kelios nepriklausomos priežiūros institucijos, kurios užtikrintų, kad būtų laikomasi duomenų apsaugos taisyklių ir imtųsi priverstinių jų vykdymo priemonių, įskaitant pakankamus įgaliojimus imtis priverstinio vykdymo priemonių, teiktų pagalbą duomenų subjektams ir juos konsultuotų kaip naudotis savo teisėmis, taip pat bendradarbiautų su komisaru, ir c) trečiosios valstybės arba atitinkamos tarptautinės organizacijos prisiimtus tarptautinius įsipareigojimus arba kitas pareigas, kurios kyla pagal teisiškai privalomas konvencijas arba dokumentus, taip pat įsipareigojimus ir pareigas dėl dalyvavimo daugiašalėse arba regioninėse sistemose, ypač susijusiose su asmens duomenų apsauga“.

komisaru ([143]). Valstybės sekretoriaus priimtos taisyklės teikiamos parlamentui ir joms taikoma „neigiamos rezoliucijos“ procedūra, pagal kurią abeji parlamento rūmai gali išsamiai išnagrinėti taisykles ir per 40 dienų priimti pasiūlymą jas panaikinti ([144]).

(78) Pagal 2018 m. DAA 74B straipsnio 1 dalį taisyklės dėl duomenų apsaugos tinkamumo turi būti peržiūrimos ne rečiau kaip kas ketverius metus ir valstybės sekretorius privalo nuolat stebėti pokyčius trečiosiose valstybėse ir tarptautinėse organizacijose, kurie gali turėti įtakos sprendimams nustatyti, iš dalies pakeisti arba panaikinti taisykles dėl duomenų apsaugos tinkamumo. Jeigu valstybės sekretorius sužino, kad kuri nors valstybė arba organizacija nebeužtikrina tinkamo asmens duomenų apsaugos lygio, jis privalo, kiek tai reikalinga, iš dalies pakeisti arba panaikinti taisykles ir pradėti konsultacijas su atitinkama trečiąja valstybe arba tarptautine organizacija, kad duomenų apsaugos tinkamumo spragos būtų pašalintos.

(79) Panašiai kaip pagal Direktyvos (ES) 2016/680 37 straipsnį, jeigu taisyklių dėl duomenų apsaugos tinkamumo nėra, asmens duomenis teisėsaugos sektoriuje perduoti bus galima tada, kai bus įdiegtos tinkamos apsaugos priemonės. Tokios apsaugos priemonės užtikrinamos a) teisiškai privalomu dokumentu, kuriame nustatomos tinkamos asmens duomenų apsaugos priemonės, arba b) duomenų valdytojo atliekamais vertinimais, kai, įvertinęs visas duomenų perdavimo aplinkybes, duomenų valdytojas padaro išvadą, kad tinkamos duomenų apsaugos priemonės yra taikomos ([145]). 2018 m. DAA taip pat nustatyta, kad tais atvejais, kai duomenų perdavimas yra grindžiamas tinkamomis apsaugos priemonėmis, informacijos komisaras vykdo ne tik įprastas priežiūros funkcijas – kompetentingos institucijos privalo perduoti informacijos pareigūnui specialią informaciją apie duomenų perdavimus ([146]).

(80) Jeigu duomenų perdavimo pagrindas yra ne sprendimas dėl duomenų apsaugos tinkamumo arba tinkamos apsaugos priemonės, duomenys gali būti perduodami tik susiklosčius tam tikroms, vadinamosioms „specialioms aplinkybėms“ ([147]). Pavyzdžiui, duomenis perduoti būtina: a) kad būtų apsaugoti gyvybiniai duomenų subjekto arba kito asmens interesai; b) kad būtų apsaugoti teisėti duomenų subjekto interesai; c) kad būtų užkirstas kelias tiesioginei ir didelei grėsmei trečiosios valstybės visuomenės saugumui; d) individualiais atvejais bet kuriuo iš teisėsaugos tikslų arba e) individualiais atvejais teisėtu tikslu (pvz., dėl teismo proceso arba siekiant gauti teisinę konsultaciją) ([148]). Galima pažymėti, kad d ir e punktai netaikomi, jeigu duomenų subjekto teisės ir laisvės yra viršesnės už su perdavimu susijusį viešąjį interesą ([149]). Šios aplinkybės atitinka konkrečias situacijas ir sąlygas, kurios pagal Direktyvos (ES) 2016/680 38 straipsnį laikomos „nukrypti leidžiančiomis nuostatomis“.

(81) Tokiomis aplinkybėmis duomenų perdavimo data, laikas, pagrindimas, gavėjo vardas, pavardė, kita aktuali informacija apie gavėją ir perduotų asmens duomenų aprašas yra dokumentuojami ir, jei to prašoma, pateikiami informacijos komisarui ([150]).

(82) Pagal 2018 m. DAA 78 straipsnį reglamentuojami „paskesnio perdavimo“ atvejai, t. y. atvejai, kai asmens duomenys perduodami iš Jungtinės Karalystės į trečiąją valstybę, o vėliau – kitai trečiajai valstybei arba tarptautinei organizacijai. Pagal 78 straipsnio 1 dalį Jungtinės Karalystės duomenis perduodantis duomenų valdytojas privalo nustatyti duomenų perdavimo sąlygą, kad duomenys negali būti toliau perduoti kitai trečiajai valstybei be duomenų valdytojo leidimo. Be to, pagal 78 straipsnio 3 dalį, panašiai kaip pagal Direktyvos (ES) 2016/680 35 straipsnio 1 dalies e punktą, tais atvejais, kai toks leidimas reikalingas, taikomi keli materialiniai reikalavimai.

([143]) Žr. valstybės sekretoriaus, veikiančio Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamento vardu, ir Informacijos komisaro biuro susitarimo memorandumą dėl Informacijos komisaro vaidmens vertinant Jungtinėje Karalystėje užtikrinamos duomenų apsaugos tinkamumą; su juo galima susipažinti šiuo adresu: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Per šį 40 dienų laikotarpį abeji Parlamento rūmai gali, jei to pageidauja, balsuoti prieš taisykles. Jeigu būtų pabalsuota prieš taisykles, jos netektų tolesnės teisinės galios.

([145]) 2018 m. DAA 75 straipsnis.

([146]) Remiantis 2018 m. DAA 75 straipsnio 3 dalimi, jeigu duomenys perduodami kliaujantis tuo, kad tinkamos apsaugos priemonės yra įdiegtos: a) duomenų perdavimas turi būti dokumentuotas; b) komisarui paprašius, dokumentai turi būti jam pateikti ir c) dokumentuose visų pirma turi būti šie duomenys: i) duomenų perdavimo data ir laikas; ii) gavėjo vardas, pavardė ir kita informacija apie jį; iii) duomenų perdavimo pagrindimas ir iv) perduotų asmens duomenų aprašas.

([147]) Duomenų tvarkymo teisėsaugos srityje gairė „Ar yra specialių aplinkybių?“; galima rasti šiuo adresu: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

([148]) 2018 m. DAA 76 straipsnis.

([149]) 2018 m. DAA 76 straipsnis.

([150]) 2018 m. DAA 76 straipsnio 3 dalis.

T. y. priimdama sprendimą, ar leisti, ar neleisti perduoti duomenis, kompetentinga institucija turi įsitikinti, kad tolesnis duomenų perdavimas yra būtinas teisėsaugos tikslu, ir, be kitų dalykų, atsižvelgti į a) aplinkybių, dėl kurių prašoma leisti perduoti duomenis, svarbą; b) tikslą, kuriam duomenys buvo perduoti iš pradžių, ir c) trečiojoje valstybėje arba tarptautinėje organizacijoje, kuriai asmens duomenys būtų perduoti, taikomus duomenų apsaugos standartus.

(83) Be to, jei duomenys, kuriuos ketinama iš Jungtinės Karalystės perduoti toliau, prieš tai buvo perduoti iš Europos Sąjungos, taikomos papildomos apsaugos priemonės.

(84) Pirma, 2018 m. DAA 73 straipsnio 1 dalies b punkte, panašiai kaip Direktyvos (ES) 2016/680 35 straipsnio 1 dalies c punkte, nustatyta, kad tuo atveju, jeigu asmens duomenis duomenų valdytojui arba kitai kompetentingai institucijai iš pradžių perdavė arba suteikė valstybė narė, laikoma, kad ta valstybė narė arba bet kuris joje veikiantis asmuo, kuris pagal Direktyvą (ES) 2016/680 laikomas kompetentinga institucija, turi leisti juos perduoti pagal valstybės narės teisės aktus.

(85) Tačiau, panašiai kaip pagal Direktyvos (ES) 2016/680 35 straipsnio 2 dalį, toks leidimas nėra reikalaujamas, jeigu a) duomenis būtina perduoti siekiant užkirsti kelią tiesioginei ir didelei grėsmei valstybės narės arba trečiosios valstybės visuomenės saugumui arba valstybės narės esminiams interesams, o b) išankstinio leidimo laiku gauti neįmanoma. Tokiu atveju nedelsiant informuojama valstybės narės institucija, kuri būtų turėjusi priimti sprendimą, ar leisti perduoti duomenis ([151]).

(86) Antra, tas pats principas taikomas duomenims, kurie pirmiausia buvo perduoti iš Sąjungos Jungtinei Karalystei, o tuomet Jungtinės Karalystės perduoti trečiajai šaliai, kuri vėliau juos perduoda trečiajai šaliai. Tokiu atveju pagal 78 skyriaus 4 dalį Jungtinės Karalystės kompetentinga institucija negali suteikti leidimo perduoti duomenis pagal 78 straipsnio 1 dalį, išskyrus atvejus, kai „valstybė narė [pirmiau perdavusi atitinkamus duomenis] arba bet kuris toje valstybėje narėje veikiantis subjektas, kuris yra kompetentinga institucija Teisėsaugos direktyvos prasme, leido perduoti duomenis pagal tos valstybės narės teisę“. Šios apsaugos priemonės yra svarbios, nes taip valstybių narių valdžios institucijos gali visoje duomenų perdavimo grandinėje užtikrinti apsaugos tęstinumą pagal ES duomenų apsaugos teisės aktus.

(87) Ši nauja tarptautinio duomenų perdavimo sistema pradėta taikyti pereinamojo laikotarpio pabaigoje ([152]). Tačiau 21 priedo 10–12 dalyse (kurios buvo įtrauktos pagal DAPER taisykles) nustatyta, kad, pereinamajam laikotarpiui pasibaigus, tam tikrais atvejais bus laikoma, kad duomenų perdavimo pagrindą sudaro taisyklės dėl duomenų apsaugos tinkamumo. Prie šio pobūdžio duomenų perdavimo priskiriamas duomenų perdavimas valstybei narei, ELPA valstybei, trečiajai šaliai, kurios atžvilgiu pereinamojo laikotarpio pabaigoje galiojo ES sprendimas dėl duomenų apsaugos tinkamumo, ar Gibraltaro teritorijai. Todėl duomenų perdavimas į šias valstybes gali būti toliau atliekamas tokia pat tvarka, kaip iki Jungtinės Karalystės išstojimo iš Sąjungos. Pasibaigus pereinamajam laikotarpiui, valstybės sekretorius privalo per ketverius metus, t. y. iki 2024 m. gruodžio mėn. pabaigos, peržiūrėti šias išvadas dėl duomenų apsaugos tinkamumo. Kaip nurodyta Jungtinės Karalystės institucijų pateiktame paaiškinime, nors valstybės sekretorius tokią peržiūrą turi atlikti iki 2024 m. gruodžio mėn. pabaigos, į pereinamojo laikotarpio nuostatas laikino galiojimo sąlyga neįtraukta, todėl, jeigu peržiūra iki 2024 m. gruodžio mėn. pabaigos nebus užbaigta, atitinkamos pereinamojo laikotarpio nuostatos savaime nenustos galioti.

2.4.9. *Atskaitomybė*

(88) Pagal atskaitomybės principą duomenis tvarkančios valdžios institucijos privalo įdiegti tinkamas technines ir organizacines priemones, kad galėtų veiksmingai laikytis savo duomenų apsaugos pareigų ir įrodyti (visų pirma kompetentingai priežiūros institucijai), kad jų laikosi.

(89) Šis principas įtvirtintas 2018 m. DAA 56 straipsnyje, kuriame yra nustatyta bendra duomenų valdytojo atskaitomybės pareiga, t. y. pareiga įdiegti tinkamas technines ir organizacines priemones, kuriomis būtų užtikrinta, kad asmens duomenų tvarkymas atitiktų 2018 m. DAA 3 dalies reikalavimus ir kad jis galėtų tai įrodyti. Įdiegtos priemonės turi būti peržiūrėtos ir atnaujintos, kai, atsižvelgiant duomenų tvarkymą, tai yra reikalinga ir proporcinga, jos taip pat turi atitikti reikiamą duomenų tvarkymo politiką.

([151]) 2018 m. DAA 73 straipsnio 5 dalis.

([152]) Ši nauja sistema turi būti taikoma atsižvelgiant į Europos Sąjungos bei Europos atominės energijos bendrijos ir Jungtinės Didžiosios Britanijos ir Šiaurės Airijos Karalystės prekybos ir bendradarbiavimo susitarimo 782 straipsnį (L 444, 2020 12 31, p. 14) (toliau – ES ir Jungtinės Karalystės prekybos ir bendradarbiavimo susitarimas); galima rasti šiuo adresu: https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:22020A1231(01)&from=LT.

(90) Kaip ir Direktyvos (ES) 2016/680 IV skyriuje, 2018 m. DAA 55–71 straipsniuose nustatyti įvairūs atskaitomybės užtikrinimo mechanizmai, kuriais naudodamiesi duomenų valdytojai bei tvarkytojai gali įrodyti, kad laikosi reikalavimų. Visų pirma, duomenų valdytojai privalo įdiegti pritaikytąsias ir standartizuotąsias duomenų apsaugos priemones, t. y. užtikrinti, kad duomenų apsaugos principai būtų veiksmingai įgyvendinami, taip pat privalo saugoti visų kategorijų duomenų tvarkymo veiklos, už kurią yra atsakingi, įrašus (įskaitant informaciją apie duomenų valdytojo tapatybę, duomenų apsaugos pareigūno kontaktinius duomenis, duomenų tvarkymo tikslus, atskleidžiamų duomenų gavėjų kategorijas, duomenų subjekto kategorijų aprašą ir asmens duomenis) ir, jei to prašoma, pateikti šiuos įrašus informacijos komisarui. Duomenų valdytojas ir tvarkytojas privalo vesti tam tikrų duomenų tvarkymo operacijų žurnalus ir pateikti juos informacijos komisarui ([153]). Duomenų valdytojų taip pat konkrečiai reikalaujama vykdant savo funkcijas bendradarbiauti su informacijos komisaru.

(91) 2018 m. DAA taip pat nustatyti papildomi reikalavimai duomenų tvarkymui, kuris gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms. Vienas iš reikalavimų – prieš tvarkant duomenis įvertinti poveikį duomenų apsaugai ir, jei iš vertinimo rezultatų matyti, kad duomenų tvarkymas keltų didelį pavojų asmenų teisėms ir laisvėms (kai nėra pavojaus mažinimo priemonių) konsultuotis su informacijos komisaru.

