KOMISSION TÄYTÄNTÖÖNPANOPÄÄTÖS (EU) 2021/1773,

annettu 28 päivänä kesäkuuta 2021,

Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 nojalla henkilötietojen suojan riittävästä tasosta Yhdistyneessä kuningaskunnassa

(tiedoksiannettu numerolla C(2021) 4801)

EUROOPAN KOMISSIO, joka

ottaa huomioon Euroopan unionin toiminnasta tehdyn sopimuksen,

ottaa huomioon luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2016/680 ([1]) ja erityisesti sen 36 artiklan 3 kohdan,

sekä katsoo seuraavaa:

1. JOHDANTO

(1) Direktiivissä (EU) 2016/680 vahvistetaan säännöt, joita sovelletaan henkilötietojen siirtoon unionin toimivaltaisilta viranomaisilta kolmansiin maihin ja kansainvälisille järjestöille, siltä osin kuin tällaiset siirrot kuuluvat sen soveltamisalaan. Toimivaltaisten viranomaisten tekemiä kansainvälisiä tiedonsiirtoja koskevat säännöt vahvistetaan direktiivin (EU) 2016/680 V luvussa ja erityisesti sen 35–40 artiklassa. Tehokkaan lainvalvontayhteistyön kannalta on tarpeen siirtää henkilötietoja Euroopan unionin ulkopuolisiin maihin tai niistä unioniin. Samalla on kuitenkin varmistettava, että tällaisten siirtojen yhteydessä ei heikennetä henkilötietojen suojan tasoa Euroopan unionissa ([2]).

(2) Direktiivin (EU) 2016/680 36 artiklan 3 kohdan mukaan komissio voi päättää täytäntöönpanosäädöksellä, että jokin kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kansainvälinen järjestö varmistaa riittävän tietosuojan tason. Tällä edellytyksellä henkilötietoja voidaan siirtää kolmanteen maahan ilman lisälupaa (paitsi jos siirtoon on saatava lupa toiselta jäsenvaltiolta, jolta tiedot on saatu), kuten direktiivin (EU) 2016/680 35 artiklan 1 kohdassa ja johdanto-osan 66 kappaleessa säädetään.

(3) Kuten direktiivin (EU) 2016/680 36 artiklan 2 kohdassa säädetään, tietosuojan tason riittävyyttä koskevan päätöksen tekemisen on perustuttava kattavaan analyysiin kolmannen maan oikeusjärjestyksestä. Komission on arvioinnissaan määritettävä, takaako kyseinen kolmas maa suojan tason, joka ”vastaa olennaisilta osin” Euroopan unionissa taattua suojan tasoa (direktiivin (EU) 2016/680 johdanto-osan 67 kappale). Vertailukohtana tässä arvioinnissa on EU:n lainsäädännön ja erityisesti direktiivin (EU) 2016/680 ja Euroopan unionin tuomioistuimen oikeuskäytännön ([3]) tarjoama suojan taso. Lisäksi Euroopan tietosuojaneuvoston määrittelemät tietosuojan riittävyyden viitearvot ([4]) ovat tältä osin merkityksellisiä.

(4) Kuten Euroopan unionin tuomioistuin on selventänyt, tämä ei edellytä, että suojelun tason pitäisi olla täysin sama ([5]). Erityisesti keinot, joita kyseisellä kolmannella maalla on käytettävissään henkilötietojen suojaamiseksi, voivat erota Euroopan unionissa käytetyistä menetelmistä, kunhan ne käytännössä varmistavat tehokkaasti suojelun riittävän tason ([6]). Tietosuojan tason riittävyyttä koskeva vaatimus ei sen vuoksi edellytä unionin sääntöjen kopiointia kohta kohdalta. Sen sijaan tarkastellaan, onko ulkomaisen järjestelmän antama suoja kokonaisuutena vaaditun tason mukainen. Tällöin selvitetään, mikä on yksityisyyteen liittyvien oikeuksien sisältö ja pannaanko ne täytäntöön ja valvotaanko niiden toteutumista tehokkaasti ([7]).

([1]) EUVL L 119, 4.5.2016, s. 89.
([2]) Ks. direktiivin (EU) 2016/680 johdanto-osan 64 kappale.
([3]) Ks. viimeksi asia C-311/18, Maximilian Schrems v. Data Protection Commissioner (”Schrems II”) ECLI:EU:C:2020:559.
([4]) Ks. helmikuussa 2021 annetut suositukset 01/2021 riittävyyden viitearvoista lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annetun direktiivin nojalla, saatavilla seuraavassa osoitteessa: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_fi
([5]) Asia C-362/14, Maximilian Schrems v. Data Protection Commissioner (”Schrems”), ECLI:EU:C:2015:650, 73 kohta.
([6]) Tuomio asiassa Schrems, 74 kohta.
([7]) Komission tiedonanto Euroopan parlamentille ja neuvostolle, Henkilötietojen vaihtaminen ja suojaaminen globalisoituneessa maailmassa, COM(2017) 7, 10.1.2017, 3.1 jakso, s. 6–7. Saatavilla seuraavassa osoitteessa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017DC0007&from=FI

(5) Komissio on analysoinut huolellisesti Yhdistyneen kuningaskunnan asiaa koskevaa lainsäädäntöä ja käytäntöä. Jäljempänä esitettyjen havaintojensa perusteella komissio katsoo, että Yhdistynyt kuningaskunta varmistaa tietosuojan riittävän tason sellaisille henkilötiedoille, joita siirretään direktiivin (EU) 2016/680 soveltamisalaan kuuluvilta unionin toimivaltaisilta viranomaisilta Yhdistyneen kuningaskunnan toimivaltaisille viranomaisille, jotka kuuluvat vuoden 2018 tietosuojalain ([8]) 3 osan soveltamisalaan.

(6) Tämän päätöksen vaikutuksena on, että näitä siirtoja voidaan tehdä ilman erillistä lupaa neljän vuoden ajan, sanotun kuitenkaan rajoittamatta direktiivin (EU) 2016/680 35 artiklassa säädettyjen edellytysten soveltamista. Määräaika on mahdollista uusia.

2. TOIMIVALTAISTEN VIRANOMAISTEN RIKOSOIKEUDELLISIA LAINVALVONTATARKOITUKSIA VARTEN SUORITTAMAAN HENKILÖTIETOJEN KÄSITTELYYN SOVELLETTAVAT SÄÄNNÖT

2.1 Perustuslaillinen kehys

(7) Yhdistynyt kuningaskunta on parlamentaarinen demokratia. Maan parlamentilla on täydellinen itsemääräämisoikeus, mikä tarkoittaa, että mikään muu valtioelin ei ole sen yläpuolella. Toimeenpanovallan käyttäjä saa toimivaltansa parlamentilta ja on toimistaan vastuussa sille. Oikeuslaitos on riippumaton. Toimeenpanovallan käyttäjän toimivalta perustuu vaaleilla valitun alahuoneen (House of Commons) luottamukseen, ja se on vastuuvelvollinen parlamentin molemmille kamareille (alahuone eli House of Commons ja ylähuone eli House of Lords). Niiden tehtävänä taas on valvoa hallituksen toimintaa ja hyväksyä lainsäädäntöehdotukset niistä käydyn keskustelun jälkeen. Yhdistyneen kuningaskunnan parlamentti on jakanut Skotlannin parlamentille, Walesin parlamentille (Senedd Cymru) ja Pohjois-Irlannin edustajakokoukselle toimivaltaa, jotta ne voivat antaa kukin alueellaan alueellista lainsäädäntöä tietyissä asioissa. Tietosuojan osalta toimivalta kuuluu Yhdistyneen kuningaskunnan parlamentille, jotta koko maassa sovelletaan sama lainsäädäntöä. Eräät muut tämän päätöksen kannalta merkitykselliset seikat kuuluvat kuitenkin alueellisen toimivallan piiriin. Esimerkiksi Skotlannin ja Pohjois-Irlannin rikosoikeusjärjestelmät, poliisitoimi (poliisiviranomaisten harjoittama toiminta) mukaan lukien, kuuluvat Skotlannin parlamentin ja Pohjois-Irlannin edustajakokouksen toimivallan piiriin ([9]).

(8) Yhdistyneellä kuningaskunnalla ei ole perustamiskirjan tapaista kirjoitettua kodifioitua perustuslakia, vaan sen perustuslailliset periaatteet ovat muodostuneet vähitellen ajan myötä, erityisesti oikeuskäytännön ja tapaoikeuden perusteella. Tiettyjen lakien perustuslaillinen arvo on tunnustettu; näitä ovat mm. Magna Carta, vuoden 1689 oikeuksien julistus (Bill of Rights 1689) ja vuoden 1998 ihmisoikeuslaki (Human Rights Act 1998). Yksilöiden perusoikeuksia on kehitetty osana perustuslakia common law -oikeudessa, mainituilla laeilla ja kansainvälisillä sopimuksilla, erityisesti Euroopan ihmisoikeussopimuksella, jonka Yhdistynyt kuningaskunta ratifioi vuonna 1951. Yhdistynyt kuningaskunta on vuonna 1987 ratifioinut myös Euroopan neuvoston yleissopimuksen (N:o 108) yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä ([10]).

(9) Euroopan ihmisoikeussopimukseen sisältyvät oikeudet on saatettu osaksi Yhdistyneen kuningaskunnan lainsäädäntöä vuoden 1998 ihmisoikeuslailla. Sen mukaan kaikilla yksilöillä on perusoikeudet ja vapaudet, jotka on vahvistettu ihmisoikeussopimuksen 2–12 ja 14 artiklassa, sen ensimmäisen pöytäkirjan 1–3 artiklassa ja kolmannentoista pöytäkirjan 1 artiklassa, luettuna yhdessä ihmisoikeussopimuksen 16–18 artiklan kanssa. Näihin kuuluvat muun muassa oikeus yksityis- ja perhe-elämän kunnioittamiseen, mihin puolestaan sisältyy oikeus tietosuojaan ja oikeus oikeudenmukaiseen oikeudenkäyntiin ([11]). Ihmisoikeussopimuksen 8 artiklassa määrätään erityisesti, että viranomaiset eivät saa puuttua tämän yksityisyydensuojaa koskevan oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

([8]) Vuoden 2018 tietosuojalaki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) Yhdistyneen kuningaskunnan perustelut tietosuojan riittävyyttä koskevalle keskustelulle (UK Explanatory Framework for Adequacy Discussion), F jakso: Law enforcement (lainvalvonta), saatavilla seuraavassa osoitteessa: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) Yleissopimuksen N:o 108 periaatteet saatettiin osaksi Yhdistyneen kuningaskunnan lainsäädäntöä alun perin vuoden 1984 tietosuojalailla (Data Protection Act 1984), joka on sittemmin korvattu vuoden 1998 tietosuojalailla ja viimeksi vuoden 2018 tietosuojalailla (luettuna yhdessä Yhdistyneen kuningaskunnan yleisen tietosuoja-asetuksen (UK GDPR) kanssa).Yhdistynyt kuningaskunta on myös allekirjoittanut vuonna 2018 edellä mainitun yleissopimuksen tarkistamisesta tehdyn pöytäkirjan (ns. yleissopimus 108+) ja valmistautuu parhaillaan yleissopimuksen ratifiointiin.

([11]) Ihmisoikeussopimuksen 6 ja 8 artikla (ks. myös vuoden 1998 ihmisoikeuslain 1 §).

(10) Vuoden 1998 ihmisoikeuslain mukaan kaiken viranomaisten toiminnan on oltava sopusoinnussa ihmisoikeussopimuksessa taatun oikeuden kanssa ([12]). Lisäksi primaari- ja sekundaarilainsäädäntöä on tulkittava ja se on pantava täytäntöön tavalla, joka on sopusoinnussa kyseisten oikeuksien kanssa ([13]). Jos yksityishenkilö katsoo, että viranomaiset ovat rikkoneet hänen oikeuksiaan, kuten oikeutta yksityisyyteen ja tietosuojaan, hän voi hakea muutosta Yhdistyneen kuningaskunnan tuomioistuimissa vuoden 1998 ihmisoikeuslain nojalla. Kun kaikki kansalliset muutoksenhakukeinot on käytetty, hän voi viime kädessä nostaa kanteen Euroopan ihmisoikeustuomioistuimessa Euroopan ihmisoikeussopimuksessa taattujen oikeuksien rikkomisesta.

2.2 **Yhdistyneen kuningaskunnan tietosuojakehys**

(11) Yhdistynyt kuningaskunta erosi unionista 31. tammikuuta 2020. Ison-Britannian ja Pohjois-Irlannin yhdistyneen kuningaskunnan eroamista Euroopan unionista ja Euroopan atomienergiayhteisöstä koskevan sopimuksen ([14]) nojalla unionin oikeutta sovellettiin Yhdistyneeseen kuningaskuntaan ja Yhdistyneessä kuningaskunnassa 31. joulukuuta 2020 päättyneen siirtymäkauden loppuun. Yhdistyneen kuningaskunnan lainsäädäntökehys, joka koskee henkilötietojen suojaa, kun toimivaltaiset viranomaiset käsittelevät henkilötietoja rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy, koostui ennen eroamista ja siirtymäkauden aikana vuoden 2018 tietosuojalain olennaisista osista; kyseisellä lailla oli saatettu direktiivi (EU) 2016/680 osaksi kansallista lainsäädäntöä.

(12) Valmistautuakseen EU:sta eroamiseen Yhdistyneen kuningaskunnan hallitus antoi Euroopan unionista (eroamisesta) vuonna 2018 annetun lain (European Union (Withdrawal) Act 2018), jäljempänä 'eroamista koskeva laki' ([15]), jolla sisällytettiin suoraan sovellettava unionin lainsäädäntö Yhdistyneen kuningaskunnan lainsäädäntöön ja säädettiin, että niin sanottu EU-oikeudesta johdettu sisäinen lainsäädäntö ("EU-derived domestic legislation") on edelleen voimassa siirtymäkauden päätyttyä. Vuoden 2018 tietosuojalain 3 osa ([16]), jolla direktiivi (EU) 2016/680 saatetaan osaksi kansallista lainsäädäntöä, on eroamista koskevassa laissa tarkoitettua EU-oikeudesta johdettua sisäistä lainsäädäntöä. Eroamista koskevan lain mukaan Yhdistyneen kuningaskunnan tuomioistuinten on tulkittava EU-oikeudesta johdettua sisäistä lainsäädäntöä Euroopan unionin tuomioistuimen, jäljempänä 'unionin tuomioistuin', asiaa koskevan oikeuskäytännön, jäljempänä 'säilytetty EU:n oikeuskäytäntö', ja unionin oikeuden yleisten periaatteiden, jäljempänä 'säilytetyt EU:n lainsäädännön yleiset periaatteet', mukaisesti, koska ne olivat voimassa välittömästi ennen siirtymäkauden päättymistä ([17]).

(13) Eroamista koskevan lain mukaan Yhdistyneen kuningaskunnan ministereillä on valtuudet antaa johdetun oikeuden säädöksiä (statutory instruments), joilla tehdään tarvittavat muutokset säilytettyyn EU:n lainsäädäntöön Yhdistyneen kuningaskunnan unionista eroamisen seurauksena. Tietosuojaa, yksityisyydensuojaa ja sähköistä viestintää koskevat säännökset (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019) ([18]) annettiin tämän valtuuden nojalla. Niillä muutetaan Yhdistyneen kuningaskunnan tietosuojalainsäädäntöä, myös vuoden 2018 tietosuojalakia, kansalliseen tilanteeseen sopivaksi ([19]).

([12]) Vuoden 1998 ihmisoikeuslain 6 §.

([13]) Vuoden 1998 ihmisoikeuslain 3 §.

([14]) Sopimus Ison-Britannian ja Pohjois-Irlannin yhdistyneen kuningaskunnan eroamisesta Euroopan unionista ja Euroopan atomienergiayhteisöstä 2019/C 384 I/01, XT/21054/2019/INIT (EUVL C 384 I, 12.11.2019, s. 1–177), jäljempänä 'erosopimus', saatavilla seuraavassa osoitteessa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=FI

([15]) Vuonna 2018 annettu laki Euroopan unionista (eroamisesta), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Vuoden 2018 tietosuojalaki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Vuoden 2018 eroamista koskevan lain 6 §.

([18]) Tietosuojaa, yksityisyydensuojaa ja sähköistä viestintää koskeva säädös (Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/uksi/2019/419/contents/made, sellaisena kuin se on muutettuna tietosuojaa, yksityisyydensuojaa ja sähköistä viestintää koskevalla vuoden 2020 säädöksellä (DPPEC 2020), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) Eroamista koskevassa säädöksessä tehdään useita muutoksia vuoden 2018 tietosuojalain 3 osaan. Monet näistä ovat teknisiä muutoksia, kuten "jäsenvaltioon" tai "direktiiviin lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta" kohdistuvien viittausten poistaminen (ks. esimerkiksi vuoden 2018 tietosuojalain 48 §:n 8 momentti tai 73 §:n 5 momentin a kohta yhdessä kansallisen lainsäädännön kanssa), jotta 3 osa toimisi tehokkaasti kansallisena lakina siirtymäkauden päätyttyä. Joissakin kohdissa tarvittiin muunlaisia muutoksia, esimerkiksi sen osalta, mikä taho tekee tietosuojan tason riittävyyttä koskevan päätöksen Yhdistyneen kuningaskunnan lainsäädäntökehystä varten (ks. vuoden 2018 tietosuojalain 74A §): Secretary of State eikä Euroopan komissio.