(92) Duomenų valdytojai taip pat privalo paskirti duomenų apsaugos pareigūną, nebent duomenų valdytojas yra teismas arba kita teisminė institucija, vykdanti teismo funkcijas ([154]). Duomenų valdytojas privalo užtikrinti, kad duomenų apsaugos pareigūnas dalyvautų sprendžiant visus su asmens duomenų apsauga susijusius klausimus, turėtų reikiamų išteklių, turėtų prieigą prie asmens duomenų ir duomenų tvarkymo operacijų ir galėtų atlikti savo užduotis savarankiškai. Duomenų apsaugos pareigūno užduotys yra išdėstytos 2018 m. DAA 71 straipsnyje; vieni iš uždavinių yra teikti informaciją ir konsultuoti, stebėti, kaip laikomasi reikalavimų, bendradarbiauti su informacijos komisaru ir būti jo kontaktiniu asmeniu. Vykdydamas savo funkcijas duomenų apsaugos pareigūnas privalo atsižvelgti į su duomenų tvarkymo operacijomis susijusius pavojus ir duomenų apsaugos pobūdį, mastą, aplinkybes bei tikslus.

2.5. **Priežiūra ir vykdymo užtikrinimas**

2.5.1. *Nepriklausoma priežiūra*

(93) Tam, kad tinkamas duomenų apsaugos lygis būtų užtikrinamas ir praktiškai, reikalinga nepriklausoma priežiūros institucija, kuriai būtų suteikti įgaliojimai stebėti, kaip laikomasi duomenų apsaugos taisyklių, ir užtikrinti, kad jų būtų laikomasi. Atlikdama savo pareigas ir naudodamasi savo įgaliojimais ši institucija turi veikti visiškai nepriklausomai ir nešališkai.

(94) Jungtinėje Karalystėje informacijos komisaras atsako už Jungtinės Karalystės BDAR ir 2018 m. DAA priežiūrą ir vykdymo užtikrinimą ([155]). Informacijos komisaras taip pat prižiūri, kaip asmens duomenis tvarko kompetentingos institucijos, patenkančios į 2018 m. DAA 3 dalies taikymo sritį ([156]). Informacijos komisaras yra vienasmenis subjektas – atskiras juridinis asmuo, kurį sudaro vienas fizinis asmuo. Informacijos komisarui talkina biuras. 2020 m. kovo 31 d. Informacijos komisaro biure dirbo 768 nuolatiniai darbuotojai ([157]). Informacijos komisarui padeda Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamentas ([158]).

([153]) 2018 m. DAA 62 straipsnis.
([154]) 2018 m. DAA 69 straipsnis.
([155]) Direktyvos (ES) 2016/680 36 straipsnio 2 dalies b punktas.
([156]) 2018 m. DAA 116 straipsnis.
([157]) Informacijos komisaro 2019–2020 m. metinę ataskaitą ir finansines ataskaitas galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.
([158]) Abiejų subjektų santykiai apibrėžti susitarime dėl valdymo. Pagrindinės pagalbą teikiančio Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamento pareigos: užtikrinti, kad informacijos komisaras būtų pakankamai finansuojamas ir turėtų pakankamai išteklių, atstovauti informacijos komisaro interesams parlamente ir kituose Vyriausybės departamentuose, užtikrinti patikimos nacionalinės duomenų apsaugos sistemos galiojimą ir teikti gaires bei paramą Informacijos komisaro biurui organizaciniais klausimais, pvz., susijusiais su nekilnojamuoju turtu, išperkamąja nuoma ir viešaisiais pirkimais (2018–2021 m. Susitarimas dėl valdymo; galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Komisaro nepriklausomumas aiškiai nustatytas Jungtinės Karalystės BDAR 52 straipsnyje, kuriame išdėstyti reikalavimai atitinka Europos Parlamento ir Tarybos reglamento (ES) 2016/679 ([159]) 52 straipsnio 1–3 dalyse nustatytus reikalavimus. Vykdydamas savo užduotis ir įgyvendindamas savo įgaliojimus pagal Jungtinės Karalystės BDAR, komisaras privalo veikti visiškai nepriklausomai, išlikti nepriklausomas nuo tiesioginės ar netiesioginės išorės įtakos jo vykdomoms užduotims ir įgaliojimams, taip pat neturėtų klausti nurodymų iš jokių asmenų ar jais vadovautis. Komisaras taip pat negali vykdyti jokių su jo pareigomis nesuderinamų veiksmų ir eidamas pareigas negali už atlygį ar be jo užsiimti jokia kita su jomis nesuderinama profesija.

(96) Informacijos komisaro skyrimo ir pašalinimo iš pareigų sąlygos nustatytos 2018 m. DAA 12 priede. Informacijos komisarą skiria Karalienė, atsižvelgdama į Vyriausybės rekomendaciją, sąžiningo ir atviro konkurso būdu. Kandidatas privalo turėti tinkamą kvalifikaciją, įgūdžius ir kompetenciją. Pagal Valstybės pareigūnų skyrimo valdymo kodeksą ([160]) skiriamų kandidatų sąrašą sudaro patariamoji vertintojų kolegija. Prieš Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamentui priimant galutinį sprendimą, atitinkamas atskirasis Parlamento komitetas privalo atlikti numatyto skirti kandidato patikrinimą. Komiteto nuomonė skelbiama viešai ([161]).

(97) Informacijos komisaro kadencija trunka septynerius metus. Informacijos komisarą iš pareigų pašalinti gali Jos Didenybė, remdamasi abiejų parlamento rūmų kreipimusi ([162]). Nė vieni Parlamento rūmai negali pateikti prašymo atleisti informacijos komisarą iš pareigų, kol ministras nepateikia ataskaitos tiems Rūmams ir joje nenurodo, kad, jo įsitikinimu, informacijos komisaras yra kaltas dėl šiurkštaus nusižengimo ir (arba) nebeatitinka sąlygų, keliamų komisaro funkcijas vykdančiam asmeniui ([163]).

(98) Informacijos komisaro veikla finansuojama iš trijų šaltinių: i) duomenų valdytojų sumokamų duomenų apsaugos mokesčių, kurie nustatomi valstybės sekretoriaus taisyklėse ([164]) ir sudaro 85–90 % metinio biuro biudžeto ([165]); ii) dotacijos forma Vyriausybės skiriamos pagalbos informacijos komisarui, kuri iš esmės naudojama informacijos komisaro veiklos išlaidoms, patiriamoms vykdant su duomenų apsauga nesusijusias užduotis, padengti ([166]); iii) už paslaugas sumokėtų mokesčių ([167]). Šiuo metu tokie mokesčiai nerenkami.

(99) Bendrosios informacijos komisaro funkcijos, susijusios su asmens duomenų tvarkymu pagal 2018 m. DAA 3 dalį, nustatytos 2018 m. DAA 13 priede. Prie jų priskiriama 2018 m. DAA 3 dalies vykdymo stebėsena ir vykdymo užtikrinimas, visuomenės informuotumo didinimas, Parlamento, Vyriausybės ir kitų institucijų konsultavimas teisėkūros ir administracinių priemonių klausimais, duomenų valdytojų ir tvarkytojų informuotumo apie jų pareigas didinimas, informacijos teikimas duomenų subjektui apie naudojimąsi duomenų subjekto teisėmis ir

([159]) 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL L 119, 2016 5 4, p. 1).

([160]) Valstybės pareigūnų skyrimo valdymo kodeksas; galima rasti šiuo adresu: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) 2015–2016 m. Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamento sesijos Bendruomenių Rūmuose antroji ataskaita; galima rasti šiuo adresu: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) Kreipimasis – tai parlamentui pateiktas prašymas, kuriuo siekiama informuoti monarchą apie parlamento nuomones konkrečiu klausimu.

([163]) 2018 m. DAA 12 priedo 3 dalis.

([164]) 2018 m. DAA 137 straipsnis.

([165]) 2018 m. DAA 137 ir 138 straipsniuose nustatytos įvairios apsaugos priemonės, kuriomis siekiama užtikrinti, kad nustatyti mokesčiai būtų tinkamo dydžio. Visų pirma, 2018 m. DAA 137 straipsnio 4 dalyje išdėstyta, į ką valstybės sekretorius privalo atsižvelgti priimdamas taisykles, kuriose nurodoma įvairių organizacijų mokėtina suma. 2018 m. DAA 138 straipsnio 1 dalyje ir 182 straipsnyje valstybės sekretoriui taip pat nustatytas teisinis reikalavimas konsultuotis su informacijos komisaru ir kitais asmenų, kuriems taisyklės gali daryti poveikį, atstovais ir taisykles priimti atsižvelgus į jų nuomones. Pagal 2018 m. DAA 138 straipsnio 2 dalį reikalaujama, kad informacijos komisaras nuolat tobulintų mokesčių taisykles, jis taip pat gali pateikti valstybės sekretoriui pasiūlymus dėl taisyklių pakeitimų. Galiausiai, išskyrus tuos atvejus, kai taisyklės priimamos siekiant atsižvelgti į padidėjusį mažmeninių kainų indeksą (tokiu atveju, joms bus taikoma neigiamos rezoliucijos procedūra), taisyklėms taikoma patvirtinamosios rezoliucijos procedūra ir jos negali būti priimtos tol, kol jų savo rezoliucija nepatvirtino kiekvieni parlamento rūmai.

([166]) Susitarime dėl valdymo paaiškinta, kad „valstybės sekretorius gali atlikti mokėjimus informacijos komisarui iš parlamento pagal 2018 m. DAA 12 priedo 9 dalį skirtų lėšų. Pasikonsultavęs su informacijos komisaru, Skaitmeninių, kultūros, žiniasklaidos ir sporto reikalų departamentas sumoka Informacijos komisaro biurui atitinkamas sumas (dotaciją pagalbos forma) informacijos komisaro administracinėms išlaidoms ir su įvairiomis konkrečiomis funkcijomis, įskaitant informacijos laisvę, susijusioms išlaidoms padengti“ (2018–2021 m. susitarimo dėl valdymo 1.12 dalis, žr. 158 išnašą).

([167]) 2018 m. DAA 134 straipsnis.

tyrimų vykdymas. Siekiant išsaugoti teismų nepriklausomumą, informacijos komisarui neleidžiama vykdyti savo funkcijų tais atvejais, kai asmens duomenis tvarko teisminius įgaliojimus turintis fizinis asmuo arba teismines funkcijas vykdantis bendrosios kompetencijos arba specializuotas teismas. Tačiau teismų priežiūrą užtikrina toliau aptartos specializuotos įstaigos.

2.5.1.1. Vykdymo užtikrinimas, įskaitant sankcijas

(100) Komisaras turi bendruosius tyrimo, taisomuosius, leidimų suteikimo ir patariamuosius įgaliojimus, susijusius su asmens duomenų tvarkymu, kuriam taikoma 2018 m. DAA 3 dalis. Komisaras yra įgaliotas informuoti duomenų valdytoją arba tvarkytoją apie įtarimus, kad buvo pažeistos 3 dalies nuostatos, teikti perspėjimus duomenų valdytojui arba duomenų tvarkytojui, kad ketinamomis vykdyti duomenų tvarkymo operacijomis gali būti pažeistos 3 dalies nuostatos ir, jeigu duomenų tvarkymo operacijomis 3 dalies nuostatos pažeidžiamos, skirti duomenų valdytojui arba tvarkytojui papeikimus. Be to, komisaras savo iniciatyva arba remdamasis gautu prašymu gali teikti nuomones Jungtinės Karalystės parlamentui, Vyriausybei arba kitoms institucijoms, įstaigoms ir visuomenei bet kuriuo su asmens duomenų apsauga susijusiu klausimu ([168]).

(101) Komisaras turi įgaliojimus visų pirma:

— įpareigoti duomenų valdytoją ir duomenų tvarkytoją (ir tam tikrais atvejais bet kurį kitą asmenį) pateikti būtiną informaciją informacinio pranešimo forma (toliau – informacinis pranešimas ([169]);

— atlikti tyrimus ir auditus ir pateikti vertinimo pranešimą, kuriame gali reikalauti, kad duomenų valdytojas arba duomenų tvarkytojas leistų komisarui patekti į konkrečias patalpas, patikrinti arba išnagrinėti dokumentus arba patikrinti ir apžiūrėti įrangą, duomenų valdytojų vardu apklausti asmens duomenis tvarkančius asmenis (toliau – vertinimo pranešimas) ([170]);

— kitais būdais gauti prieigą prie duomenų valdytojų ir duomenų tvarkytojų dokumentų ir patekti į jų patalpas pagal 2018 m. DAA 154 straipsnį (toliau – įgaliojimai patekti į patalpas ir atlikti patikrinimą);

— įgyvendinti taisomuosius įgaliojimus ir, be kita ko, teikti įspėjimus arba papeikimus, išdėstyti nurodymus vykdymo pranešime ir jame reikalauti, kad duomenų valdytojai ir (arba) duomenų tvarkytojai imtųsi konkrečių veiksmų arba jų nesiimtų (toliau – vykdymo pranešimas) ([171]), ir

— skirti administracines baudas paskelbdamas pranešimą apie nuobaudą (toliau – pranešimas apie nuobaudą) ([172]).

(102) Informacijos komisaro reguliavimo veiksmų plane aprašytos aplinkybės, kuriomis jis priima informacinį, vertinimo, vykdymo pranešimą arba pranešimą apie nuobaudą ([173]). Vykdymo pranešime gali būti nustatyti reikalavimai, kurie, komisaro manymu, yra tinkami pažeidimui ištaisyti. Pranešime apie nuobaudą reikalaujama, kad asmuo sumokėtų informacijos komisarui pranešime nurodytą sumą. Pranešimas apie nuobaudą gali būti pateiktas, jeigu nesilaikoma kurių nors 2018 m. DAA nuostatų ([174]), arba toks pranešimas gali būti pateiktas duomenų valdytojui arba tvarkytojui, kuris nesilaikė informacinio pranešimo, vertinimo pranešimo arba vykdymo pranešimo.

(103) Tiksliau, svarstydamas, ar duomenų valdytojui arba tvarkytojui teikti pranešimą apie nuobaudą, ir nustatydamas nuobaudos dydį informacijos komisaras privalo atsižvelgti į 2018 m. DAA 155 straipsnio 3 dalyje išdėstytus dalykus, tarp jų – į pažeidimo pobūdį ir šiurkštumą, ar pažeidimas padarytas tyčia, ar dėl aplaidumo, visus veiksmus, kurių duomenų valdytojas arba duomenų tvarkytojas ėmėsi, kad sumažintų duomenų subjektų patirtą

([168]) 2018 m. DAA 13 priedo 2 dalis.
([169]) 2018 m. DAA 142 straipsnis (taikomi 2018 m. DAA 143 straipsnyje nustatyti apribojimai).
([170]) 2018 m. DAA 146 straipsnis(taikomi 2018 m. DAA 147 straipsnyje nustatyti apribojimai).
([171]) 2018 m. DAA 149–151 straipsniai (taikomi 2018 m. DAA 152 straipsnyje nustatyti apribojimai.
([172]) 2018 m. DAA 155 straipsnis (taikomi 2018 m. DAA 156 straipsnyje nustatyti apribojimai).
([173]) Reguliavimo veiksmų politika; galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Informacijos komisaras pranešimą apie nuobaudą, visų pirma, gali pateikti tada, jeigu nevykdomos 2018 m. DAA 149 straipsnio 2, 3, 4 arba 5 dalyse nurodytos pareigos.

žalą, duomenų valdytojo arba duomenų tvarkytojo atsakomybės laipsnį (atsižvelgiant į duomenų valdytojo arba duomenų tvarkytojo įdiegtas technines arba organizacines priemones) ir visus svarbius ankstesnius duomenų valdytojo arba duomenų tvarkytojo padarytus pažeidimus, asmens duomenų, kuriuos paveikė pažeidimas, kategorijas ir tai, ar nuobauda būtų veiksminga, proporcinga ir atgrasanti.

(104) Didžiausia nuobauda, kuri gali būti skirta pranešimu apie nuobaudą, yra a) 17 500 000 GBP, jeigu nesilaikoma duomenų apsaugos principų (2018 m. DAA 35, 36, 37 straipsnių, 38 straipsnio 1 dalies, 39 straipsnio 1 dalies ir 40 straipsnio), pareigos laikytis skaidrumo ir gerbti asmens teises (2018 m. DAA 44, 45, 46, 47, 48, 49, 52 ir 53 straipsniai) ir asmens duomenų tarptautinio perdavimo principų (2018 m. DAA 73, 75, 76, 77 arba 78 straipsniai) ir b) 8 700 000 GBP kitais atvejais ([175]). Jeigu nesilaikoma informacinio pranešimo, vertinimo pranešimo arba vykdymo pranešimo reikalavimų, didžiausia nuobauda, kurią galima skirti įteikiant pranešimą apie nuobaudą, yra 17 500 000 GBP.

(105) Kaip pažymėta naujausiose metinėse ataskaitose (2018–2019 m. ([176]), 2019–2020 m. ([177])), informacijos komisaras atliko įvairius tyrimus, kaip baudžiamosios teisėsaugos institucijos tvarko asmens duomenis. Pavyzdžiui, komisaras atliko tyrimą ir 2019 m. spalio mėn. paskelbė nuomonę dėl to, kaip teisėsaugos institucijos naudoja veido atpažinimo technologijas viešose vietose. Tyrime ypač daug dėmesio skirta Pietų Velso ir Londono policijos tarnybos naudojamiems gyvo veido atpažinimo pajėgumams. Informacijos komisaras išnagrinėjo Londono policijos tarnybos Gaujų narių duomenų bazę ([178]) ir nustatė įvairių šiurkščių duomenų apsaugos teisės pažeidimų, kurie galėjo sumažinti visuomenės pasitikėjimą šia duomenų baze ir tuo, kaip naudojami duomenys.

(106) 2018 m. lapkričio mėn. informacijos komisaras paskelbė vykdymo pranešimą, o Londono policijos tarnyba atitinkamai ėmėsi būtinų veiksmų, kad padidintų saugumą ir atskaitomybę ir užtikrintų, kad duomenys būtų naudojami proporcingai.

(107) Kitas nesenas šios srities vykdymo veiksmų pavyzdys – 2018 m. gegužės mėn. komisaras skyrė Karalienės prokuratūrai 325 000 GBP baudą už tai, kad pastaroji prarado neužšifruotus DVD su policijos apklausų įrašais. Informacijos komisaras taip pat atliko tyrimus platesnėmis temomis, pavyzdžiui, per pirmąjį 2020 m. pusmetį atliko tyrimą dėl mobiliųjų telefonų duomenų išgavimo policijos veiklos tikslais ir dėl to, kaip policija tvarko aukų duomenis.

(108) Be šių informacijos komisarui suteiktų vykdymo įgaliojimų, taip pat pažymėtina, kad tam tikri duomenų apsaugos teisės aktų pažeidimai laikomi nusikalstamomis veikomis, todėl už jas gali būti skiriamos baudžiamosios sankcijos (2018 m. DAA 196 straipsnis). Pavyzdžiui, baudžiamosios sankcijos gali būti skirtos už tai, kad asmens duomenys buvo gauti arba atskleisti be duomenų valdytojo sutikimo, už tarpininkavimą asmens duomenis atskleidžiant kitam asmeniui be duomenų valdytojo sutikimo ([179]), į informaciją, kurią sudaro nuasmeninti asmens duomenys, vėl įtraukiant tapatybės duomenis be duomenų valdytojo, atsakingo už asmens duomenų nuasmeninimą, sutikimo ([180]), tyčia trukdant komisarui vykdyti savo įgaliojimus, susijusius su asmens duomenų patikrinimu pagal tarptautinius įsipareigojimus ([181]) ir jeigu atsakant į informacinį pranešimą pateikiami klaidingi pareiškimai arba sunaikinama su informaciniu pranešimu arba vertinimo pranešimu susijusi informacija ([182]).

(109) Pagal 2018 m. DAA 139 straipsnį informacijos komisaras taip pat privalo pateikti kiekvieniems Parlamento rūmams bendrą ataskaitą apie tai, kaip vykdė savo funkcijas pagal šį aktą ([183]).

([175]) 2018 m. DAA 157 straipsnis.

([176]) Informacijos komisaro 2018–2019 m. metinę ataskaitą ir finansines ataskaitas galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Informacijos komisaro 2019–2020 m. metinė ataskaita (žr. 157 išnašą).

([178]) Duomenų bazė, kurioje registruojami žvalgybos duomenys, susiję su įtariamais gaujų nariais ir gaujų padarytų nusikaltimų aukomis.

([179]) 2018 m. DAA 170 straipsnis.

([180]) 2018 m. DAA 171 straipsnis.

([181]) 2018 m. DAA 119 straipsnis.

([182]) 2018 m. DAA 144 ir 148 straipsniai.

([183]) Kaip nurodyta susitarime dėl valdymo, metinėje ataskaitoje: i) pateikiama informacija apie visą informacijos komisaro kontroliuojamos organizacijos, jai pavaldžių įstaigų arba bendrų įmonių veiklą; ii) informacija pateikiama pagal Iždo finansinės informacijos teikimo vadovą; iii) pateikiamas vadovybės pareiškimas, kuriame nurodoma, kaip apskaitos pareigūnas per metus administravo ir valdė organizacijos išteklius ir kaip organizacijai sekasi valdyti su jos tikslų ir uždavinių įgyvendinimu susijusią riziką ir iv) aprašoma pagrindinė praėjusių finansinių metų veikla, pasiekti rezultatai ir pateikiama būsimų planų santrauka (2018–2021 m. susitarimo dėl valdymo 3.26 punktas, žr. 158 išnašą);

2.5.2. *Teismų vykdoma priežiūra*

(110) Teismų ir teisminių institucijų vykdomo asmens duomenų tvarkymo priežiūra yra dvejopa. Jeigu teisėjo pareigas einantis asmuo arba teismas veikia ne pagal teisminius įgaliojimus, priežiūrą vykdo informacijos komisaras. Jeigu duomenų valdytojas veikia pagal teisminius įgaliojimus, informacijos komisaras negali vykdyti priežiūros funkcijų ([184]) ir priežiūrą vykdo specialios įstaigos. Tai atitinka poziciją, kurios laikomasi Direktyvos (ES) 2016/680 32 straipsnyje.

(111) Visų pirma pažymėtina, kad antruoju atveju Anglijos ir Velso teismų ir Anglijos ir Velso pirmosios ir aukštesnės instancijos specializuotų teismų priežiūrą atlieka Teisminė duomenų apsaugos kolegija ([185]). Be to, lordas vyriausiasis teisėjas ir vyresnysis specializuotų teismų pirmininkas paskelbtame pareiškime dėl privatumo ([186]) nurodo, kaip Anglijos ir Velso teismai tvarko asmens duomenis teisminių funkcijų vykdymo tikslais. Panašų pranešimą yra paskelbę Šiaurės Airijos ([187]) ir Škotijos teisėjai ([188]).

(112) Be to, Šiaurės Airijoje Šiaurės Airijos lordas vyriausiasis teisėjas paskyrė Aukštojo teismo teisėją eiti už duomenų priežiūrą atsakingo teisėjo pareigas ([189]). Jis taip pat paskelbė Šiaurės Airijos teisėjams skirtas gaires dėl veiksmų, kurių reikia imtis praradus duomenis arba tuo atveju, jeigu jie gali būti prarasti, ir gaires dėl to, kokia tvarka reikia spręsti visus su tuo susijusius klausimus ([190]).

(113) Škotijoje lordas pirmininkas paskyrė už duomenų priežiūrą atsakingą teisėją tirti visus su duomenų apsauga susijusiais pagrindais teikiamus skundus. Tai nustatyta teisminio skundų nagrinėjimo taisyklėse, kurios yra identiškos Anglijoje ir Velse nustatytoms taisyklėms ([191]).

(114) Aukščiausiajame Teisme vienam iš jo teisėjų pavedama duomenų apsaugos priežiūros funkcija.

([184]) 2018 m. DAA 117 straipsnis.

([185]) Kolegija privalo teikti rekomendacijas teisėjams ir juos mokyti. Ji taip pat nagrinėja duomenų subjektų skundus, susijusius su bendrosios kompetencijos teismų, specializuotų teismų ir fizinių asmenų, vykdančių teisminės funkcijas, tvarkomais asmens duomenimis. Kolegija siekia suteikti priemones, kuriomis būtų galima išspręsti bet kurį skundą. Jeigu skundo pateikėjas nebuvo patenkintas kolegijos sprendimu ir pateikė papildomus įrodymus, kolegija gali nagrinėti jo skundą pakartotinai. Pati kolegija finansinių sankcijų neskiria, tačiau jeigu mano, kad buvo padarytas pakankamai šiurkštus 2018 m. DAA pažeidimas, ji gali perduoti bylą Teisėjų elgesio tyrimo biurui (angl. *Judicial Conduct Investigation Office* arba JCIO), kuris išnagrinės skundą. Jeigu skundas tenkinamas, sprendimą dėl veiksmų, kurių reikėtų imtis pareigūno atžvilgiu, priima lordas kancleris arba vyriausiasis teisėjas (arba vyresnysis teisėjas, kuris yra įgaliotas veikti jo vardu). Tai galėtų būti (pagal griežtumą): oficialus patarimas, oficialius įspėjimas ir papeikimas, ir galutinė priemonė – pašalinimas iš pareigų. Jeigu fizinis asmuo nepatenkintas tuo, kaip JCIO išnagrinėjo skundą, jis gali toliau skųstis Teisėjų skyrimo ir elgesio ombudsmenui (žr. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsmenas turi įgaliojimus prašyti JCIO iš naujo ištirti skundą ir gali pasiūlyti sumokėti skundo pateikėjui kompensaciją, jeigu mano, kad dėl netinkamo administravimo jis patyrė žalą.

([186]) Lordo vyriausiojo teisėjo ir vyriausiojo specializuotų teismų pirmininko pareiškimą dėl privatumo galima rasti šiuo adresu: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Šiaurės Airijos lordo vyriausiojo teisėjo paskelbtą pareiškimą dėl privatumo galima rasti šiuo adresu: https://judiciaryni.uk/data-privacy.

([188]) Škotijos bendrosios kompetencijos ir specializuotų teismų pareiškimą dėl privatumo galima rasti šiuo adresu: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Už duomenų priežiūrą atsakingas teisėjas teikia teisėjams rekomendacijas ir tiria pažeidimus ir (arba) skundus, susijusius su teismų arba fizinių asmenų, kurie veikia turėdami teisminius įgaliojimus, tvarkomais asmens duomenimis.

([190]) Jeigu manoma, kad skundas arba pažeidimas yra rimtas, jis pagal Šiaurės Airijos lordo vyriausiojo teisėjo paskelbtą skundų nagrinėjimo praktikos kodeksą perduodamas toliau tirti teisminių skundų pareigūnui. Išnagrinėjus tokį skundą: tolesnių veiksmų apskritai gali būti nesiimama, gali būti duodamas patarimas arba skiriamas mentorius, įteikiamas neoficialus įspėjimas, oficialus įspėjimas, galutinis įspėjimas, nustatomi praktikos apribojimai arba byla perduodama specializuotam statutinių pareigūnų teismui. Šiaurės Airijos lordo vyriausiojo teisėjo paskelbtą skundų nagrinėjimo praktikos kodeksą galima rasti šiuo adresu: 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]) Bet kurį pagrįstą skundą tiria duomenų priežiūros teisėjas ir jis perduodamas lordui pirmininkui, kuris turi įgaliojimus pateikti patarimą, oficialų įspėjimą arba papeikimą, jei, jo manymu, tai yra būtina (lygiavertės taisyklės taikomos specializuoto teismo nariams ir jas galima rasti šiuo adresu: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Teisių gynimas*

(115) Siekiant užtikrinti tinkamą apsaugą ir, visų pirma, individualių teisių įgyvendinimą, duomenų subjektui turėtų būti suteikta veiksmingų administracinių ir teisminių teisių gynimo priemonių, įskaitant kompensaciją už patirtą žalą.

(116) Pirma, duomenų subjektas turi teisę pateikti skundą informacijos komisarui, jeigu mano, kad tvarkant jo asmens duomenis buvo pažeistos 2018 m. DAA 3 dalies nuostatos ([192]). Kaip aprašyta 100–109 konstatuojamosiose dalyse, informacijos komisaras turi įgaliojimus įvertinti, ar duomenų valdytojas ir duomenų tvarkytojas laikosi 2018 m. DAA, jeigu nesilaiko – reikalauti, kad jie imtųsi arba nesiimtų tam tikrų veiksmų, ir skirti baudas.

(117) Antra, 2018 m. DAA nustatyta teisė imtis teisių gynimo priemonių prieš informacijos komisaro veiksmus. Jeigu komisaras, nagrinėdamas duomenų subjekto pateiktą skundą, nepadaro pažangos ([193]), skundo pateikėjas gali ginti savo teises teisme ir kreiptis į specializuotą pirmosios instancijos teismą ([194]) bei prašyti įpareigoti komisarą imtis reikiamų priemonių skundui išnagrinėti arba informuoti skundo pateikėją apie padarytą pažangą ([195]). Be to, bet kuris asmuo, kuris iš komisaro gauna bet kurį iš minėtų pranešimų (informacinį, vertinimo, vykdymo pranešimą arba pranešimą dėl nuobaudos), gali pateikti skundą specializuotam pirmosios instancijos teismui. Jeigu specializuotas teismas mano, kad komisaro sprendimas neatitinka įstatymo arba kad informacijos komisaras turėjo kitaip pasinaudoti savo diskrecija, specializuotas teismas privalo priimti skundą arba pakeisti kitą pranešimą ar sprendimą, kurį galėjo pateikti arba priimti informacijos komisaras ([196]).

(118) Trečia, asmenys gali pasinaudoti teisminėmis teisių gynimo priemonėmis prieš duomenų valdytojų ir duomenų tvarkytojų veiksmus tiesiogiai kreipdamiesi į teismus pagal 2018 m. DAA 167 straipsnį. Jeigu, atsižvelgdamas į duomenų subjekto prašymą, teismas įsitikina, kad duomenų apsaugos teisės aktuose nustatytos duomenų subjekto teisės buvo pažeistos, teismas gali įpareigoti duomenų valdytoją arba jo vardu veikiantį duomenų tvarkytoją imtis nutartyje nurodytų veiksmų dėl duomenų tvarkymo arba nesiimti nutartyje nurodytų veiksmų. Be to, pagal 2018 m. DAA 169 straipsnį bet kuris asmuo, kuris dėl duomenų apsaugos teisės akte (įskaitant 2018 m. DAA 3 dalį), išskyrus Jungtinės Karalystės BDAR, nustatyto reikalavimo pažeidimo patyrė žalos, turi teisę į tai, kad duomenų valdytojas arba duomenų tvarkytojas kompensuotų jam patirtą žalą, išskyrus atvejus, kai duomenų valdytojas arba duomenų tvarkytojas įrodo, kad jis jokiu atveju neatsako už įvykį, dėl kurio atsirado žala. Žalą sudaro finansiniai nuostoliai ir su jais nesusijusi žala, pvz., stresas.