(14) Näin ollen oikeudelliset vaatimukset, jotka koskevat henkilötietojen suojaa Yhdistyneessä kuningaskunnassa erosopimuksen mukaisen siirtymäkauden jälkeen, kun toimivaltaiset viranomaiset käsittelevät henkilötietoja rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy, vahvistetaan edelleen vuoden 2018 tietosuojalain asiaa koskevissa osissa, sellaisina kuin ne ovat muutettuina tietosuojaa, yksityisyydensuojaa ja sähköistä viestintää koskevalla säädöksellä, erityisesti sen 3 osalla. Yhdistyneen kuningaskunnan yleistä tietosuoja-asetusta (UK GDPR) ei sovelleta tämäntyyppiseen käsittelyyn.

(15) Vuoden 2018 tietosuojalain 3 osassa vahvistetaan säännöt, jotka koskevat henkilötietojen käsittelyä rikosoikeudellisia lainvalvontatarkoituksia varten, mukaan lukien tietosuojaperiaatteet, käsittelyn oikeudelliset perusteet (lainmukaisuus), rekisteröityjen oikeudet, toimivaltaisten viranomaisten velvollisuudet rekisterinpitäjinä ja tietojen edelleen siirtämistä koskevat rajoitukset. Samalla lainvalvontaan sovellettavat valvontaa, täytäntöönpanoa ja oikeussuojakeinoja koskevat säännöt sisältyvät vuoden 2018 tietosuojalain 5 ja 6 osaan.

(16) Kun lisäksi otetaan huomioon poliisivoimien merkittävä rooli lainvalvonnassa, huomioon olisi otettava myös poliisitoimintaa koskevat säännöt. Koska poliisitoiminta on hajautettu, eri säädöksiä, jotka ovat kuitenkin usein sisällöltään samankaltaisia, sovelletaan poliisitoimintaan a) Englannissa ja Walesissa, b) Skotlannissa ja c) Pohjois-Irlannissa ([20]). Lisäksi erityyppisissä ohjeissa annetaan lisäselvennyksiä siitä, miten poliisin valtuuksia olisi käytettävä. Poliisin ohjeista on kolme päämuotoa: 1) lainsäädännössä olevat ohjeet, kuten vuoden 1996 poliisilain (Police Act 1996) ([21]) mukaiset eettiset säännöt (Code of Ethics) ([22]) ja poliisin hallussa olevien tietojen hallintaa koskeva ohjesääntö (Code of Practice on the Management of Police Information) ([23]) tai poliisista ja rikosasioiden todistusaineistosta annetun lain (Police and Criminal Evidence Act) ([24]) mukaiset PACE-säännöt (PACE codes) ([25]), 2) poliisiakatemian (College of Policing) antamat poliisin hallussa olevien tietojen hallintaa koskevat poliisin sisäiset ohjeet (Authorised Professional Practice on the Management of Police Information) ([26]) ja 3) poliisin julkaisemat toimintaohjeet. Kansallinen poliisipäälliköiden neuvosto (National Police Chiefs Council), joka on Yhdistyneen kuningaskunnan poliisivoimien koordinointielin, julkaisee toimintaohjeita, jotka kaikki poliisivoimat ovat hyväksyneet ja joita sen vuoksi sovelletaan kansallisesti ([27]). Näiden ohjeiden tarkoituksena on varmistaa, että poliisivoimat hallinnoivat tietoja yhdenmukaisesti ([28]).

(17) Secretary of State antoi vuonna 2005 poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön käyttäen vuoden 1996 poliisilain 39A §:ssä säädettyjä valtuuksia ([29]). Poliisilain nojalla annettavilla ohjesäännöillä on oltava Secretary of Staten hyväksyntä, ja ne edellyttävät kansallisen rikosviraston kuulemista, ennen kuin ne esitetään parlamentille. Poliisilain 39A §:n 7 momentissa edellytetään, että poliisi ottaa asianmukaisesti huomioon lain

([20]) Tarkempi selvitys poliisivoimista ja niiden valtuuksista Yhdistyneessä kuningaskunnassa: UK Explanatory Framework for Adequacy Discussion, F jakso: Law Enforcement (ks. alaviite 9).

([21]) Vuoden 1996 poliisilaki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/1996/16/contents

([22]) Englannin ja Walesin poliisitoiminnan periaatteita ja standardeja koskeva ohjesääntö (Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales), saatavilla seuraavassa osoitteessa: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Pohjois-Irlannin poliisilaitoksen eettiset säännöt (Police Service Northern Ireland Code of Ethic), saatavilla seuraavassa osoitteessa: https://www.nipolicingboard.org.uk/psni-code-ethics; Skotlannin poliisitoiminnan eettiset säännöt (Code of Ethic for policing in Scotland), saatavilla seuraavassa osoitteessa: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([23]) Poliisin hallussa olevien tietojen hallintaa koskeva ohjesääntö, saatavilla seuraavassa osoitteessa: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([24]) Vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annettu laki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/1984/60/contents

([25]) Vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annetun lain käytännesäännöt, saatavilla seuraavassa osoitteessa: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([26]) Poliisin hallussa olevien tietojen hallintaa koskevat poliisin sisäiset ohjeet, saatavilla seuraavassa osoitteessa: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Poliisin tietosuojan ammattilaisille tarkoitettu tietosuojakäsikirja (Data Protection Manual for Police Data Protection Professionals), saatavilla seuraavassa osoitteessa: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) Esimerkiksi poliisin hallussa olevien tietojen hallintaa koskevaa ohjesääntöä (ks. alaviite 22) sovelletaan poliisin hallussa olevan operatiivisen tiedon säilyttämiseen (ks. tämän päätöksen johdanto-osan 47 kappale).

([29]) Yhdistyneen kuningaskunnan viranomaisten toimittamien tietojen mukaan tietosuojan riittävyyttä koskevien neuvottelujen aikana poliisiakatemia oli laatimassa tiedonhallintaa koskevaa ohjesääntöä, jolla korvattiin poliisin hallussa olevien tietojen hallintaa koskeva ohjesääntö. Ohjesäännön luonnos julkaistiin julkista kuulemista varten 25. tammikuuta 2021, ja se on saatavilla seuraavassa osoitteessa: https://www.college.police.uk/article/information-records-management-consultation

nojalla annetut säännöt, joten poliisin odotetaan noudattavan niitä ([30]). Lisäksi muiden kuin lakisääteisten ohjeiden (kuten poliisin hallussa olevien tietojen hallintaa koskevat poliisin sisäiset ohjeet) on aina oltava yhdenmukaisia poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön kanssa, joka on säädöshierarkiassa niiden yläpuolella ([31]). Vaikka poliisit saattavat tietyissä operatiivisissa tilanteissa joutua poikkeamaan näistä ohjeista, heidän on joka tapauksessa noudatettava vuoden 2018 tietosuojalain 3 osan vaatimuksia ([32]).

(18) Tietosuojavaltuutettu (Information Commissioner) antaa lisätietoja ([33]) henkilötietojen käsittelystä Yhdistyneen kuningaskunnan lainvalvonnassa (lisätietoja tietosuojavaltuutetusta on johdanto-osan 93–109 kappaleissa). Vaikka nämä ohjeet eivät olekaan muodollisesti velvoittavia, tuomioistuinten olisi otettava huomioon niiden rikkominen, koska niillä on tulkinnallista merkitystä. Lisäksi niistä käy ilmi, miten tietosuojalainsäädäntöä tulkitaan ja miten tietosuojavaltuutettu valvoo sen noudattamista ([34]).

(19) Kuten johdanto-osan 8–10 kappaleessa todetaan, Yhdistyneen kuningaskunnan lainvalvontaviranomaisten on varmistettava Euroopan ihmisoikeussopimuksen ja yleissopimuksen N:o 108 noudattaminen.

(20) Yhdistyneen kuningaskunnan rikosoikeudellisten lainvalvontaviranomaisten suorittamaa tietojen käsittelyä koskeva oikeudellinen kehys on rakenteeltaan ja pääpiirteiltään hyvin samanlainen kuin EU:ssa sovellettava oikeudellinen kehys. Tämä tarkoittaa, että kehys ei perustu ainoastaan kansallisissa laeissa säädettyihin ja EU-lainsäädännön puitteissa muokattuihin velvoitteisiin, vaan myös kansainvälisessä oikeudessa vahvistettuihin velvoitteisiin. Tämä johtuu erityisesti siitä, että Yhdistynyt kuningaskunta on liittynyt Euroopan ihmisoikeussopimukseen ja yleissopimukseen N:o 108, sekä siitä, että maa kuuluu Euroopan ihmisoikeustuomioistuimen toimivallan piiriin. Nämä oikeudellisesti sitovista kansainvälisistä sopimuksista johtuvat velvoitteet, jotka koskevat erityisesti henkilötietojen suojaa, ovat näin ollen erityisen tärkeä osa tässä päätöksessä arvioitavaa oikeudellista kehystä.