(119) Ketvirta, bet kuris asmuo, kuris mano, kad valdžios institucijos pažeidė jo teises, įskaitant teises į privatumą ir duomenų apsaugą, savo teises gali ginti Jungtinės Karalystės teismuose pagal 1998 m. Žmogaus teisių aktą. Pagal 2018 m. DAA 3 dalį duomenų valdytojais, t. y. kompetentingomis institucijomis visada yra laikomos valdžios institucijos, kaip apibrėžta 1998 m. Žmogaus teisių akte. Asmuo, kuris teigia, kad valdžios institucija veikė (arba siūlo veikti) su Konvencijoje įtvirtintomis teisėmis nesuderinamu būdu, taip pažeidžiant 1998 m. Žmogaus teisių akto 6 straipsnio 1 dalį, gali atitinkamame bendrosios kompetencijos arba specializuotame teisme iškelti institucijai bylą arba remtis atitinkamomis teisėmis bet kuriame teisminiame procese, kai jis tapo (arba galėjo tapti) neteisėto veiksmo auka ([197]).

([192]) 2018 m. DAA 165 straipsnis.

([193]) 2018 m. DAA 166 straipsnyje konkrečiai nurodyti šie atvejai: a) komisaras dėl skundo nesiima tinkamų veiksmų; b) komisaras nepateikia skundo pateikėjui informacijos apie skundo nagrinėjimo eigą arba rezultatą iki trijų mėnesių laikotarpio, kuris pradedamas skaičiuoti nuo dienos, kurią komisaras gavo skundą, pabaigos arba c) komisaras per tą laikotarpį nebaigia nagrinėti skundo ir nepateikia skundo pateikėjui tokios informacijos dar per 3 mėnesius.

([194]) Specializuotas pirmosios instancijos teismas turi kompetenciją nagrinėti skundus dėl Vyriausybės reguliavimo įstaigų priimtų sprendimų. Jeigu sprendimą priėmė informacijos komisaras, kompetentinga kolegija yra Bendroji reguliavimo kolegija, kurios jurisdikcija galioja visoje Jungtinėje Karalystėje.

([195]) 2018 m. DAA 166 straipsnis.

([196]) 2018 m. DAA 161 ir 162 straipsniai.

([197]) Žr. 2016 m. sprendimą dėl Londono policijos *Brown / Commissioner*, kuriame teismas policijai iškeltoje byloje patenkino ieškovo prašymą dėl duomenų apsaugos. Teismas priėmė ieškovui palankų sprendimą ir patenkino jo ieškinius dėl 1998 m. DAA įtvirtintų pareigų pažeidimo, 1998 m. Žmogaus teisių akto pažeidimo (ir atitinkamos EŽTK 8 straipsnyje įtvirtintos teisės pažeidimo) ir su piktnaudžiavimu privačia informacija susijusio delikto (atsakovas galiausiai sutiko, kad pažeidė DAA ir EŽTK, todėl sprendime dėmesys daugiausia nagrinėta, kokią teisių gynimo priemonę tikslingiausia taikyti). Už padarytus pažeidimus teismas priteisė sumokėti ieškovui piniginę kompensaciją žalai atlyginti.

(120) Jeigu teismas nustato, kad kuris nors valdžios institucijos veiksmas yra neteisėtas, jis, atsižvelgdamas į savo įgaliojimus, gali nustatyti jo manymu teisingą ir tinkamą teisių gynimo priemonę arba priimti jo manymu teisingą ir tinkamą nutartį ([198]). Teismas taip pat gali pirminės teisės akto nuostatą paskelbti nesuderinama su teise, kuri yra garantuojama pagal EŽTK.

(121) Galiausiai, išnaudojęs nacionalines teisių gynimo priemones, fizinis asmuo dėl EŽTK garantuojamų žmogaus teisių pažeidimų savo teises gali ginti Europos Žmogaus Teisių Teisme.

2.6. **Tolesnis dalijimasis informacija**

(122) Pagal Jungtinės Karalystės teisę viena teisėsaugos institucija gali teikti duomenis kitoms JK institucijoms kitais tikslais nei tie, dėl kurių duomenys iš pradžių buvo surinkti (tiksliau – perduoti duomenis toliau), laikydamasi tam tikrų sąlygų.

(123) Panašiai kaip pagal Direktyvos (ES) 2016/680 4 straipsnio 2 dalį, pagal 2018 m. DAA 36 straipsnio 3 dalį kompetentingos institucijos teisėsaugos tikslu surinktus asmens duomenis leidžiama tvarkyti toliau (tą gali daryti pradinis arba kitas duomenų valdytojas) bet kuriuo kitu teisėsaugos tikslu, jeigu duomenų valdytojas pagal įstatymą turi įgaliojimus tvarkyti duomenis kitu tikslu ir duomenų tvarkymas yra būtinas ir proporcingas tam tikslui ([199]). Šiuo atveju gaunančiosios institucijos atliekamam duomenų tvarkymui taikomos visos 2018 m. DAA 3 dalyje numatytos pirmiau išanalizuotos apsaugos priemonės.

(124) Pagal Jungtinės Karalystės teisinę tvarką ir įvairius jos įstatymus toks tolesnis dalijimasis duomenimis yra leidžiamas. Visų pirma, i) pagal 2017 m. Skaitmeninės ekonomikos aktą valdžios institucijoms duomenimis leidžiama dalytis keliais tikslais, pvz., dėl bet kurio sukčiavimo viešajame sektoriuje atvejo, susijusio su valdžios institucijų nuostoliais arba nuostolių rizika ([200]), arba skolos valdžios institucijai arba Karalienei atveju ([201]); ii) pagal 2013 m. Nusikaltimų ir teismų aktą, kuriame leidžiama dalytis informacija su Nacionaline nusikaltimų agentūra ([202]) kovos su sunkiais ir organizuotais nusikaltimais, jų tyrimo ir baudžiamojo persekiojimo tikslais; iii) pagal 2007 m. Sunkių nusikaltimų aktą, kuriame valdžios institucijoms leidžiama atskleisti informaciją kovos su sukčiavimu organizacijoms, siekiant užkirsti kelią sukčiavimui ([203]).

(125) Šiuose teisės aktuose aiškiai nustatyta, kad dalijimasis informacija turi atitikti 2018 m. DAA nustatytas taisykles. Be to, tam, kad policijai būtų lengviau vykdyti duomenų apsaugos pareigas pagal Jungtinės Karalystės BDAR, DAA ir 1998 m. Žmogaus teisių aktą, Policijos koledžas paskelbė Dalijimosi informacija leistinos profesinės praktikos aprašą ([204]). Tai, ar dalijantis duomenimis yra laikomasi atitinkamų duomenų apsaugos teisės aktų, žinoma, gali būti peržiūrima teismine tvarka ([205]).

(126) Be to, panašiai kaip Direktyvos (ES) 2016/680 9 straipsnyje, 2018 m. DAA nustatyta, kad bet kuriuo teisėsaugos tikslu surinkti asmens duomenys gali būti tvarkomi ne teisėsaugos tikslu, kai tai leidžiama daryti pagal įstatymą ([206]). Šios rūšies duomenimis galima dalytis dviem atvejais: 1) kai baudžiamosios teisėsaugos institucija dalijasi duomenimis su nebaudžiamosios teisėsaugos institucija, išskyrus žvalgybos tarnybas (pvz., finansų arba mokesčių institucija, konkurencijos institucija, jaunimo gerovės tarnyba ir pan.), ir 2) kai baudžiamosios teisėsaugos institucija

([198]) 1998 m. Žmogaus teisių akto 8 straipsnio 1 dalis.

([199]) 2018 m. DAA 36 straipsnio 3 dalis.

([200]) 2017 m. Skaitmeninės ekonomikos akto 56 straipsnis, galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) 2017 m. Skaitmeninės ekonomikos akto 48 straipsnis.

([202]) 2013 m. Nusikaltimų ir teismų akto 7 straipsnis; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2013/22/contents.

([203]) 2007 m. Sunkių nusikaltimų akto 68 straipsnis; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([204]) Dalijimosi informacija leistina profesinė praktika; galima rasti šiuo adresu: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

([205]) Pavyzdžiui, žr. Sprendimą M / *the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), kuriame aukštojo teismo buvo prašoma išnagrinėti dalijimąsi duomenimis tarp policijos ir Verslo partnerystės kovos su nusikalstamumu srityje organizacijos (angl. *Business Crime Reduction Partnership* arba BCRP), t. y. organizacijos, įgaliotos administruoti pranešimų apie draudimus schemas, pagal kurias asmenims draudžiama patekti šios organizacijos narių komercines patalpas. Teismas įvertino dalijimąsi duomenimis, kuris buvo vykdomas pagal susitarimą, kurio tikslas – apsaugoti visuomenę ir užkirsti kelią nusikaltimams, ir galiausiai padarė išvadą, kad dauguma dalijimosi duomenimis aspektų buvo teisėti, išskyrus aspektus, susijusius su tam tikra neskelbtina informacija, kuria dalijosi policija ir BCRP. Kitas pavyzdys – Sprendimas *Cooper / NCA* [2019] EWCA Civ 16, kuriame apeliacinis teismas pritarė policijos ir Sunkių organizuotų nusikaltimų agentūros (angl. *Serious Organised Crime Agency* arba SOCA), t. y. dabar NCA priklausančios teisėsaugos agentūros, dalijimuisi duomenimis.

([206]) 2018 m. DAA 36 straipsnio 4 dalis.

dalijasi duomenimis su žvalgybos tarnybomis. Pirmuoju atveju asmens duomenų tvarkymui bus taikomas Jungtinės Karalystės BDAR ir 2018 m. DAA 2 dalis. Kaip nurodyta pagal Reglamentą (ES) 2016/679 priimtame sprendime, Jungtinės Karalystės BDAR ir 2018 m. DAA 2 dalyje nustatytomis apsaugos priemonėmis sukurtas apsaugos lygis yra iš esmės lygiavertis Sąjungoje užtikrinamam apsaugos lygiui ([207]).

(127) Antruoju atveju, kai baudžiamosios teisėsaugos institucijos surinktais duomenimis dalijamasi su žvalgybos tarnyba nacionalinio saugumo tikslais, teisinis pagrindas, kuriuo leidžiama dalytis tokiais duomenimis, yra 2008 m. Kovos su terorizmu aktas (2008 m. KTA) ([208]). Pagal 2008 m. KTA bet kuris asmuo gali teikti informaciją bet kuriai žvalgybos tarnybai bet kurioms šios tarnybos funkcijoms, įskaitant su nacionaliniu saugumu susijusias funkcijas, vykdyti.

(128) Dėl sąlygų, kuriomis duomenimis galima dalytis nacionalinio saugumo tikslais, pažymėtina, kad pagal Žvalgybos tarnybų aktą ir Saugumo tarnybų aktą žvalgybos tarnybos gali gauti tik jų funkcijoms pagal įstatymą vykdyti būtinus duomenis. Kompetentingos institucijos, kurios patenka į 2018 m. DAA 3 dalies taikymo sritį ir nori dalytis duomenimis su žvalgybos tarnybomis, turės įvertinti įvairius veiksnius ir (arba) apribojimus ir kartu atsižvelgti į Žvalgybos tarnybų akte ir Saugumo tarnybų akte nustatytas žvalgybos tarnybų funkcijas ([209]). 2008 m. KTA 20 straipsnyje aiškiai nurodyta, kad bet koks dalijimasis duomenimis pagal 2008 m. KTA 19 straipsnį vis tiek turi atitikti duomenų apsaugos teisės aktus; tai reiškia, kad taikomi visi 2018 m. DAA nustatyti apribojimai ir reikalavimai. Be to, teisėsaugos institucijos ir žvalgybos tarnybos pagal 1998 m. Žmogaus teisių aktą yra laikomos valdžios institucijomis, todėl privalo užtikrinti, kad jų veikloje būtų gerbiamos pagal EŽTK, įskaitant jos 8 straipsnį, garantuojamos teisės. Kitaip tariant, pagal šiuos reikalavimus teisėsaugos institucijos ir žvalgybos tarnybos visais duomenimis dalijasi laikydamosi duomenų apsaugos teisės aktų ir EŽTK.

(129) Žvalgybos tarnyboms nacionalinio saugumo tikslais tvarkant iš teisėsaugos institucijų gautus asmens duomenis yra taikomos įvairios sąlygos ir apsaugos priemonės ([210]). 2018 m. DAA 4 dalis taikoma visam žvalgybos tarnybų arba jų vardu atliekamam duomenų tvarkymui. Joje nustatyti pagrindiniai duomenų apsaugos principai (teisėtumas,

([207]) Komisijos įgyvendinimo sprendimas pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje, C(2021)4800.

([208]) 2008 m. Kovos su terorizmu akto 19 straipsnis; galima rasti šiuo adresu: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) 1994 m. Žvalgybos tarnybos akto (žr. https://www.legislation.gov.uk/ukpga/1994/13/contents) 2 straipsnio 2 dalyje nustatyta, kad „Vyriausioji žvalgybos tarnyba atsako už tos tarnybos veiksmingumą ir privalo užtikrinti: a) kad žvalgybos tarnyba negautų jokios kitos informacijos, išskyrus informaciją, kuri yra būtina jos funkcijoms tinkamai vykdyti, ir kad ji neatskleistų jokios informacijos, išskyrus tai, kas yra būtina i) siekiant to tikslo; ii) atsižvelgiant į nacionalinio saugumo interesus; iii) siekiant užkirsti kelią sunkiems nusikaltimams arba juos atskleisti, arba iv) nagrinėjant bet kokią baudžiamąją bylą, ir b) kad žvalgybos tarnyba nesiimtų jokių veiksmų, kuriais būtų palaikomi kurios nors Jungtinės Karalystės politinės partijos interesai“, o 1989 m. Saugumo tarnybų akto (žr. https://www.legislation.gov.uk/ukpga/1989/5/contents) 2 straipsnio 2 dalyje nustatyta, kad „generalinis direktorius atsako už tarnybos veiksmingumą ir privalo užtikrinti a) kad tarnyba negautų jokios informacijos, išskyrus informaciją, kuri yra būtina jos funkcijoms tinkamai vykdyti, ir kad ji neatskleistų jokios informacijos, išskyrus tai, kas yra būtina siekiant užkirsti kelią sunkiems nusikaltimams arba juos atskleisti [arba tai, kas būtina bet kurios baudžiamosios bylos nagrinėjimo tikslais] ir b) kad tarnyba nesiimtų jokių veiksmų, kuriais būtų palaikomi kurios nors politinės partijos interesai, ir c) tvarką, dėl kurios susitarta su Nacionalinės nusikaltimų agentūros generaliniu direktoriumi, kuria remiantis tarnybos veikla pagal šio akto 1 straipsnio 4 dalį būtų koordinuojama su policijos pajėgomis, Nacionaline nusikaltimų agentūra ir kitomis teisėsaugos tarnybomis“.