2.3 **Aineellinen ja alueellinen soveltamisala**

(21) Vuoden 2018 tietosuojalain 3 osan aineellinen soveltamisala vastaa direktiivin (EU) 2016/680 2 artiklan 2 kohdassa säädettyä soveltamisalaa. Kyseistä 3 osaa sovelletaan toimivaltaisen viranomaisen suorittamaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

(22) Lisäksi rekisterinpitäjä kuuluu kyseisen 3 osan soveltamisalaan vain, jos se on ”toimivaltainen viranomainen” ja käsittely suoritetaan ”lainvalvontatarkoituksessa”. Sen vuoksi tässä päätöksessä arvioitavaa tietosuojajärjestelmää sovelletaan näiden toimivaltaisten viranomaisten kaikkiin lainvalvontatehtäviin.

(23) Tietosuojalain 30 §:ssä määritellään ”toimivaltaisen viranomaisen” käsite siten, että se on vuoden 2018 tietosuojalain liitteen 7 luettelossa mainittu henkilö tai muu henkilö siltä osin, kuin henkilöllä on lakisääteisiä tehtäviä lainvalvonnassa. Liitteen 7 luettelossa oleviin toimivaltaisiin viranomaisiin kuuluvat poliisivoimien lisäksi kaikki Yhdistyneen kuningaskunnan ministeriöiden osastot ja muut viranomaiset, joiden tehtävänä on tutkinta (esim. vero- ja tulliviraston päällikkö (Commissioner for Her Majesty’s Revenue and Customs), Walesin verovirasto (Welsh

([30]) Asiassa R v. the Commission of Police of the Metropolis [2014] EWCA Civ 585 vahvistettiin poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön oikeudellinen asema, ja tuomari Laws totesi, että suur-Lontoon poliisikomentajan (Metropolitan Police Commissioner) on otettava huomioon poliisin hallussa olevien tietojen hallintaa koskeva ohjesääntö ja poliisin hallussa olevien tietojen hallintaa koskevat poliisin sisäiset ohjeet vuoden 1996 poliisilain 39A §:n nojalla.

([31]) Poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön noudattamista valvoo Her Majesty’s Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS).

([32]) Ks. tältä osin poliisiakatemian kanta, joka koskee poliisin hallussa olevien tietojen hallintaa koskevien poliisin sisäisten ohjeiden noudattamista poliisitoiminnassa kaikilta osin. Sen mukaan poliisiakatemia pitää poliisin sisäisiä ohjeita poliisitoiminnan ohjeiden virallisena lähteenä. Poliisien ja henkilöstön odotetaan ottavan poliisin sisäiset ohjeet huomioon hoitaessaan velvollisuuksiaan. Saattaa kuitenkin olla tilanteita, joissa on olemassa perusteltu operatiivinen syy sille, että poliisivoimat poikkeavat poliisin sisäisistä ohjeista, edellyttäen, että tähän on selkeät perusteet. Poliisivoimien olisi kannettava vastuu kaikista paikallisista ja kansallisista riskeistä, jotka liittyvät toimintaan, jossa ei noudateta kansallisesti sovittuja suuntaviivoja, ja jos seurauksena on vaaratilanne tai tutkinta (esimerkiksi riippumattoman poliisitoimintaa tutkivan viraston (Independent Office of Police Conduct) kautta), poliisivoimat ovat vastuussa kaikista riskeistä. Poliisin sisäiset ohjeet ovat saatavilla seuraavassa osoitteessa: https://www.app.college.police.uk/faq-page/

([33]) Henkilötietojen käsittelyä lainvalvonnassa koskevat ohjeet (Guide to Law Enforcement Processing), saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) Ks. asia Bridges v. Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), jossa High Court totesi, että vaikka tietosuojavaltuutetun ohjeet eivät olleet lainsäädännön tasoisia, ”harkitessaan sitä, onko rekisterinpitäjä noudattanut 64 §:n mukaista velvoitetta [suorittaa tietosuojaa koskeva vaikutustenarviointi suuririskisen käsittelyn osalta], tuomioistuin ottaa huomioon tietosuojavaltuutetun tietosuojaa koskevista vaikutustenarvioinneista antamat ohjeet”.

Revenue Authority), kilpailu- ja markkinaviranomainen (Competition and Markets Authority) tai kiinteistörekisteri (Her Majesty's Land Register) tai kansallinen rikosvirasto (National Crime Agency)), syyttäjävirastot (prosecutorial agencies), muut rikosoikeusvirastot ja muut viranhaltijat tai organisaatiot, jotka suorittavat lainvalvontatehtäviä ([35]). Vuoden 2018 tietosuojalain 3 osaa sovelletaan myös tuomioistuimiin niiden hoitaessa oikeudellisia tehtäviään, lukuun ottamatta rekisteröidyn oikeuksia ja tietosuojavaltuutetun valvontaa koskevaa osaa ([36]). Liitteessä 7 oleva toimivaltaisten viranomaisten luettelo ei ole lopullinen, ja Secretary of State voi päivittää sitä asetuksilla ottaen huomioon julkisten virastojen organisaatiossa tapahtuneet muutokset ([37]).

(24) Henkilötietojen käsittelyllä on myös oltava lainvalvontatarkoitus, joka kattaa rikosten ennalta estämisen, tutkimisen, paljastamisen tai rikoksiin liittyvät syytetoimet tai rikosoikeudellisten seuraamusten täytäntöönpanon, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy ([38]). Toimivaltaisen viranomaisen suorittamaan henkilötietojen käsittelyyn ei sovelleta vuoden 2018 tietosuojalain 3 osaa, jos sitä ei suoriteta lainvalvontatarkoituksessa. Näin on esimerkiksi silloin, kun kilpailu- ja markkinaviranomainen tutkii tapauksia, joita ei ole kriminalisoitu (esim. yritysten väliset sulautumat). Tällöin sovelletaan Yhdistyneen kuningaskunnan yleistä tietosuoja-asetusta yhdessä vuoden 2018 tietosuojalain 2 osan kanssa, koska toimivaltaiset viranomaiset käsittelevät henkilötietoja muissa kuin lainvalvontatarkoituksissa. Määrittääkseen, mitä tietosuojajärjestelmää (vuoden 2018 tietosuojalain 3 tai 2 osa) sovelletaan kyseessä olevien henkilötietojen käsittelyyn, toimivaltaisen viranomaisen eli rekisterinpitäjän on harkittava, onko tällaisen käsittelyn "ensisijainen tarkoitus" jokin vuoden 2018 tietosuojalain mukaisista lainvalvontatarkoituksista.

(25) Vuoden 2018 tietosuojalain 3 osan alueellisen soveltamisalan osalta 207 §:n 2 momentissa säädetään, että tietosuojalakia sovelletaan henkilötietojen käsittelyyn sellaisen henkilön toiminnan yhteydessä, jonka toimialue kattaa koko Yhdistyneen kuningaskunnan alueen. Tähän sisältyvät Englannin, Walesin, Skotlannin ja Pohjois-Irlannin alueiden viranomaiset, jotka kuuluvat vuoden 2018 tietosuojasopimuksen 3 osan aineelliseen soveltamisalaan ([39]).

2.3.1 *Henkilötietojen ja käsittelyn määritelmät*

(26) Henkilötietojen ja käsittelyn keskeiset käsitteet on määritelty vuoden 2018 tietosuojalain 3 §:ssä, ja niitä sovelletaan koko tietosuojalaissa. Määritelmät vastaavat läheisesti direktiivin (EU) 2016/680 3 artiklassa vahvistettuja määritelmiä. Vuoden 2018 tietosuojalain mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan elävään henkilöön ([40]) liittyviä tietoja. Vuoden 2018 tietosuojalain 3 §:n 3 momentin mukaan henkilö on tunnistettavissa, jos hänet voidaan tietojen perusteella tunnistaa suoraan tai epäsuorasti. Näihin tietoihin kuuluvat viittaus nimeen tai tunnisteeseen taikka yhteen tai useampaan henkilön fyysiselle, fysiologiselle, geneettiselle, psyykkiselle, taloudelliselle, kulttuuriselle tai sosiaaliselle identiteetille ominaiseen tekijään. 'Käsittelyllä' tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin, kuten a) kerääminen, tallentaminen, järjestäminen, jäsentäminen tai säilyttäminen; b) muokkaaminen tai muuttaminen; c) haku, kysely tai käyttö; d) luovuttaminen siirtämällä, levittämällä tai asettamalla muutoin saataville; e) yhteensovittaminen tai yhdistäminen; tai f) rajoittaminen, poistaminen tai tuhoaminen. Lisäksi laissa määritellään 'arkaluontoinen käsittely' seuraavasti: "a) sellaisten henkilötietojen käsittely, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys; b) geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten; c) terveyttä koskevien tietojen käsittely; d) henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely" ([41]). Tältä osin vuoden 2018 tietosuojalain 205 §:ssä määritellään 'biometriset tiedot' ([42]), 'terveyttä koskevat tiedot' ([43]) ja 'geneettiset tiedot' ([44]).

([35]) Vuoden 2018 tietosuojalain liitteessä 7 luetellaan muun muassa yleisten syyttäjien johtajat, Pohjois-Irlannin syyttäjäviranomaisten johtaja tai tietosuojavaltuutettu.

([36]) Vuoden 2018 tietosuojalain 43 §:n 3 momentti.

([37]) Vuoden 2018 tietosuojalain 30 §:n 3 momentti. Tiedustelupalvelut (salainen tiedustelupalvelu (Secret Intelligence Service), turvallisuuspalvelu (Security Service) ja tiedustelupalvelu (Government Communications Headquarters)) eivät ole toimivaltaisia viranomaisia (ks. vuoden 2018 tietosuojalain 30 §:n 2 momentti), eikä vuoden 2018 tietosuojalain 3 osaa sovelleta mihinkään niiden toimintaan. Niiden toimet kuuluvat vuoden 2018 tietosuojalain 4 osan soveltamisalaan.

([38]) Vuoden 2018 tietosuojalain 31 §.

([39]) Tämä tarkoittaa sitä, että vuoden 2018 tietosuojalakia ja siten myöskään tätä päätöstä ei sovelleta Yhdistyneen kuningaskunnan kruunun alaisuuteen kuuluvilla alueilla eikä muilla Yhdistyneen kuningaskunnan merentakaisilla alueilla, kuten esimerkiksi Falklandinsaarilla tai Gibraltarin alueella.

([40]) Edesmenneen henkilön henkilötiedot eivät kuulu vuoden 2018 tietosuojalain soveltamisalaan.

([41]) Vuoden 2018 tietosuojalain 35 §:n 8 momentti.

([42]) 'Biometrisillä tiedoilla' tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä tietyllä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön yksiselitteinen tunnistaminen voidaan varmistaa.

([43]) 'Terveystiedoilla' tarkoitetaan luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, mukaan lukien tiedot terveyspalvelujen tarjoamisesta, jotka ilmaisevat hänen terveydentilansa.

([44]) 'Geneettisillä tiedoilla' tarkoitetaan henkilötietoja, jotka koskevat luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista selviää yksilöllistä tietoa kyseisen luonnollisen henkilön fysiologiasta tai terveydentilasta ja jotka on saatu erityisesti kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla.

(27) Vuoden 2018 tietosuojalain 32 §:ssä selvennetään 'rekisterinpitäjän' ja 'henkilötietojen käsittelijän' määritelmiä lainvalvontatarkoituksessa tapahtuvan henkilötietojen käsittelyn yhteydessä noudattaen tarkasti direktiivin (EU) 2016/680 vastaavia määritelmiä. Rekisterinpitäjällä tarkoitetaan toimivaltaista viranomaista, joka määrittää henkilötietojen käsittelyn tarkoitukset ja keinot. Jos käsittely on lain mukaan pakollista, rekisterinpitäjä on se toimivaltainen viranomainen, jota laissa säädetty velvoite koskee. Henkilötietojen käsittelijällä tarkoitetaan henkilöä, joka käsittelee henkilötietoja rekisterinpitäjän puolesta (muu henkilö kuin rekisterinpitäjän työntekijä).

2.4 **Suojatoimet, oikeudet ja velvollisuudet**

2.4.1 *Tietojenkäsittelyn lainmukaisuus ja asianmukaisuus*

(28) Vuoden 2018 tietosuojalain 35 §:n mukaan henkilötietojen käsittelyn on oltava lainmukaista ja asianmukaista, samalla tavalla kuin direktiivin (EU) 2016/680 4 artiklan 1 kohdan a alakohdassa säädetään. Vuoden 2018 tietosuojalain 35 §:n 2 momentin mukaan henkilötietojen käsittely jotakin lainvalvontatarkoitusta varten on lainmukaista vain, jos käsittely perustuu lainsäädäntöön ja rekisteröity on antanut suostumuksensa tietojen käsittelyyn tätä tarkoitusta varten tai jos käsittely on tarpeen toimivaltaisen viranomaisen tätä tarkoitusta varten suorittaman tehtävän suorittamiseksi.

2.4.1.1 Lakiin perustuva käsittely

(29) Vuoden 2018 tietosuojalain 3 osan soveltamisalaan kuuluvan tietojenkäsittelyn lainmukaisuuden varmistamiseksi tällaisen käsittelyn on perustuttava lainsäädäntöön, kuten myös direktiivin (EU) 2016/680 8 artiklassa säädetään. "Lainmukaisella" tietojenkäsittelyllä tarkoitetaan, että siihen on saatu lupa joko lain, common law'n tai kuninkaallisen etuoikeuden (royal prerogatives) nojalla ([45]).

(30) Toimivaltaisten viranomaisten toimivaltuudet ovat yleensä lakisääteisiä, mikä tarkoittaa, että niiden tehtävät ja valtuudet on määritelty selkeästi parlamentin hyväksymässä lainsäädännössä ([46]). Tietyissä tapauksissa poliisi ja muut vuoden 2018 tietosuojalain liitteessä 7 luetellut toimivaltaiset viranomaiset voivat käyttää perusteena common law -oikeutta, kun ne käsittelevät henkilötietoja ([47]). Common law perustuu tuomioistuinten ennakkotapauksiin. Common law on merkityksellinen, kun tarkastellaan poliisin siihen perustuvia toimivaltuuksia ja poliisin keskeistä velvollisuutta suojella yleisöä paljastamalla ja ehkäisemällä rikollisuutta ([48]). Poliisivoimilla on kuitenkin sekä common law -oikeuteen että

([45]) Vuoden 2018 tietosuojalain selittävät huomautukset, 181 kohta, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf

([46]) Esimerkiksi kansallisen rikosviraston (National Crime Agency) toimivallasta säädetään vuonna 2013 rikoksista ja tuomioistuimista annetussa laissa (Crime and Courts Act 2013), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2013/22/contents. Vastaavasti elintarvikenormiviraston (Food Standards Agency) toimivallasta säädetään vuoden 1999 elintarvikelaissa (Food Standards Act 1999), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/1999/28/contents. Muita esimerkkejä ovat vuonna 1985 rikoksentekijöiden syytteeseenpanosta annettu laki (Prosecution of Offenders Act 1985), jolla perustettiin valtionsyyttäjänvirasto (Crown Prosecution Service) (ks. https://www.legislation.gov.uk/ukpga/1985/23/contents); vuoden 2005 vero- ja tullilaki, jolla perustettiin vero- ja tullivirasto (Her Majesty's Revenue and Customs) (ks. https://www.legislation.gov.uk/ukpga/2005/11/contents); vuoden 1995 Skotlannin rikosprosessilaki (Criminal Procedure (Scotland) Act 1995), jolla perustettiin rikosasioiden tarkastuslautakunta (Scottish Criminal Cases Review Commission) (ks. https://www.legislation.gov.uk/ukpga/1995/46/contents); vuoden 2002 Pohjois-Irlannin oikeudenkäyttölaki (Justice (Northern Ireland) Act 2002), jolla perustettiin Pohjois-Irlannin syyttäjälaitos (ks. https://www.legislation.gov.uk/ukpga/2002/26/contents), ja törkeiden petosten torjuntavirasto (Serious Fraud Office), joka perustettiin ja jolle annettiin toimivaltuudet vuoden 1987 rikosoikeuslaissa (Criminal Justice Act 1987) (ks. https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Yhdistyneen kuningaskunnan viranomaisten antamien tietojen mukaan esimerkiksi Skotlannin syyttäjälaitoksen (Crown Office and Procurator Fiscal Service) ylimmän syyttäjän (Lord Advocate) toimivalta tutkia kuolemantapauksia ja nostaa syytteitä rikoksista perustuu common law -oikeuteen, kun taas osa hänen tehtävistään on vahvistettu laissa. Lisäksi kruunun ja sitä kautta useat hallituksen, ministeriöiden ja ministerien toimivaltuudet perustuvat lakien, common law -oikeuden ja kuninkaallisen etuoikeuden yhdistelmään (nämä ovat kruunulle annettuja common law -toimivaltuuksia, joita ministerit kuitenkin käyttävät).

([48]) UK Explanatory Framework for adequacy Discussion, F jakso: Law Enforcement, sivu 8 (ks. alaviite 9).

lainsäädäntöön ([49]) perustuva toimivalta velvollisuutensa suorittamiseen. Jos poliisilla on lakisääteinen toimivalta, se syrjäyttää common law -valtuudet ([50]).