([210]) Apsaugos priemonės ir žvalgybos tarnybų įgaliojimų apribojimai yra reglamentuojami ir 2016 m. Tyrimo įgaliojimų aktu; šiuo aktu, Anglijos, Velso ir Šiaurės Airijos 2000 m. Tyrimo įgaliojimų reguliavimo aktu ir Škotijos 2000 m. Tyrimo įgaliojimų reguliavimo (Škotija) aktu sukurtas naudojimosi tokiais įgaliojimais teisinis pagrindas. Tačiau šie įgaliojimai tolesniam duomenų perdavimui nėra aktualūs, nes jie yra susiję su žvalgybos tarnybų teise tiesiogiai rinkti asmens duomenis. Dėl įgaliojimų, žvalgybos agentūroms suteiktų pagal Tyrimų įgaliojimų aktą, vertinimo žr. Komisijos įgyvendinimo sprendimą pagal Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje, C(2021) 4800.

sąžiningumas ir skaidrumas ([211]), tikslo apribojimas ([212]), duomenų kiekio mažinimas ([213]), tikslumas ([214]), saugojimo ribojimas ([215]) ir saugumas ([216]), nustatytos specialių kategorijų asmens duomenų tvarkymo sąlygos ([217]), numatytos duomenų subjektų teisės ([218]), reikalaujama užtikrinti pritaikytąją duomenų apsaugą ([219]) ir reglamentuojami tarptautiniai asmens duomenų perdavimai ([220]).

(130) Kartu 2018 m. DAA 110 straipsnyje nustatyta 2018 m. DAA 4 dalies nuostatų taikymo išimtis, kai tokia išimtis yra būtina siekiant užtikrinti nacionalinį saugumą. 2018 m. DAA 110 straipsnio 2 dalyje nurodyta, kurioms nuostatoms leidžiama taikyti išimtį. Prie jų priskirti duomenų apsaugos principai (išskyrus teisėtumo principą), duomenų subjekto teisės, pareiga informuoti informacijos komisarą apie duomenų saugumo pažeidimą, informacijos komisaro įgaliojimai atlikti patikrinimus pagal tarptautinius įpareigojimus, tam tikri informacijos komisaro vykdymo užtikrinimo įgaliojimai, nuostatos, kuriomis už tam tikrus duomenų apsaugos pažeidimus taikoma baudžiamoji atsakomybė, ir nuostatos, susijusios su specialiais duomenų tvarkymo tikslais, pvz., žurnalistikos, akademiniais arba meniniais tikslais. Šia išimtimi galima remtis kiekvienu atveju atlikus analizę ([221]). Kaip paaiškino Jungtinės Karalystės institucijos ir kaip patvirtinta Jungtinės Karalystės teismų praktikoje, „a) duomenų valdytojas privalo atsižvelgti į faktines pasekmes nacionaliniam saugumui arba gynybai, jeigu jis privalėtų laikytis konkrečios duomenų apsaugos nuostatos ir jeigu pagrįstai galėtų laikytis įprastos taisyklės nepadarydamas poveikio nacionaliniam saugumui arba gynybai)“ ([222]). Tai, ar išimtimi pasinaudota tinkamai, prižiūri informacijos komisaras ([223]).

([211]) Kaip nurodyta 2018 m. DAA 86 straipsnio 6 dalyje, siekiant nustatyti, ar duomenys tvarkomi sąžiningai ir skaidriai, būtina atsižvelgti į jų gavimo metodą. Šiuo atžvilgiu sąžiningumo ir skaidrumo reikalavimas laikomas įvykdytu, jeigu duomenys gaunami iš asmens, kuris pagal įstatymą yra įgaliotas arba privalo juos teikti.

([212]) Pagal 2018 m. DAA 87 straipsnį duomenų tvarkymo tikslai turi būti konkretūs, aiškūs ir teisėti. Duomenų negalima tvarkyti su tikslais, kuriais jie buvo surinkti, nesuderinamu būdu. Pagal 87 straipsnio 3 dalį tolesnis suderinamas asmens duomenų tvarkymas gali būti leidžiamas tik tada, jeigu duomenų valdytojui pagal įstatymą leidžiama tvarkyti duomenis tuo tikslu ir jeigu duomenų tvarkymas kitu tikslu yra būtinas ir proporcingas. Duomenų tvarkymas turėtų būti laikomas suderinamu, jeigu duomenys tvarkomi archyvavimo tikslais viešojo intereso labui, mokslinių arba istorinių tyrimų arba statistiniais tikslais ir jei tokiam tvarkymui taikomos tinkamos apsaugos priemonės (2018 m. DAA 87 straipsnio 4 dalis).

([213]) Asmens duomenys turėtų būti tinkami, aktualūs ir neperteklinai (2018 m. DAA 88 straipsnis).

([214]) Asmens duomenys turėtų būti tikslūs ir nauji (2018 m. DAA 89 straipsnis).

([215]) Asmens duomenys neturėtų būti saugomi ilgiau, nei to reikia (2018 m. DAA 90 straipsnis).

([216]) Pagal šeštąjį duomenų apsaugos principą duomenų tvarkymo metodai turi apimti tinkamas apsaugos nuo rizikos, kylančios dėl asmens duomenų tvarkymo, priemones. Rizika apima (tuo neapsiribojant) netyčinę arba neteisėtą prieigą prie asmens duomenų, jų sunaikinimą, praradimą, naudojimą, keitimą arba atskleidimą (2018 m. DAA 91 straipsnis). Pagal 107 straipsnį taip pat reikalaujama, kad 1) kiekvienas duomenų valdytojas įdiegtų tinkamas apsaugos priemones, proporcingas rizikai, kylančiai dėl asmens duomenų tvarkymo, ir 2) automatizuoto duomenų tvarkymo atveju kiekvienas duomenų valdytojas ir kiekvienas duomenų tvarkytojas įdiegtų rizikos vertinimu pagrįstas prevencines arba rizikos mažinimo priemones.

([217]) 2018 m. DAA 86 straipsnio 2 dalies b punktas ir 10 priedas.

([218]) 2018 m. DAA 4 dalies 3 skyrius, visų pirma teisė susipažinti su duomenimis, juos ištaisyti ir ištrinti, teisė nesutikti, kad duomenys būtų tvarkomi ir būtų naudojami sprendimams automatizuotu būdu priimti, teisė įsikišti į automatizuotą sprendimų priėmimą ir teisė būti informuotam apie sprendimų priėmimą. Be to, duomenų valdytojas privalo suteikti duomenų subjektui informacijos apie jo asmens duomenų tvarkymą.

([219]) 2018 m. DAA 103 straipsnis. Mirusio asmens duomenys nepatenka į 2018 m. DAA taikymo sritį.

([220]) 2018 m. DAA 109 straipsnis. Asmens duomenis perduoti tarptautinėms organizacijoms arba į valstybes už Jungtinės Karalystės ribų yra įmanoma, jeigu duomenų perdavimas yra būtinas ir proporcingas duomenų valdytojui vykdant teisės aktuose nustatytas funkcijas arba kitais tam tikruose 1989 m. Saugumo tarnybų akto ir 1994 m. Žvalgybos tarnybų akto straipsniuose nustatytais tikslais.

([221]) Žr. Sprendimą *Baker / Secretary of State for the Home Department* [2001] UKIT NSA2 (toliau – Sprendimas *Baker / Secretary of State*).

([222]) Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinio saugumo duomenų apsaugos ir tyrimo įgaliojimų sistema“, p. 15–16, galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Taip pat žr. Sprendimą *Baker / Secretary of State* (žr. 220 išnašą), kuriame teismas panaikino vidaus reikalų sekretoriaus išduotą nacionalinį saugumo sertifikatą ir pritarė nacionalinio saugumo išimties taikymui, motyvuodamas tuo, kad nebuvo jokios priežasties numatyti bendrą pareigos atsakyti į prašymus leisti susipažinti su duomenimis išimtį ir kad leidimas taikyti tokią išimtį visomis aplinkybėmis, neatlikus kiekvieno atvejo analizės, viršija tai, kas būtina ir proporcinga nacionaliniam saugumui užtikrinti.

([223]) Žr. informacijos komisaro ir Jungtinės Karalystės žvalgybos tarnybų susitarimo memorandumą, pagal kurį „informacijos komisaras, gavęs duomenų subjekto skundą, įsitikina, kad klausimas buvo išnagrinėtas teisingai ir, kai taikytina, kad bet kokia išimtis buvo taikoma tinkamai“ (Informacijos komisaro biuro ir Jungtinės Karalystės žvalgybos tarnybų susitarimo memorandumo 16 punktas; galima rasti šiuo adresu: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Be to, kadangi „nacionalinio saugumo“ užtikrinimo tikslais bet kurios iš pirmiau paminėtų teisių gali būti apribotos, 2018 m. DAA 79 straipsnyje numatyta, kad duomenų valdytojas gali prašyti išduoti Ministrų kabineto arba generalinio prokuroro pasirašytą sertifikatą, kuriuo patvirtinama, kad tų teisių apribojimas yra būtina ir proporcinga priemonė nacionaliniam saugumui užtikrinti ([224]). Jungtinės Karalystės Vyriausybė yra paskelbusi gaires dėl nacionalinio saugumo sertifikatų pagal 2018 m. DAA, kuriose pirmiausia pabrėžiama, kad bet kokie duomenų subjektų teisių apribojimai nacionalinio saugumo užtikrinimo tikslais turi būti proporcingi ir būtini ([225]). Visi nacionalinio saugumo sertifikatai turi būti skelbiami Informacijos komisaro interneto svetainėje ([226]).

(132) Sertifikato galiojimo trukmė turėtų būti konkreti ir neviršyti penkerių metų, kad įstatymų vykdomoji valdžia galėtų jį nuolat peržiūrėti ([227]). Sertifikate nurodomi asmens duomenys arba asmens duomenų kategorijos, kurioms taikoma išimtis, taip pat 2018 m. DAA nuostatos, kurioms taikoma išimtis ([228]).

(133) Svarbu pažymėti, kad nacionalinio saugumo sertifikatai nesuteikia papildomo pagrindo apriboti duomenų apsaugos teises nacionalinio saugumo sumetimais. Kitaip tariant, duomenų valdytojas arba duomenų tvarkytojas sertifikatu gali remtis tik tada, jei padaro išvadą, kad nacionalinio saugumo išimtį taikyti būtina ir kad ji konkrečiu atveju turi būti taikoma. NET jei nacionalinio saugumo sertifikatas sprendžiant konkretų klausimą yra taikomas, informacijos komisaras gali tirti, ar konkrečiu atveju remtis nacionalinio saugumo išimtimi buvo pagrįsta ([229]).

(134) Bet kuris asmuo, kurį sertifikato išdavimas paveikė tiesiogiai, gali pateikti skundą aukštesniajam specializuotam teismui ([230]) dėl to sertifikato ([231]) arba, jeigu sertifikate duomenys nurodomi pateikiant bendrą aprašymą, ginčyti sertifikato taikymą konkretiems duomenims ([232]).

(135) Specializuotas teismas peržiūrės sprendimą išduoti sertifikatą ir nuspręs, ar buvo pagrįstų priežasčių jį išduoti ([233]). Jis gali nagrinėti įvairius klausimus, įskaitant būtinumą, proporcingumą ir teisėtumą, atsižvelgdamas į poveikį duomenų subjektų teisėms ir poreikį užtikrinti nacionalinį saugumą. Todėl specializuotas teismas gali nuspręsti, kad tam tikriems asmens duomenims, dėl kurių pateiktas skundas, sertifikatas netaikomas ([234]).

([224]) 2018 m. DAA panaikinta galimybė sertifikatą išduoti pagal 1998 m. Duomenų apsaugos akto 28 straipsnio 2 dalį. Tačiau galimybė išduoti sertifikatus pagal „seną tvarką“ vis dar egzistuoja, nes taikant 1998 m. aktą iškilo istorinis iššūkis (žr. 2018 m. DAA 20 priedo 5 dalies 17 punktą). Vis dėlto tokia galimybė, panašu, taikoma itin retai, tik tam tikrais atvejais: pavyzdžiui, jei duomenų subjektas užginčija nacionalinio saugumo išimties taikymą, kai duomenis tvarko valdžios institucija, tą daranti pagal 1998 m. aktą. Pažymėtina, kad tokiais atvejais bus taikomas visas 1998 m. DAA 28 straipsnis, įskaitant galimybę duomenų subjektui užginčyti sertifikato galiojimą. Šiuo metu nacionalinio saugumo sertifikatai pagal 1998 m. DAA neišduodami.

([225]) Jungtinės Karalystės gairės dėl nacionalinio saugumo sertifikatų pagal 2018 m. duomenų apsaugos aktą; galima rasti šiuo adresu: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) Pagal 2018 m. DAA 130 skyrių informacijos komisaras gali nuspręsti neskelbti sertifikato teksto ar jo dalies, jei tai prieštarautų nacionalinio saugumo interesams, viešajam interesui arba galėtų kelti pavojų kurio nors asmens saugumui. Tačiau tokiais atvejais informacijos komisaras paskelbia, kad sertifikatas buvo išduotas.

([227]) Jungtinės Karalystės gairių dėl nacionalinio saugumo sertifikatų 15 dalis, žr. 225 išnašą.

([228]) Jungtinės Karalystės gairių dėl nacionalinio saugumo sertifikatų 5 dalis, žr. 225 išnašą.

([229]) 2018 m. DAA 102 straipsnyje nustatyta, kad duomenų valdytojas turi gebėti įrodyti, kad laikėsi 2018 m. DAA. Tai reiškia, kad žvalgybos tarnyba turėtų įrodyti informacijos komisarui, kad, remdamasi išimtimi, ji atsižvelgė į konkrečias bylos aplinkybes. Informacijos komisaras taip pat skelbia nacionalinio saugumo sertifikatų registrą; galima rasti šiuo adresu: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Aukštesnysis specializuotas teismas turi kompetenciją nagrinėti skundus dėl žemesnės instancijos administracinių specializuotų teismų priimtų sprendimų ir specialią kompetenciją nagrinėti tiesioginius skundus dėl tam tikrų Vyriausybės įstaigų sprendimų.

([231]) 2018 m. DAA 111 straipsnio 3 dalis.

([232]) 2018 m. DAA 111 straipsnio 5 dalis.

([233]) Sprendime *Baker / Secretary of State* (žr. 221 išnašą) specializuotas informacinis teismas panaikino vidaus reikalų sekretoriaus išduotą nacionalinį saugumo sertifikatą, motyvuodamas tuo, kad nebuvo jokios priežasties numatyti bendrą pareigos atsakyti į prašymus leisti susipažinti su duomenimis išimtį ir kad leidimas taikyti tokią išimtį visomis aplinkybėmis, neatlikus kiekvieno atvejo analizės, viršija tai, kas būtina ir proporcinga nacionaliniam saugumui užtikrinti.

([234]) Jungtinės Karalystės gairių dėl nacionalinio saugumo sertifikatų 25 dalis, žr. 225 išnašą.

(136) Kitą galimų apribojimų grupę sudaro apribojimai, pagal 2018 m. DAA 11 straipsnį taikomi tam tikroms 2018 m. DAA 4 dalies nuostatoms ([235]), siekiant apsaugoti kitus su bendru viešuoju interesu arba saugomais interesais susijusius svarbius tikslus, pvz., Parlamento neliečiamumą, advokato teisę neatskleisti profesinės paslapties, teismo proceso vykdymą arba ginkluotųjų pajėgų kovinį veiksmingumą. Šių nuostatų taikymo išimtis yra taikoma tam tikrų kategorijų informacijai (pagrįsta pagal kategoriją) arba ta apimtimi, kuria šių nuostatų taikymas galėtų pakenkti saugomam interesui (pagrįsta pagal žalą) ([236]). Pagal žalą pagrįstomis išimtimis galima remtis tik tada, jeigu būtų tikimybės, kad nurodytų duomenų apsaugos nuostatų taikymas gali pakenkti atitinkamam interesui. Todėl išimtis visada turi būti pagrindžiama nurodant atitinkamą žalą, kuri galėtų atsirasti konkrečiu atveju. Pagal informacijos kategoriją pagrįstomis išimtimis galima remtis tik mokslinės, siauriai apibrėžtos kategorijos informacijos, kuriai leidžiama taikyti išimtį, atžvilgiu. Pagal tikslą ir poveikį šios išimtys yra panašios į kai kurias Jungtinės Karalystės BDAR nustatytas išimtis (2018 m. DAA 2 priedas), o šios atitinka BDAR 23 straipsnyje numatytas išimtis.

(137) Iš to, kas nurodyta pirmiau, galima daryti išvadą (tokio paties aiškinimo taip pat laikėsi teismai ir Informacijos komisija), kad pagal taikytinas Jungtinės Karalystės teisės normas yra nustatyti apribojimai ir sąlygos, kuriais užtikrinama, kad šios išimtys ir apribojimai neviršytų to, kas yra būtina ir proporcinga nacionaliniam saugumui užtikrinti.

(138) Žvalgybos tarnybų vykdomą asmens duomenų tvarkymą pagal 2018 m. DAA 4 dalį prižiūri informacijos komisaras ([237]).

(139) Bendrosios informacijos komisaro funkcijos, susijusios su asmens duomenų tvarkymo žvalgybos tarnybose priežiūra pagal 2018 m. DAA 4 dalį, nustatytos 2018 m. DAA 13 priede. Prie jų priskiriama (tuo neapsiribojant) 2018 m. DAA 4 dalies vykdymo stebėsena ir vykdymo užtikrinimas, visuomenės informuotumo didinimas, Parlamento, Vyriausybės ir kitų institucijų konsultavimas teisėkūros ir administracinių priemonių klausimais, duomenų valdytojų ir duomenų tvarkytojų informuotumo apie jų pareigas didinimas, informacijos teikimas duomenų subjektui apie naudojimąsi duomenų subjekto teisėmis ir tyrimų vykdymas.

(140) Pagal 2018 m. DAA 3 dalį komisaras yra įgaliotas pranešti duomenų valdytojams apie įtariamą pažeidimą ir pateikti perspėjimą, kad duomenų tvarkymas gali pažeisti taisykles, o jei pažeidimas pasitvirtina – pareikšti papeikimus. Jeigu kurios nors akto nuostatos pažeidžiamos, jis taip pat gali teikti vykdymo pranešimus ir pranešimus dėl nuobaudų ([238]). Tačiau kitaip negu pagal kitas 2018 m. DAA dalis, komisaras negali pateikti nacionalinio saugumo įvertinimo ([239]).

(141) Taip pat pažymėtina, kad 2018 m. DAA 110 straipsnyje numatyta naudojimosi tam tikrais komisaro įgaliojimais išimtis, kai tai yra reikalinga nacionaliniam saugumui užtikrinti. Tai – komisaro įgaliojimas leisti (bet kurio tipo) pranešimus pagal DAA (informacinį, vertinimo, vykdymo pranešimus ir pranešimą dėl nuobaudų), įgaliojimas vykdyti patikrinimus pagal tarptautinius įsipareigojimus, įgaliojimas patekti į patalpas ir atlikti patikrinimą, taip pat

([235]) Tai apima: i) 4 dalyje nurodyti duomenų apsaugos principai, išskyrus duomenų tvarkymo teisėtumo reikalavimą pagal pirmąjį principą ir tai, kad duomenų tvarkymas turi atitikti vieną iš 9 ir 10 prieduose nustatytų sąlygų; ii) duomenų subjektų teisės ir iii) pareigos, susijusios su informacijos komisaro informavimu apie saugumo pažeidimus.

([236]) Kaip nurodyta Jungtinės Karalystės aiškinamajame dokumente, pagal informacijos kategorijas taikomos šios išimtys: i) informacijai apie Karališkųjų apdovanojimų ir titulų suteikimą; ii) advokato profesinės informacijos apsaugai; iii) informacijai apie konfidencialų darbą, mokymą ar švietimą ir iv) egzaminų darbams ir įvertinimams. Žala pagrįstos išimtys yra susijusios su: i) nusikaltimų prevencija arba išaiškinimu, nusikaltėlių sulaikymu ir baudžiamuoju persekiojimu; ii) parlamento narių neliečiamumu; iii) teismo procesais; iv) Karališkųjų ginkluotųjų pajėgų koviniu veiksmingumu; v) Jungtinės Karalystės ekonomine gerove; vi) derybomis su duomenų subjektu; vii) mokslinių, istorinių tyrimų arba statistiniais tikslais; viii) archyvavimu viešojo intereso labui. Diskusijoms dėl duomenų apsaugos tinkamumo skirto Jungtinės Karalystės aiškinamojo dokumento H skirsnis „Nacionalinis saugumas“, p. 13, žr. 222 išnašą.

([237]) 2018 m. DAA 116 straipsnis.

([238]) Pagal kartu skaitomus 2018 m. DAA 149 straipsnio 2 dalį ir jo 155 straipsnį, vykdymo pranešimai ir pranešimai dėl nuobaudų gali būti teikiami duomenų valdytojui arba duomenų tvarkytojui už 2018 m. DAA 4 dalies 2 skyriaus (duomenų tvarkymo principai), 2018 m. DAA 4 dalies nuostatų, pagal kurias duomenų subjektui suteikiamos jo teisės, 2018 m. DAA 108 straipsnyje nustatyto reikalavimo pranešti apie asmens duomenų saugumo pažeidimą komisarui ir 2018 m. DAA 109 straipsnyje nustatytų asmens duomenų perdavimo į trečiąsias valstybes, konvencijos nepasirašiusias valstybes ir tarptautines organizacijas principų pažeidimus. (Daugiau informacijos apie vykdymo pranešimus ir pranešimus dėl nuobaudų pateikta 102–103 konstatuojamosiose dalyse.)

([239]) Pagal 2018 m. DAA 147 straipsnio 6 dalį informacijos pareigūnas negali pateikti vertinimo pranešimo 2000 m. Informacijos laisvės akto 23 straipsnio 3 dalyje nurodytai įstaigai. Tai – Saugumo tarnyba (MI5), Slaptoji žvalgybos tarnyba (MI6) ir Vyriausybės komunikacijos biuras.

taisyklės dėl nusikaltimų ([240]). Kaip paaiškinta 136 konstatuojamojoje dalyje, šios išimtys bus taikomos tik tada, jei tai konkrečiu atveju bus reikalinga ir proporcinga. Šių išimčių taikymas tam tikrais atvejais gali būti peržiūrėtas teismine tvarka ([241]).

(142) Informacijos pareigūnas ir Jungtinės Karalystės žvalgybos tarnybos pasirašė susitarimo memorandumą ([242]), kuriame įtvirtinta bendradarbiavimo įvairiais klausimais, įskaitant pranešimus apie duomenų saugumo pažeidimus ir duomenų subjektų skundų tvarkymą, sistema. Visų pirma, jame numatyta, kad informacijos komisaras, gavęs skundą, įvertina, ar su nacionaliniu saugumu susijusios išimtys buvo panaudotos tinkamai. Remiantis atitinkamomis Jungtinės Karalystės Vyriausybės gairėmis dėl nacionalinio saugumo sertifikatų, teikiamų pagal Duomenų apsaugos aktą, atsakymai į informacijos komisaro užklausas, susijusias su individualių skundų nagrinėjimu, turi būti pateikti per 20 darbo dienų, o jei turi būti pateikta neskelbtina informacija – atsakymai turi būti teikiami naudojantis atitinkamais saugiais kanalais. Nuo 2018 m. balandžio mėn. iki šiol informacijos pareigūnas gavo 21 asmens skundą dėl žvalgybos tarnybų. Kiekvienas skundas buvo įvertintas, o duomenų subjektas buvo informuotas apie vertinimo rezultatą ([243]).

(143) Taip pat pažymėtina, kad Žvalgybos ir saugumo komitetas (toliau – ŽSK) vykdo parlamentinę priežiūrą, kaip žvalgybos tarnybos tvarko duomenis. Komiteto veiklos įstatyminis pagrindas nustatytas 2013 m. Teisingumo ir saugumo akte (2013 m. TSA) ([244]). Jame nurodyta, kad ŽSK yra Jungtinės Karalystės parlamento komitetas. ŽSK sudaro abiejų Parlamento rūmų nariai, kuriuos, pasikonsultavęs su opozicijos lyderiu, skiria Ministras Pirmininkas ([245]). ŽSK privalo kasmet pateikti Parlamentui ataskaitą apie savo funkcijų vykdymą ir teikti kitas, jo nuomone reikalingas, ataskaitas ([246]).

(144) Nuo 2013 m. ŽSK suteikta daugiau įgaliojimų, įskaitant įgaliojimą vykdyti saugumo tarnybų operatyvinės veiklos priežiūrą. Pagal 2013 m. TSA 2 straipsnį ŽSK pavesta prižiūrėti nacionalinio saugumo tarnybų išlaidas, administravimą, politiką ir operacijas. 2013 m. TSA nurodyta, kad ŽSK gali vykdyti operatyvinių klausimų tyrimus,

([240]) Nuostatos, kurioms gali būti taikomos išimtys: 108 straipsnis (komisaro informavimas apie asmens duomenų saugumo pažeidimą), 119 straipsnis (patikrinimas pagal tarptautinius įpareigojimus), 142–154 straipsniai ir 15 priedas (komisaro pranešimai ir įgaliojimai patekti į patalpas bei atlikti patikrinimą), 170–173 straipsniai (su asmens duomenimis susiję nusikaltimai). Taip pat, kalbant apie duomenų tvarkymą žvalgybos tarnybose, 13 priedo (kitos bendrosios Komisaro funkcijos) 1 punkto a ir g papunkčiai ir 2 punktas.

([241]) Žr., pvz., Sprendimą byloje *Baker v Secretary of State for the Home Department* (žr. 221 išnašą).

([242]) Informacijos komisaro ir Jungtinės Karalystės žvalgybos tarnybų susitarimo memorandumas, žr. 231 išnašą.

([243]) Septyniais iš tų atvejų informacijos komisaras rekomendavo skundo pateikėjui aiškintis su duomenų valdytoju (taip turi būti daroma, kai asmuo kreipiasi į informacijos komisarą, tačiau prieš tai turėjo kreiptis į duomenų valdytoją), vienu iš tų atvejų informacijos komisaras pateikė duomenų valdytojui bendrą rekomendaciją (tokia rekomendacija teikiama, kai paaiškėja, kad duomenų valdytojas teisės aktų nepažeidė, tačiau informacijos komisarui pateikto skundo būtų buvę galima išvengti, jeigu duomenų valdytojo praktika būtų patobulinta), o likusiais 13 atvejų duomenų valdytojas jokių veiksmų imtis neprivalėjo (tokia išvada daroma, kai asmens pateikti skundai patenka į 2018 m. Duomenų apsaugos akto taikymo sritį, nes jie teikiami dėl asmens informacijos tvarkymo, tačiau, remiantis duomenų valdytojo pateikta informacija, nustatoma, kad teisės aktai pažeisti nebuvo).

([244]) Kaip paaiškino Jungtinės Karalystės institucijos, pagal Teisingumo ir saugumo aktą ŽSK kompetencijos sritis buvo išplėsta – į ją įtraukta platesnė žvalgybos sektoriaus, ne vien trijų tarnybų, priežiūra, numatyta galimybė peržiūrėti šių tarnybų anksčiau vykdytą veiklą nacionaliniams interesams svarbiose srityse.

([245]) 2013 m. TSA 1 straipsnis. Ministrai nariais būti negali. ŽSK nariai savo pareigas eina Parlamento kadencijos, per kurią buvo paskirti, laikotarpiu. Jie gali būti pašalinti juos paskyrusių Parlamento rūmų rezoliucija, jeigu netenka parlamento nario statuso arba tampa ministrais. Narys taip pat gali atsistatydinti.

([246]) Komiteto ataskaitas ir pareiškimus galima rasti šiuo adresu: http://isc.independent.gov.uk/committee-reports. 2015 m. ŽSK parengė ataskaitą „Privatumas ir saugumas. Moderni ir skaidri teisinė bazė“ (žr. https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), kurioje išnagrinėjo teisės aktus, kuriais reglamentuojami žvalgybos agentūrų naudojami žvalgybos metodai, ir pateikė keletą rekomendacijų, kurios vėliau buvo apsvarstytos ir įtrauktos į Žvalgybos įgaliojimų bilį, vėliau tapusį įstatymu (2016 m. Tyrimo įgaliojimų aktas). Vyriausybės atsakymą dėl Privatumo ir saugumo ataskaitos galima rasti šiuo adresu: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

kai jie nėra susiję su vykdomomis operacijomis ([247]). Ministro pirmininko ir ŽSK susitarimo memorandume ([248]) išsamiai išdėstyta, į ką reikia atsižvelgti svarstant, ar veikla nėra kurios nors vykdomos operacijos dalis ([249]). Ministras pirmininkas gali prašyti, kad ŽSK ištirtų vykdomas operacijas; tarnybų pateiktą informaciją ŽSK taip pat gali peržiūrėti savanoriškai.

(145) Pagal 2013 m. TSA 1 priedą ŽSK gali prašyti bet kurios iš trijų žvalgybos tarnybų vadovų atskleisti bet kurią informaciją. Agentūra privalo suteikti tokią informaciją, nebent valstybės sekretorius tai vetuoja ([250]). Jungtinės Karalystės institucijos paaiškino, kad praktiškai informacijos, kuri ŽSK neteikiama, yra labai nedaug ([251]).

(146) Dėl teisių gynimo priemonių pirmiausia pažymėtina, kad pagal 2018 m. DAA 165 straipsnio 2 dalį duomenų subjektas gali pateikti informacijos komisarui skundą, jeigu mano, kad tvarkant jo asmens duomenis buvo pažeistos 2018 m. DAA 4 dalies nuostatos, be kita jo, piktnaudžiauta nacionalinio saugumo tikslais nukrypti leidžiančiomis nuostatomis ir apribojimais.

(147) Taip pat pažymėtina, kad pagal 2018 m. DAA 4 dalį asmenys turi teisę kreiptis į Aukštąjį teismą (Škotijoje – Sesijų teismą) su prašymu nurodyti duomenų valdytojui leisti pasinaudoti teise susipažinti su duomenimis ([252]), paprieštarauti duomenų tvarkymui ([253]) ir ištaisyti arba ištrinti duomenis.

(148) Asmenys taip pat turi teisę reikalauti iš duomenų valdytojo arba duomenų tvarkytojo atlyginti žalą, patirtą dėl to, kad nebuvo laikomasi 2018 m. DAA 4 dalies reikalavimo ([254]). Žalą sudaro finansiniai nuostoliai ir su jais nesusijusi žala, pvz., stresas ([255]).

(149) Galiausiai pažymėtina, kad dėl bet kokio Jungtinės Karalystės žvalgybos tarnybų elgesio ([256]) asmuo gali pateikti skundą Tyrimo įgaliojimų teismui. Anglijos, Velso ir Šiaurės Airijos Tyrimo įgaliojimų teismas yra įsteigtas pagal 2000 m. tyrimo įgaliojimų reguliavimo aktą, Škotijos Tyrimo įgaliojimų teismas yra įsteigtas pagal 2000 m. Tyrimo įgaliojimų reguliavimo (Škotija) aktą ir yra nepriklausomas nuo vykdomosios valdžios institucijų ([257]). Pagal 2000 m. Tyrimo įgaliojimų reguliavimo akto 65 straipsnį Tyrimo įgaliojimų teismo narius skiria Jos Didenybė penkerių metų kadencijai.