(31) Oikeuskäytännön mukaan poliisin common law -oikeuden mukaisiin valtuuksiin ja velvollisuuksiin sisältyvät kaikki toimenpiteet, jotka poliisin mielestä ovat välttämättömiä rauhan ylläpitämiseksi, rikosten ehkäisemiseksi tai omaisuuden suojelemiseksi rikoksilta ([51]). Common law -valtuudet eivät ole rajoittamattomia valtuuksia. Niihin kohdistuu monenlaisia rajoituksia, kuten tuomioistuinten ([52]) asettamia rajoituksia ja lainsäädännössä, erityisesti vuoden 1998 ihmisoikeuslaissa ja vuoden 2010 tasa-arvolaissa (Equality Act) ([53]), säädettyjä rajoituksia. Lisäksi niiden toimivaltaisten viranomaisten osalta, jotka käsittelevät tietoja vuoden 2018 tietosuojalain 3 osan nojalla, mainitussa laissa vahvistetut vaatimukset rajoittavat common law -valtuuksien käyttöä ([54]). Kaikissa tietojenkäsittelyä koskevissa päätöksissä on myös otettava huomioon sovellettavien ohjeiden, kuten poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön, vaatimukset sekä asianomaisessa Yhdistyneen kuningaskunnan osassa sovellettavat ohjeet ([55]). Hallitus ja operatiivinen poliisitoimi ovat antaneet useita ohjeasiakirjoja sen varmistamiseksi, että poliisit käyttävät toimivaltuuksiaan common law -oikeuden tai asiaa koskevan lain asettamissa rajoissa ([56]).

(32) Kuninkaalliset etuoikeudet muodostavat osan ”oikeutta”. Niillä viitataan tiettyihin kruunulle annettuihin ja toimeenpanovallan käyttäjän käytettävissä oleviin toimivaltuuksiin, jotka eivät perustu säädettyyn lakiin vaan monarkin suvereniteettiin ([57]). On hyvin vähän esimerkkejä etuoikeuksista, joilla on merkitystä lainvalvonnan kannalta. Niihin kuuluu esimerkiksi keskinäisen oikeusavun kehys, jonka perusteella Secretary of State voi jakaa tietoja kolmansien maiden kanssa lainvalvontatarkoituksia varten, eikä tällaista toimivaltaa jakaa tietoja ole aina

([49]) Keskeiset säädökset, joissa säädetään tärkeimmistä poliisivaltuuksista (pidättäminen, etsinnät, vapaudenmenetyksen jatkamista koskeva lupa, sormenjälkien ottaminen, intiimien näytteiden ottaminen, salakuuntelu, pääsy viestintätietoihin), ovat seuraavat: i) Englannin ja Walesin osalta vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annettu laki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/1984/60/contents (sellaisena kuin se on muutettuna vuonna 2012 vapauksien suojelusta annetulla lailla (Protection of Freedoms Act 2012), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2012/9/contents) ja vuonna 2016 tutkintavaltuuksista annettu laki (Investigatory Powers Act 2016), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) Skotlannin osalta rikosoikeuslaki (Criminal Justice (Scotland) Act 2016), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/asp/2016/1/contents ja rikosprosessilaki (Criminal Procedure (Scotland) Act 1995), saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/1995/46/contents) iii) Pohjois-Irlannin osalta vuoden 1989 poliisista ja rikosasioiden todistusaineistosta annettu laki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/nisi/1989/1341/contents

([50]) Yhdistyneen kuningaskunnan viranomaiset ovat selittäneet, että säädetyn lain ensisijaisuus on vakiintunut jo kauan sitten Yhdistyneessä kuningaskunnassa. Tämä käy ilmi jo asiassa Entick v. Carrington [1765] EWHC KB J98 annetussa tuomiossa, jossa tunnustettiin, että toimeenpanovallan käytettävyydessä oli rajoituksia, ja vahvistettiin periaate, jonka mukaan tapaoikeuden mukaiset valtaoikeudet ja monarkin ja hallituksen etuoikeudet ovat hierarkiassa maanlain (law of the land) alapuolella.

([51]) Ks. asia Rice v. Connolly [1966] 2 QB 414.

([52]) Ks. asia R(Catt) v. Association of Chief police Officers [2015] AC 1065, jossa sen osalta, onko poliisilla valtuudet hankkia ja säilyttää tietoja yksittäisestä henkilöstä (joka on tehnyt rikoksen), lordi Sumption katsoi, että common law -oikeuden mukaan poliisilla on oikeus hankkia ja tallentaa tietoja poliisitoimintaa varten eli yleisesti ottaen yleisen järjestyksen ylläpitämiseksi sekä rikosten ehkäisemiseksi ja paljastamiseksi. Yksityisyyteen puuttuvat tiedonhankintamenetelmät, kuten yksityisalueelle tunkeutuminen tai henkilön fyysiseen koskemattomuuteen kohdistuvat teot (muut kuin common law -valtuuksiin perustuvat pidätykset) eivät sisälly näihin valtuuksiin. Tuomari katsoi, että tässä tapauksessa common law -valtuudet riittivät täysin siihen, että näissä valituksissa kyseessä olleen kaltaisen julkisen tiedon hankkiminen ja tallentaminen oli sallittua.

([53]) Vuoden 2010 tasa-arvolaki, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) Esimerkki tapauksesta, jossa poliisin common law -valtuuksia arvioidaan vuoden 1998 tietosuojalain puitteissa, ks. High Courtin asiassa Bridges v. Chief Constable of South Wales Police antama tuomio (ks. alaviite 33). Ks. myös asiat Vidal-Hall v. Google Inc [2015] EWCA Civ 311 ja Richard v. BBC [2018] EWHC 1837 (Ch).

([55]) Ks. esimerkiksi Pohjois-Irlannin poliisiviraston todisteiden hallintaa koskevat ohjeet, saatavilla seuraavassa osoitteessa: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Parlamentin alahuone on julkaissut muistion, jossa esitellään Englannin ja Walesin poliisin keskeiset common law -säännöt ja lakisääteiset toimivaltuudet (ks. https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Asiakirjan mukaan esimerkiksi valta ylläpitää ”kruunun rauhaa” perustuu common law -oikeuteen samoin kuin voimankäyttö, kun taas pysäytys- ja etsintävaltuudet perustuvat aina säädettyyn lakiin. Lisäksi Skotlannin hallitus antaa verkkosivustollaan tietoa poliisin pidätys- ja pysäytysvaltuuksista (ks. https://www.gov.scot/policies/police/police-powers/).

([57]) Yhdistyneen kuningaskunnan viranomaisten toimittamien tietojen mukaan hallituksen valtaoikeuksiin kuuluvat esimerkiksi sopimusten tekeminen ja ratifiointi, diplomatian harjoittaminen ja asevoimien käyttö rauhan ylläpitämiseksi poliisin tukena Yhdistyneessä kuningaskunnassa.

vahvistettu lainsäädännössä ([58]). Kuninkaallisiin etuoikeuksiin sovelletaan common law -periaatteita ([59]), ja koska ne ovat normihierarkiassa säädetyn lain alapuolella, niihin sovelletaan myös vuoden 1998 ihmisoikeuslaissa ja vuoden 2018 tietosuojalaissa säädettyjä rajoituksia ([60]).

(33) Yhdistyneen kuningaskunnan järjestelmässä edellytetään samalla tavalla kuin direktiivin (EU) 2016/680 8 artiklassa, että lainmukaisuuden periaatteen noudattamiseksi toimivaltaisten viranomaisten olisi varmistettava, että kun henkilötietojen käsittely perustuu lakiin, sen on myös oltava ”tarpeen” lainvalvontatarkoituksessa suoritettavan tehtävän suorittamiseksi. Tietosuojavaltuutetun ohjeissa selvennetään tältä osin, että käsittelyn on oltava kohdennettu ja oikeasuhteinen keino tavoitteen saavuttamiseksi. Käsittely ei ole lainmukaista, jos tavoite voidaan kohtuudella saavuttaa muilla vähemmän yksityisyyteen puuttuvilla keinoilla. Väite, jonka mukaan käsittely on tarpeen, koska liiketoimintaa on päätetty harjoittaa tietyllä tavalla, ei ole riittävä. Kysymys on siitä, onko käsittely tarpeen ilmoitettua tarkoitusta varten ([61]).

2.4.1.2 Käsittely rekisteröidyn ”suostumuksen” perusteella

(34) Kuten johdanto-osan 28 kappaleessa todetaan, vuoden 2018 tietosuojalain 35 §:n 2 momentissa säädetään mahdollisuudesta käsitellä henkilötietoja henkilön ”suostumuksen” perusteella.

(35) Suostumus ei kuitenkaan näytä olevan tämän päätöksen soveltamisalaan kuuluvien käsittelytoimien kannalta merkityksellinen oikeusperusta. Itse asiassa tämän päätöksen soveltamisalaan kuuluvat käsittelytoimet koskevat aina tietoja, jotka jäsenvaltion toimivaltainen viranomainen on siirtänyt direktiivin (EU) 2016/680 nojalla Yhdistyneen kuningaskunnan toimivaltaiselle viranomaiselle. Näin ollen niihin ei yleensä liity viranomaisen ja rekisteröityjen välistä suoraa vuorovaikutusta (tietojen keruuta), joka voi perustua vuoden 2018 tietosuojalain 35 §:n 2 momentin a kohdan mukaiseen suostumukseen.