(150) Specializuoto teismo narį iš pareigų pašalinti gali Jos Didenybė, remdamasi abiejų Parlamento rūmų ([258]) kreipimusi ([259]).

(151) Kad galėtų pateikti ieškinį Tyrimo įgaliojimų teismui (nuolatinis reikalavimas) pagal 2000 m. Tyrimo įgaliojimų reguliavimo akto 65 straipsnį asmuo turi būti įsitikinęs, kad i) žvalgybos tarnybos veiksmai buvo susiję su juo pačiu, bet kuriuo jo turtu, bet kuriuo jo siųstu, jam siųstu arba skirtu pranešimu, jo naudojimusi bet kuria pašto paslauga, telekomunikacijų paslauga arba sistema ([260]) ir kad ii) tie veiksmai įvykdyti „ginčytinomis

([247]) 2013 m. TSA 2 straipsnis.
([248]) Ministro pirmininko ir ŽSK susitarimo memorandumas; galima rasti šiuo adresu: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Ministro pirmininko ir ŽSK susitarimo memorandumo 14 straipsnis, žr. 248 išnašą.
([250]) Valstybės sekretorius gali vetuoti informacijos atskleidimą dviem pagrindais: jeigu informacija yra neskelbtina ir jos ŽSK nereikėtų atskleisti dėl nacionalinio saugumo arba jeigu, valstybės sekretoriaus paprašius pateikti informaciją Bendruomenių rūmų atskirajam departamentų veiklos tikrinimo komitetui, dėl informacijos pobūdžio valstybės sekretorius padarytų išvadą (dėl įvairių priežasčių, ne vien dėl nacionalinio saugumo), kad jos tikslinga neatskleisti (2013 m. TSA 1 priedo 4 punkto 2 papunktis).
([251]) Jungtinės Karalystės aiškinamojo rašto H skyrius „Nacionalinis saugumas“, p. 43.
([252]) 2018 m. DAA 94 straipsnio 11 dalis.
([253]) 2018 m. DAA 99 straipsnio 4 dalis.
([254]) 2018 m. DAA 169 straipsnis, pagal kurį „asmuo, kuris patyrė žalą dėl duomenų apsaugos teisės aktų reikalavimų nesilaikymo“ gali teikti ieškinį.
([255]) 2018 m. DAA 169 straipsnio 5 dalis.
([256]) Žr. Tyrimo įgaliojimų reguliavimo akto 65 straipsnio 2 dalies b punktą.
([257]) Pagal 2000 m. Tyrimo įgaliojimų reguliavimo akto 3 priedą nariai privalo turėti nurodytos teisminio darbo patirties ir juos turi būti galima paskirti naujai kadencijai.
([258]) 2000 m. RIPA 3 priedo 1 dalies 5 punktas.
([259]) Dėl sąvokos „kreipimasis“ žr. 183 išnašą.
([260]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 65 straipsnio 4 dalis.

aplinkybėmis“ ([261]) ir juos įvykdė „žvalgybos tarnyba“ arba jie įvykdyti „žvalgybos tarnybos vardu“ ([262]). Kadangi sąvoka „įsitikinęs“ buvo išaiškinta gana plačiai ([263]), ieškiniui specializuotame teisme pareikšti taikoma nedaug nuolatinių reikalavimų.

(152) Jeigu specializuotas teismas nagrinėja jam pateiktą skundą, jis privalo ištirti, ar asmenys, prieš kuriuos skunde pateikti kokie nors kaltinimai, ėmėsi veiksmų prieš skundo pateikėją, taip pat ištirti, kokiais įgaliojimais remiantis pažeidimai esą buvo padaryti, taip pat ar nurodyti veiksmai iš tiesų padaryti ([264]). Jeigu specializuotas teismas nagrinėja bylą, priimdamas sprendimą toje byloje jis privalo taikyti tuos pačius principus, kuriuos taikytų atlikdamas teisminę peržiūrą ([265]).

(153) Specializuotas teismas privalo informuoti skundo pateikėją, ar sprendimas priimtas jo ar ne jo naudai ([266]). Pagal 2000 m. Tyrimo įgaliojimų reguliavimo akto 67 straipsnio 6 ir 7 dalis specializuotas teismas turi teisę priimti nutartis dėl laikinųjų priemonių ir priteisti atlyginti žalą arba priimti kitokį jo nuomone tinkamą sprendimą ([267]). Pagal 2000 m. Tyrimo įgaliojimų reguliavimo akto 67A straipsnį teismo sprendimą galima skųsti apeliacine tvarka, jei teismas arba atitinkamas apeliacinis teismas duoda tam leidimą.

(154) Visų pirma, asmuo gali pareikšti ieškinį (arba pasinaudoti kita teisių gynimo priemone) Tyrimo įgaliojimų teismui, jeigu mano, kad valdžios institucija veikė (arba siūlo veikti) su EŽTK įtvirtintomis teisėmis, įskaitant teisę į privatumą ir duomenų apsaugą, nesuderinamu būdu, todėl tas veiksmas pagal 1998 m. Žmogaus teisių akto 6 straipsnio 1 dalį yra neteisėtas. Tyrimo įgaliojimų teismui suteikta išimtinė jurisdikcija nagrinėti visus pagal Žmogaus teisių aktą pareikštus ieškinius dėl žvalgybos tarnybų. Taigi, kaip pažymėjo Aukštasis teismas, „faktą, ar Žmogaus teisių aktas buvo pažeistas, remiantis atitinkamos bylos medžiaga, iš esmės gali nagrinėti ir sprendimą dėl to priimti nepriklausomas specializuotas teismas, turintis prieigą prie visos atitinkamos medžiagos, įskaitant slaptą medžiagą. <...> Šiuo atžvilgiu turime galvoje ir tai, kad pats Tyrimo įgaliojimų teismas dabar pats gali teikti apeliacinį skundą atitinkamam apeliaciniam teismui (Anglijoje ir Velse – Apeliaciniam teismui). Aukščiausiasis teismas neseniai priimtame sprendime konstatavo, kad Tyrimo įgaliojimų teismui iš esmės gali būti taikoma teisminė peržiūra: žr. Sprendimą *R (Privacy International) / Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219“ ([268]). Jeigu Tyrimo įgaliojimų teismas nustato, kad kuris nors valdžios institucijos aktas yra neteisėtas, jis, atsižvelgdamas į savo įgaliojimus, gali nustatyti jo manymu teisingą ir tinkamą teisių gynimo priemonę arba priimti jo manymu teisingą ir tinkamą nutartį ([269]).

([261]) Tokios aplinkybės – tai valdžios institucijų veiksmai pagal įgaliojimus (pvz., pagal orderį, leidimą ir (arba) pranešimą dėl pranešimų perėmimo ir pan.) arba aplinkybės (nepriklausomai nuo to, ar įgaliojimas yra, ar jo nėra), kuriomis taip elgtis nebūtų buvę tinkama neturint įgaliojimo arba bent neapsvarsčius, ar tokio įgaliojimo nereikėtų gauti. Jeigu tam tikrus veiksmus leido Teismų komisaras, yra laikoma, kad veiksmai vykdyti ginčytinomis aplinkybėmis (2000 m. Tyrimo įgaliojimų reguliavimo akto 65 (7ZA) straipsnis), o kiti veiksmai, kurie įvykdomi be teisėjo pareigas vykdančio asmens leidimo, nėra laikomi vykdytais ginčytinomis aplinkybėmis (2000 m. Tyrimo įgaliojimų reguliavimo akto 65 straipsnio 7 ir 8 dalys).

([262]) Kaip paaiškino Jungtinės Karalystės institucijos, kadangi skundo pateikimo riba yra žema, specializuotas teismas neretai nustato, kad valdžios institucijos skundo nė nenagrinėjo. Naujausioje Tyrimo įgaliojimų teismo statistikos ataskaitoje nurodyta, kad 2016 m. Teismas gavo 209 skundus, iš kurių 52 % buvo pripažinti nerimtais arba nepagrįstais, dėl 25 % padaryta išvada, kad „sprendimas negalimas“. Jungtinės Karalystės institucijos paaiškino, jog tai reiškia, kad skundo pateikėjo atžvilgiu jokia slapta veikla nebuvo vykdoma arba jokiais įgaliojimais nebuvo naudojamasi arba kad slaptos veiklos metodai buvo naudojami, tačiau ta veikla buvo teisėta. Dar 11 % atvejų konstatuota, kad skundas nepriklauso teismo jurisdikcijai, skundas buvo atsiimtas arba negaliojantis, 5 % atvejų skundas atmestas dėl senaties, o 7 % atvejų priimtas sprendimas skundo pateikėjo naudai. Tyrimo įgaliojimų teismo 2016 m. statistikos ataskaita; galima rasti šiuo adresu: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([263]) Žr. Sprendimą *Human Rights Watch / Secretary of State* [2016] UKIPTrib15_165-CH. Šioje byloje Tyrimo įgaliojimų teismas, remdamasis su EŽTK susijusia teismų praktika, konstatavo, kad tinkamas kriterijus, kalbant apie įsitikinimą, kad koks nors žvalgybos tarnybos arba jos vardu vykdytas elgesys, patenkantis į 2000 m. Tyrimo įgaliojimų reguliavimo akto 68 straipsnio 5 dalies taikymo sritį, pasireiškė, yra tai, ar tokiam įsitikinimui yra pagrindo, įskaitant tai, kad asmuo gali tvirtinti, jog yra smurto auka vien dėl to, kad slaptos priemonės egzistuoja arba kad teisės aktuose yra leidžiama taikyti slaptas priemones, tik tada, jeigu gali įrodyti, kad dėl jo asmeninės padėties jis patiria riziką, kad tokios priemonės jam gali būti taikomos (žr. Sprendimo *Human Rights Watch / Secretary of State* 41 punktą).

([264]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 67 straipsnio 3 dalis.

([265]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 67 straipsnio 2 dalis.

([266]) 2000 m. Tyrimo įgaliojimų reguliavimo akto 68 straipsnio 4 dalis.

([267]) Pavyzdžiui, gali būti nurodyta sunaikinti visus valdžios institucijos apie bet kurį asmenį turimos informacijos įrašus.

([268]) Aukštojo teisingumo teismo sprendimo *Liberty*, [2019] EWHC 2057 (Admin), 170 punktas.

([269]) 1998 m. Žmogaus teisių akto 8 straipsnio 1 dalis.

(155) Išnaudojęs nacionalines teisių gynimo priemones, fizinis asmuo dėl EŽTK garantuojamų žmogaus teisių pažeidimų, susijusių su jo teisėmis, įskaitant teisę į privatumą ir duomenų apsaugą, gali kreiptis į Europos Žmogaus Teisių Teismą.

(156) Iš to, kas išdėstyta pirmiau, galima daryti išvadą, kad Jungtinės Karalystės baudžiamosios teisėsaugos institucijoms dalijantis duomenimis, dėl kurių priimamas šis sprendimas, su kitomis valdžios institucijomis, įskaitant žvalgybos tarnybas, yra taikomi apribojimai ir sąlygos, kuriomis užtikrinama, kad duomenimis toliau būtų dalijamasi, jei tai reikalinga ir proporcinga, ir taikomos tam tikros 2018 m. DAA nustatytos duomenų apsaugos priemonės. Be to, tai, kaip duomenys tvarkomi atitinkamose valdžios institucijose, prižiūri nepriklausomos tarnybos, o nukentėję asmenys gali pasinaudoti veiksmingomis teisminėmis teisių gynimo priemonėmis.

3. **IŠVADA**

(157) Komisija mano, kad pagal 2018 m. DAA 3 dalį užtikrinama asmens duomenų, kuriuos Sąjungos kompetentingos institucijos perduoda Jungtinės Karalystės kompetentingoms institucijoms baudžiamosios teisėsaugos tikslais, apsauga yra iš esmės lygiavertė pagal Direktyvą (ES) 2016/680 užtikrinamai apsaugai.

(158) Komisija taip pat mano, kad pagal Jungtinės Karalystės teisę numatyti priežiūros mechanizmai ir teisių gynimo galimybės, vertinant juos kaip visumą, sudaro galimybę praktiškai nustatyti padarytus pažeidimus ir už juos bausti, ir suteikia duomenų subjektui teisių gynimo priemonių, kad jis galėtų susipažinti su savo asmens duomenimis ir vėliau pasiekti, kad šie duomenys būtų ištaisyti arba ištrinti.

(159) Galiausiai pažymėtina, kad, remdamasi turima informacija apie Jungtinės Karalystės teisinę sistemą, Komisija mano, kad bet kokios intervencinės priemonės, kurių imasi Jungtinės Karalystės valdžios institucijos viešojo intereso tikslais asmenų, kurių asmens duomenys perduodami iš Europos Sąjungos Jungtinei Karalystei, teisių atžvilgiu, įskaitant atvejus, kai teisėsaugos institucijos dalijasi asmens duomenimis su kitomis valdžios institucijomis, pavyzdžiui, nacionalinėmis saugumo tarnybomis, apsiribos tuo, kas yra būtinai reikalinga, kad būtų pasiektas atitinkamas teisėtas tikslas, ir kad yra veiksmingų teisinės apsaugos priemonių, kurių galima imtis prieš tokias intervencines priemones.

(160) Todėl reikėtų priimti sprendimą, kad pagal Direktyvos (ES) 2016/680 36 straipsnio 2 dalį, aiškinamą atsižvelgiant į Pagrindinių teisių chartiją, yra laikytina, kad Jungtinė Karalystė užtikrina tinkamą duomenų apsaugos lygį.

(161) Ši išvada grindžiama tiek Jungtinės Karalystės vidaus tvarka, tiek jos tarptautiniais įsipareigojimais, ypač tuo, kaip ji laikosi Europos žmogaus teisių konvencijos ir paklūsta Europos žmogaus teisių teismo jurisdikcijai. Todėl tolesnis šių tarptautinių įsipareigojimų laikymasis yra ypač svarbus vertinimo, kuriuo remiantis priimamas šis sprendimas, aspektas.

4. **ŠIO SPRENDIMO PADARINIAI IR DUOMENŲ APSAUGOS INSTITUCIJŲ VEIKSMAI**

(162) Valstybės narės ir jų institucijos privalo imtis priemonių, kurios yra būtinos siekiant užtikrinti atitiktį Sąjungos institucijų aktams, nes preziumuojama, kad Sąjungos institucijų teisės aktai yra teisėti, todėl sukelia teisinių pasekmių, kol jų galiojimo laikotarpis nesibaigia, jie nėra pripažinti netekusiais galios, panaikinti patenkinus ieškinį dėl panaikinimo, paskelbti negaliojančiais išnagrinėjus prašymą priimti prejudicinį sprendimą arba neteisėtumu grindžiamą prieštaravimą.

(163) Todėl Komisijos sprendimas dėl duomenų apsaugos tinkamumo, kurį ji priėmė pagal Direktyvos (ES) 2016/680 36 straipsnio 3 dalį, yra privalomas visoms valstybių narių, kurioms jis skirtas, institucijoms, įskaitant šių valstybių narių nepriklausomas priežiūros institucijas. Visų pirma taikant šį sprendimą, perdavimai iš Sąjungos duomenų valdytojo arba duomenų tvarkytojo Jungtinėje Karalystėje esantiems duomenų valdytojams arba duomenų tvarkytojams gali vykti be jokio papildomo leidimo.