(36) Vaikka suostumuksen käyttämistä perusteena ei näin ollen pidetä merkityksellisenä tämän päätöksen nojalla suoritettavan arvioinnin kannalta, on syytä todeta kattavuuden vuoksi, että lainvalvontaan liittyvä käsittely ei koskaan perustu pelkästään suostumukseen, sillä toimivaltaisella viranomaisella on aina oltava valtuudet käsitellä tietoja ([62]). Tarkemmin sanottuna ja samoin kuin direktiivissä (EU) 2016/680 ([63]) sallitaan, tämä tarkoittaa sitä, että suostumus on lisäedellytys sille, että mahdollistetaan tietyt rajoitetut ja erityiset käsittelytoimet, joita ei muutoin voitaisi suorittaa, esimerkiksi sellaisen henkilön DNA-näytteen ottaminen ja käsittely, joka ei ole epäilty. Tässä tapauksessa käsittelyä ei suoriteta, jos suostumusta ei anneta tai se peruutetaan ([64]).

([58]) Ks. tietojen edelleen siirtämistä koskevan Yhdistyneen kuningaskunnan järjestelmän arviointi johdanto-osan 74–87 kappaleessa.

([59]) Ks. asia Bancoult v. Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, jossa tuomioistuimet katsoivat, että myös valta antaa määräyksiä (Orders in Council) kuului yleisen tuomioistuinvalvonnan piiriin.

([60]) Ks. asia Attorney-General v. De Keyser’s Royal Hotel Ltd [1920] [1920] AC 508, jossa tuomioistuin katsoi, että etuoikeuksien suomia valtuuksia ei voida käyttää, kun ne on korvattu lainsäädännössä säädetyillä valtuuksilla; asia Laker Airways Ltd v. Department of Trade [1977] QB 643, jossa tuomioistuin totesi, että etuoikeuksien suomia valtuuksia ei voida käyttää säädetyn lain kiertämiseksi; asia R v. Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, jossa tuomioistuin katsoi, että etuoikeuksien suomia valtuuksia ei voida käyttää, jos ne ovat ristiriidassa hyväksytyn lainsäädännön kanssa, vaikka hyväksytty lainsäädäntö ei olisi vielä voimassa; asia R (Miller) v. Secretary of State for Exiting the European Union [2017] UKSC 5, jossa tuomioistuin vahvisti, että säädetyllä lailla voidaan mukauttaa ja poistaa etuoikeuksia. Alahuoneen muistiossa esitetty yleiskatsaus kuninkaallisten etuoikeuksien ja säädettyyn lakiin tai common law -oikeuteen liittyvien toimivaltuuksien välisestä suhteesta, saatavilla seuraavassa osoitteessa: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) Henkilötietojen käsittelyä lainvalvonnassa koskevat ohjeet, ensimmäisen periaatteen kuvaus (“What is the first principle about?”), saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Tämä johtuu vuoden 2018 tietosuojalain asianomaisen säännöksen sanamuodosta. Sen mukaan henkilötietojen käsittely jotakin lainvalvontatarkoitusta varten on lainmukaista vain, jos ja siltä osin kuin käsittely ”perustuu lainsäädäntöön” ja a) rekisteröity on antanut suostumuksensa tietojen käsittelyyn tätä tarkoitusta varten tai b) käsittely on tarpeen toimivaltaisen viranomaisen tätä tarkoitusta varten suorittaman tehtävän toteuttamiseksi.

([63]) Ks. direktiivin (EU) 2016/680 johdanto-osan 35 ja 37 kappale.

([64]) Yhdistyneen kuningaskunnan viranomaiset ovat selittäneet, että suostumus voi olla asianmukainen perusta tietojen käsittelylle esimerkiksi silloin, kun poliisi saa kadonneen henkilön tapausta tutkittaessa DNA-näytteen, jota voidaan verrata ruumiiseen, jos sellainen löydetään. Tällaisessa tilanteessa poliisin ei olisi asianmukaista pakottaa rekisteröityä toimittamaan näyte. Sen sijaan poliisi pyytää henkilön suostumuksen, joka annetaan vapaaehtoisesti ja joka voidaan peruuttaa milloin tahansa. Jos suostumus peruutetaan, tietoja ei enää voida käsitellä, ellei näytteen käsittelyn jatkamiselle ole ilmennyt uutta oikeusperustaa (esim. rekisteröidystä on tullut epäilty). Toinen esimerkki voisi olla tilanne, jossa poliisi tutkii rikosta, jonka uhri (esim. ryöstön, seksuaalirikoksen tai perheväkivallan uhri, henkirikoksen uhrin sukulaiset tai muu rikoksen uhri) voisi hyötyä uhrien tukipalvelusta (riippumaton hyväntekeväisyysjärjestö, jonka tehtävänä on tukea rikoksesta ja traumaattisista tapahtumista kärsiviä ihmisiä). Tällaisessa tilanteessa poliisi toimittaa uhrien tukipalvelulle henkilötiedot, kuten nimen ja yhteystiedot, vain jos uhri on antanut siihen suostumuksensa.

(37) Tapauksissa, joissa edellytetään yksilön suostumusta, suostumuksen on oltava yksiselitteinen ja se on annettava toteuttamalla selvästi suostumusta ilmaiseva toimi ([65]). Poliisivoimilla on oltava tietosuojaseloste, joka sisältää muun muassa tarvittavat tiedot suostumuksen asianmukaisesta käytöstä. Lisäksi jotkin poliisin yksiköt julkaisevat lisäaineistoa siitä, miten ne noudattavat tietosuojalainsäädäntöä, esimerkiksi miten ja milloin ne käyttäisivät suostumusta oikeusperustana ([66]).

2.4.1.3 Arkaluontoinen käsittely

(38) ”Erityisiä tietoryhmiä” käsiteltäessä olisi sovellettava erityisiä suojatoimia. Vuoden 2018 tietosuojalain 3 osassa samoin kuin direktiivin (EU) 2016/680 10 artiklassa säädetään vahvemmista suojatoimista niin sanottua arkaluontoista käsittelyä varten ([67]).

(39) Vuoden 1998 tietosuojalain 35 §:n 3 momentin mukaan toimivaltaiset viranomaiset voivat käsitellä arkaluontoisia tietoja lainvalvontatarkoituksessa vain kahdessa tapauksessa: 1) rekisteröity on antanut suostumuksensa tietojen käsittelyyn lainvalvontatarkoituksessa, ja käsittelyn ajankohtana rekisterinpitäjällä on käytössään asianmukainen toimintapoliittinen asiakirja ([68]); tai 2) käsittely on ehdottoman välttämätöntä lainvalvontatarkoitusta varten, käsittely täyttää vähintään yhden vuoden 2018 tietosuojalain liitteessä 8 vahvistetuista edellytyksistä, ja käsittelyn suorittamishetkellä rekisterinpitäjällä on käytössään asianmukainen toimintapoliittinen asiakirja ([69]).

(40) Ensimmäisen tapauksen osalta ja kuten johdanto-osan 38 kappaleessa selitetään, suostumuksen käyttämistä perusteena ei pidetä merkityksellisenä tämän päätöksen soveltamisalaan kuuluvassa siirtotilanteessa ([70]).

(41) Jos arkaluontoisten tietojen käsittely ei perustu suostumukseen, se voidaan suorittaa käyttäen jotakin vuoden 2018 tietosuojalain liitteessä 8 luetelluista edellytyksistä. Nämä edellytykset liittyvät käsittelyyn, joka on tarpeen laissa säädettyjä tarkoituksia, tuomiovaltaa, rekisteröidyn tai toisen henkilön elintärkeiden etujen suojaamista, lasten ja vaarassa olevien henkilöiden suojelua, oikeudellisia vaateita, oikeudellisia toimia, petosten ehkäisemistä ja arkistointia varten, jos rekisteröity on selvästi julkistanut henkilötiedot. Lukuun ottamatta tapauksia, joissa tiedot on selvästi julkistettu, kaikkiin liitteessä 8 esitettyihin edellytyksiin sovelletaan ”ehdottoman välttämättömyyden” kriteeriä. Kuten tietosuojavaltuutettu on selventänyt, ”tässä yhteydessä ehdottoman välttämätön tarkoittaa, että käsittelyn on liityttävä pakottavaan yhteiskunnalliseen tarpeeseen, eikä tavoitetta voida kohtuudella saavuttaa

([65]) Vuoden 2018 tietosuojalain 3 osassa ei ole erillistä suostumuksen määritelmää henkilötietojen käsittelyä varten. Tietosuojavaltuutettu on antanut ohjeita vuoden 2018 tietosuojalain 3 osan mukaisesta ”suostumuksen” käsitteestä selventäen, että sillä on sama merkitys ja sen olisi oltava yhdenmukainen yleisessä tietosuoja-asetuksessa olevan määritelmän kanssa. Sen mukaan suostumuksen on oltava vapaaehtoinen, yksilöity ja tietoisesti annettu, ja sen antajan on voitava aidosti valita, että hän antaa suostumuksen käsitellä tietoja. (Guide to Law Enforcement Processing, “What is the first principle about?” (ks. alaviite 64) ja suostumusta koskeva tietosuojaohje (Guide to Data Protection on consent), saatavana seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Ks. esim. tiedot Lincolnshiren poliisin verkkosivuilla (ks. https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) tai West Yorkshiren poliisin verkkosivuilla (ks. https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Vuoden 2018 tietosuojalain 35 §:n 8 momentti.