(164) Tuo pačiu reikėtų priminti, kad pagal Direktyvos (ES) 2016/680 47 straipsnio 5 dalį ir kaip paaiškinta Teisingumo Teismo sprendime *Schrems*, tais atvejais, kai nacionalinė duomenų apsaugos institucija suabejoja, ar Komisijos sprendimas dėl duomenų apsaugos tinkamumo yra suderinamas su asmens pagrindinėmis teisėmis į privatumą ir duomenų apsaugą, įskaitant atvejus, kai abejonėms pagrindo suteikia skundas, ji turi galėti pasinaudoti nacionalinėje teisėje numatytomis teisinėmis teisių gynimo priemonėmis ir galimybe pareikšti prieštaravimus nacionaliniam teismui, o teismui tokiu atveju gali prireikti kreiptis į Teisingumo Teismą su prašymu priimti prejudicinį sprendimą ([270]).

([270]) Sprendimo *Schrems* 65 punktas.

5. **SPRENDIMO STEBĖSENA, SUSTABDYMAS, PANAIKINIMAS ARBA KEITIMAS**

(165) Pagal Direktyvos (ES) 2016/680 36 straipsnio 4 dalį Komisija privalo nuolat stebėti atitinkamus pokyčius Jungtinėje Karalystėje po to, kai bus priimtas šis sprendimas, siekdama įvertinti, ar ji vis dar užtikrina iš esmės lygiavertį apsaugos lygį. Tokia stebėsena yra ypač svarbi šiuo atveju, nes Jungtinė Karalystė administruos, taikys ir užtikrins naują duomenų apsaugos režimą, kuriam nebetaikoma Sąjungos teisė ir kuris gali būti keičiamas. Šiuo atžvilgiu ypač bus stebima, kaip Jungtinė Karalystė praktiškai laikysis taisyklių dėl asmens duomenų perdavimo trečiosioms šalims, be kita ko, sudarydama tarptautinius susitarimus, ir į tai, kokį poveikį tai gali turėti pagal šį sprendimą perduodamų duomenų apsaugos lygiui; ir kaip bus užtikrinama veiksminga galimybė naudotis asmens teisėmis srityse, kurioms taikomas šis sprendimas. Be kita ko, Komisija stebės teismų praktikos raidą ir informacijos komisaro bei kitų nepriklausomų įstaigų vykdomą priežiūrą.

(166) Siekiant palengvinti šią stebėseną Jungtinės Karalystės institucijos turėtų nedelsdamos ir reguliariai informuoti Komisiją apie bet kokius materialinius Jungtinės Karalystės teisinės tvarkos pokyčius, kurie daro poveikį pagal šį sprendimą reglamentuojamai teisinei sistemai, taip pat apie bet kokius praktikos, susijusios su šiame sprendime vertinamų asmens duomenų tvarkymu, pokyčius, ypač tokiue, kurie susiję su 165 konstatuojamojoje dalyje nurodytais elementais.

(167) Taip pat pažymėtina, jog tam, kad Komisija galėtų veiksmingai vykdyti stebėsenos funkciją, valstybės narės turėtų Komisijai pranešti apie visus atitinkamus veiksmus, kurių ėmėsi nacionalinės duomenų apsaugos institucijos, visų pirma dėl ES duomenų subjektų užklausų ar skundų, susijusių su asmens duomenų perdavimu iš Sąjungos verslo subjektams Jungtinėje Karalystėje. Komisijai taip pat reikėtų pranešti apie visus požymius, kad Jungtinės Karalystės valdžios institucijų, atsakingų už nusikalstamų veikų prevenciją, tyrimą, atskleidimą ar baudžiamąjį persekiojimą už jas, įskaitant bet kokias priežiūros įstaigas, veiksmais nėra užtikrinama reikiamo lygio apsauga.

(168) Jeigu iš turimos informacijos, ypač iš informacijos, surinktos vykdant stebėseną pagal šį sprendimą, arba iš informacijos, kurią pateikia Jungtinės Karalystės arba valstybių narių institucijos, paaiškėja, kad Jungtinėje Karalystėje užtikrinamas duomenų apsaugos lygis nebėra pakankamas, Komisija turėtų apie tai informuoti kompetentingas Jungtinės Karalystės institucijas ir paprašyti per nustatytą terminą (jis negali būti ilgesnis nei trys mėnesiai) imtis tinkamų priemonių. Prireikus, atsižvelgiant į svarstomo klausimo pobūdį ir (arba) priemones, kurių reikia imtis, šis terminas gali būti pratęstas nustatytam laikui.

(169) Jeigu, iki nustatyto termino pabaigos kompetentingos Jungtinės Karalystės institucijos tų priemonių nesiima arba kitais būdais tinkamai neįrodo, kad duomenų apsaugos lygis, dėl kurio priimamas šis sprendimas, tebėra tinkamas, Komisija pradeda Direktyvos (ES) 2016/680 58 straipsnio 2 dalyje nurodytą procedūrą ir iš dalies arba visiškai sustabdo arba panaikina šį sprendimą.

(170) Kitu atveju Komisija pradeda procedūrą, kad šis sprendimas būtų iš dalies pakeistas, visų pirma nustato, kad duomenų perdavimui turi būti taikomos papildomos sąlygos, arba apriboja išvadą dėl duomenų apsaugos tinkamumo taip, kad ji galiotų tik tam duomenų perdavimui, kurį vykdant užtikrinamas duomenų apsaugos tęstinumas.

(171) Remdamasi deramai pagrįstu poreikiu imtis skubių veiksmų, Komisija pagal Direktyvos (ES) 2016/680 58 straipsnio 3 dalį pasinaudos galimybe priimti įgyvendinimo aktus, kurie pradedami taikyti iš karto, dėl šio sprendimo sustabdymo, panaikinimo arba pakeitimo.

6. **ŠIO SPRENDIMO GALIOJIMO TRUKMĖ IR ATNAUJINIMAS**

(172) Reikėtų atsižvelgti į tai, kad, pasibaigus susitarime dėl išstojimo nustatytam pereinamajam laikotarpiui ir nustojus taikyti laikinąją nuostatą, išdėstytą ES ir Jungtinės Karalystės prekybos ir bendradarbiavimo susitarimo 782 straipsnyje, Jungtinė Karalystė administruos, taikys ir vykdys naujus duomenų apsaugos reikalavimus, palyginti su tais, kurie buvo taikomi, kai ji privalėjo laikytis Europos Sąjungos teisės. Dėl to pagal šį sprendimą vertinta duomenų apsaugos teisinė sistema gali būti iš dalies pakeista, taip pat gali atsirasti kitų svarbių pokyčių.

(173) Todėl šiame sprendime tikslinga numatyti, kad sprendimas bus taikomas ketverius metus nuo įsigaliojimo.

(174) Visų pirma, jeigu iš informacijos, kuri bus surinkta vykdant stebėseną pagal šį sprendimą, paaiškės, kad nustatyti faktai dėl Jungtinėje Karalystėje užtikrinamo duomenų apsaugos lygio tinkamumo faktiniu ir teisiniu požiūriais tebegalioja, Komisija turėtų ne vėliau kaip likus šešiems mėnesiams iki šio sprendimo galiojimo pabaigos pradėti šio sprendimo keitimo procedūrą ir, visų pirma, laikino taikymo laikotarpį pratęsti dar ketveriems metams. Bet koks įgyvendinimo aktas, kuriuo iš dalies keičiamas šis sprendimas, turi būti priimtas laikantis Direktyvos (ES) 2016/680 58 straipsnio 2 dalyje nurodytos procedūros.

7. **BAIGIAMOSIOS PASTABOS**

(175) Europos duomenų apsaugos valdyba paskelbė savo nuomonę ([271]), į kurią buvo atsižvelgta rengiant šį sprendimą.

(176) Šiame sprendime numatytos priemonės atitinka pagal Direktyvos (ES) 2016/680 58 straipsnį įsteigto komiteto nuomonę.

(177) Pagal prie ES sutarties ir SESV pridėto Protokolo Nr. 21 dėl Jungtinės Karalystės ir Airijos pozicijos dėl laisvės, saugumo ir teisingumo erdvės 6a straipsnį Airijai nėra privalomos Direktyvoje (ES) 2016/680, taigi ir šiame įgyvendinimo sprendime, nustatytos taisyklės, kurios yra susijusios su valstybių narių vykdomu asmens duomenų tvarkymu atliekant veiklą, kuriai taikomas SESV trečiosios dalies V antraštinės dalies 4 arba 5 skyrius, tais atvejais, kai Airijai nėra privalomos taisyklės, kuriomis reglamentuojamos teisminio bendradarbiavimo baudžiamosiose bylose ar policijos bendradarbiavimo, kurį vykdant turi būti laikomasi pagal SESV 16 straipsnį nustatytų nuostatų, formos. Be to, pagal Tarybos įgyvendinimo sprendimą (ES) 2020/1745 ([272]), Airijoje Direktyva (ES) 2016/680 turi būti įgyvendinama ir laikinai taikoma nuo 2021 m. sausio 1 d. Todėl Airija privalo laikytis šio įgyvendinimo sprendimo tokiomis pat Įgyvendinimo sprendime (ES) 2020/1745 nustatytomis sąlygomis, kokios taikomos Airijoje taikant Direktyvą (ES) 2016/680 dėl Šengeno *acquis*, kurio Airija laikosi.

(178) Pagal Protokolo Nr. 22 dėl Danijos pozicijos, pridėto prie Europos Sąjungos sutarties ir Sutarties dėl Europos Sąjungos veikimo, 2 ir 2a straipsnius, Danija neprivalo laikytis Direktyvos (ES) 2016/680, taigi ir šio įgyvendinimo sprendimo, teisės normų dėl asmens duomenų tvarkymo valstybėse narėse ir neprivalo jų taikyti vykdydama į SESV trečios dalies V antraštinės dalies 4 ir 5 skyrių taikymo sritį patenkančią veiklą. Tačiau, kadangi Direktyva (ES) 2016/680 yra pagrįsta Šengeno *acquis*, pagal minėto protokolo 4 straipsnį Danija 2016 m. spalio 26 d. pranešė nusprendusi įgyvendinti Direktyvą (ES) 2016/680. Todėl Danija pagal tarptautinę teisę privalo įgyvendinti šį įgyvendinimo sprendimą.

(179) Dėl Islandijos ir Norvegijos pažymėtina, kad šiuo įgyvendinimo sprendimu plėtojamos Šengeno *acquis* nuostatos, kaip numatyta Europos Sąjungos Tarybos ir Islandijos Respublikos bei Norvegijos Karalystės sudarytame susitarime dėl šių dviejų valstybių asociacijos įgyvendinant, taikant ir plėtojant Šengeno *acquis* ([273]).

(180) Dėl Šveicarijos pažymėtina, kad šiuo įgyvendinimo sprendimu plėtojamos Šengeno *acquis* nuostatos, kaip numatyta Europos Sąjungos, Europos bendrijos ir Šveicarijos Konfederacijos susitarime dėl Šveicarijos Konfederacijos asociacijos įgyvendinant, taikant ir plėtojant Šengeno *acquis* ([274]).

(181) Dėl Lichtenšteino pažymėtina, kad šiuo įgyvendinimo sprendimu plėtojamos Šengeno *acquis* nuostatos, kaip apibrėžta Europos Sąjungos, Europos bendrijos, Šveicarijos Konfederacijos ir Lichtenšteino Kunigaikštystės protokole dėl Lichtenšteino Kunigaikštystės prisijungimo prie Europos Sąjungos, Europos bendrijos ir Šveicarijos Konfederacijos susitarimo dėl Šveicarijos Konfederacijos asociacijos įgyvendinant, taikant ir plėtojant Šengeno *acquis* ([275]),

---

([271]) Nuomonė 15/2021 dėl Europos Komisijos įgyvendinimo sprendimo pagal Direktyvą (ES) 2016/680 dėl tinkamos asmens duomenų apsaugos Jungtinėje Karalystėje projekto, kurią galima rasti adresu https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) 2020 m. lapkričio 18 d. Tarybos įgyvendinimo sprendimas (ES) 2020/1745 dėl Šengeno *acquis* nuostatų duomenų apsaugos srityje taikymo ir dėl tam tikrų Šengeno *acquis* nuostatų laikino taikymo Airijoje (OL L 393, 2020 11 23, p. 3).

([273]) OL L 176, 1999 7 10, p. 36.

([274]) OL L 53, 2008 2 27, p. 52.

([275]) OL L 160, 2011 6 18, p. 21.

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Pagal Direktyvos (ES) 2016/680 36 straipsnį yra laikytina, kad Jungtinė Karalystė užtikrina tinkamą asmens duomenų, kuriuos Europos Sąjunga perduoda Jungtinės Karalystės valdžios institucijoms, atsakingoms už baudžiamųjų nusikaltimų prevenciją, tyrimą, atskleidimą, baudžiamąjį persekiojimą už juos arba bausmių vykdymą, apsaugos lygį.

2 straipsnis

Jei valstybių narių kompetentingos priežiūros institucijos, siekdamos apsaugoti asmenis tvarkant jų asmens duomenis, įgyvendina savo įgaliojimus pagal Direktyvos (ES) 2016/680 47 straipsnį dėl duomenų perdavimo Jungtinės Karalystės valdžios institucijoms, kuris patenka į 1 straipsnyje nustatytą taikymo sritį, atitinkama valstybė turi nedelsdama apie tai informuoti Komisiją.

3 straipsnis

1. Komisija nuolat stebi teisinės sistemos, kuria grindžiamas šis sprendimas, taikymą, įskaitant sąlygas, kuriomis vykdomas tolesnis duomenų perdavimas ir įgyvendinamos asmens teisės, siekdama įvertinti, ar Jungtinė Karalystė ir toliau užtikrina tinkamą 1 straipsnyje nurodytą apsaugos lygį.

2. Valstybės narės ir Komisija informuoja vienos kitas apie atvejus, kai informacijos komisaras arba bet kuri kita kompetentinga Jungtinės Karalystės institucija neužtikrina teisės aktų, kuriais remiantis priimamas šis sprendimas, laikymosi.

3. Valstybės narės ir Komisija informuoja vienos kitas apie visus požymius, kad Jungtinės Karalystės valdžios institucijų kišimasis į asmenų teisę į jų asmens duomenų apsaugą viršija tai, kas yra būtinai reikalinga, arba apie tai, kad nuo tokio kišimosi nėra jokios veiksmingos teisinės apsaugos.

4. Jeigu Komisija sužino, kad tinkamas apsaugos lygis nebėra užtikrinamas, ji informuoja kompetentingas Jungtinės Karalystės institucijas ir gali sustabdyti šio sprendimo galiojimą, jį panaikinti arba iš dalies pakeisti.

5. Komisija taip pat gali sustabdyti šio sprendimo galiojimą, jį panaikinti arba iš dalies pakeisti, jei dėl nepakankamo Jungtinės Karalystės Vyriausybės bendradarbiavimo Komisija negali nustatyti, ar 1 straipsnio nurodyta išvada nesikeičia.

4 straipsnis

Šis sprendimas baigia galioti 2025 m. birželio 27 d., nebent jo galiojimas būtų pratęstas pagal Direktyvos (ES) 2016/680 58 straipsnio 2 dalyje nurodytą procedūrą.

5 straipsnis

Šis sprendimas skirtas valstybėms narėms.

Priimta Briuselyje 2021 m. birželio 28 d.

Komisijos vardu
Didier REYNDERS
Komisijos narys