([68]) Vuoden 2018 tietosuojalain 35 §:n 4 momentti.

([69]) Vuoden 2018 tietosuojalain 35 §:n 5 momentti.

([70]) Kattavuuden vuoksi on syytä huomata, että kun käsittely perustuu suostumukseen, suostumuksen on oltava vapaaehtoinen, yksilöity ja tietoisesti annettu, ja sen antajan on erityisesti voitava valita suostuminen tietojen käsittelyyn. Lisäksi kun rekisterinpitäjä käsittelee tietoja rekisteröidyn suostumuksen perusteella, sillä on oltava käytössään ”asianmukainen toimintapoliittinen asiakirja”. Vuoden 2018 tietosuojalain 42 §:ssä esitetään vaatimukset, jotka asianmukaisen toimintapoliittisen asiakirjan on täytettävä. Siinä tehdään selväksi, että asiakirjassa on vähintään selitettävä, miten rekisterinpitäjän on meneteltävä varmistaakseen tietosuojaperiaatteiden noudattamisen, ja mitkä ovat henkilötietojen säilyttämistä ja poistamista koskevat rekisterinpitäjän toimintaperiaatteet. Vuoden 2018 tietosuojalain 42 §:n mukaan tämä tarkoittaa, että rekisterinpitäjän on esitettävä asiakirja, jossa a) selitetään rekisterinpitäjän menettelyt tietosuojaperiaatteiden noudattamisen varmistamiseksi; ja b) selitetään rekisterinpitäjän toimintaperiaatteet, jotka koskevat rekisteröidyn suostumuksen perusteella käsiteltävien henkilötietojen säilyttämistä ja poistamista tai ilmoituksen antamista siitä, kuinka kauan henkilötietoja todennäköisesti säilytetään. Toimintapoliittisessa asiakirjassa edellytetään erityisesti, että rekisterinpitäjän on aina toteutettava a ja b alakohdassa mainitut seikat käsittelytoimien kirjaamista koskevan velvoitteensa suorittamiseksi. Tietosuojavaltuutettu on julkaissut henkilötietojen käsittelyä lainvalvonnassa koskevan malliasiakirjan, jossa tarkastellaan myös arkaluontoisen käsittelyn edellytyksiä (Guide to Law Enforcement Processing. Conditions for sensitive processing, saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing). Tietosuojavaltuutettu voi ryhtyä valvontatoimiin, jos rekisterinpitäjä ei täytä näitä vaatimuksia. Myös tuomioistuimet tarkastelevat asianmukaista toimintapoliittista asiakirjaa käsitellessään vuoden 2018 tietosuojalain mahdollisia rikkomisia. Esimerkiksi äskettäisessä asiassa R (Bridges) v. Chief Constable of South Wales Police tuomioistuimet tarkastelivat rekisterinpitäjän asianmukaista toimintapoliittista asiakirjaa ja pitivät sitä riittävänä mutta katsoivat, että sen täydentämisestä voisi olla hyötyä. Tämän seurauksena Etelä-Walesin poliisi tarkasteli asianmukaista toimintapoliittista asiakirjaa ja päivitti sitä tietosuojavaltuutetun uusien ohjeiden mukaisesti (ks. alaviite 33). Lisäksi vuoden 2018 tietosuojalain 42 §:n 3 momentin mukaan rekisterinpitäjän olisi tarkasteltava asianmukaista toimintapoliittista asiakirjaa säännöllisesti uudelleen. Vuoden 2018 tietosuojalain 42 §:n 4 momentin mukaan rekisterinpitäjän on täydentävänä suojatoimena pidettävä käsittelytoimista laajennettua kirjaa. Tämä velvoite on laajempi verrattuna yleiseen velvoitteeseen, jonka mukaan rekisterinpitäjän on pidettävä kirjaa vuoden 2018 tietosuojalain 61 §:ssä säädetyistä käsittelytoimista.

vähemmän yksityisyyteen puuttuvilla keinoilla" ([71]). Lisäksi joihinkin edellytyksiin sovelletaan lisärajoituksia. Esimerkiksi jotta voitaisiin käyttää perustana "laissa säädettyjä tarkoituksia" tai "suojelua koskevia edellytyksiä" (liitteessä 8 oleva 1 ja 4 kohta) on lisävaatimuksena, että näin voidaan saavuttaa merkittävää yleistä etua. Lisäksi lapsen suojelua koskevien edellytysten osalta (liitteessä 8 oleva 4 kohta) rekisteröidyn on myös oltava tietynikäinen ja hänen on katsottava olevan vaarassa. Lisäksi rekisterinpitäjä voi soveltaa liitteessä 8 olevassa 4 kohdassa säädettyä edellytystä vain erityisissä olosuhteissa ([72]). Vastaavasti "oikeudellisia toimia" (liitteessä 8 oleva 7 kohta) ja "petosten ehkäisemistä" (liitteessä 8 oleva 8 kohta) koskevien edellytysten soveltamiseen on olemassa rajoituksia. Molempia ehtoja voidaan soveltaa vain tiettyihin rekisterinpitäjiin. Oikeudellisia toimia koskevaa edellytystä voi soveltaa ainoastaan tuomioistuin tai muu oikeusviranomainen, ja petostentorjuntaa koskevaa edellytystä voivat soveltaa ainoastaan rekisterinpitäjät, jotka ovat petostentorjuntaorganisaatioita.

(42) Kun käsittely perustuu johonkin liitteessä 8 luetelluista edellytyksistä ja vuoden 2018 tietosuojalain 42 §:ssä edellytetään, että käytössä on "asianmukainen toimintapoliittinen asiakirja" – jossa selitetään, miten rekisterinpitäjän on meneteltävä varmistaakseen tietosuojaperiaatteiden noudattamisen, ja mitkä ovat henkilötietojen säilyttämistä ja poistamista koskevat rekisterinpitäjän toimintaperiaatteet – ja sovelletaan laajennettuja kirjan pitämistä koskevia velvoitteita.

2.4.2 *Käyttötarkoituksen rajaaminen*

(43) Henkilötietoja olisi käsiteltävä tiettyä tarkoitusta varten ja käytettävä myöhemmin vain siltä osin, kuin se ei ole ristiriidassa kyseisen tarkoituksen kanssa. Tämä tietosuojaperiaate taataan vuoden 2018 tietosuojalain 36 §:ssä. Tässä säännöksessä ja direktiivin (EU) 2016/680 4 artiklan 1 kohdan b alakohdassa edellytetään, että a) lainvalvonta-tarkoituksen, jota varten henkilötietoja kerätään, on aina oltava tietty, nimenomainen ja laillinen, ja b) näin kerättyjä henkilötietoja ei saa käsitellä tavalla, joka on yhteensopimaton sen tarkoituksen kanssa, jota varten ne on kerätty.

(44) Kun toimivaltaiset viranomaiset käsittelevät tietoja lainvalvontatarkoituksessa, tähän tarkoitukseen voivat kuulua arkistointi, tieteellinen tai historiallinen tutkimus ja tilastointi ([73]). Näissä tapauksissa vuoden 2018 tietosuojalaissa myös selvennetään, että arkistointi (tai käsittely tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten) ei ole sallittua, jos se tehdään tiettyä rekisteröityä koskevien päätösten osalta tai jos se todennäköisesti aiheuttaa hänelle huomattavaa vahinkoa tai kärsimystä ([74]).

2.4.3 *Täsmällisyys ja tietojen minimointi*

(45) Tietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Tietojen on oltava myös asianmukaisia ja olennaisia, eivätkä ne saa olla liian laajoja siihen tarkoitukseen nähden, jota varten niitä käsitellään. Direktiivin (EU) 2016/680 4 artiklan 1 kohdan c, d ja e alakohdan tavoin nämä periaatteet on varmistettu vuoden 2018 tietosuojalain 37 ja 38 §:ssä. On toteutettava kaikki kohtuulliset toimenpiteet sen varmistamiseksi, että virheelliset ([75]) henkilötiedot

([71]) Henkilötietojen käsittelyä lainvalvonnassa koskevat ohjeet, "Arkaluontoisen käsittelyn edellytykset" (ks. alaviite 70).

([72]) Käsittely suoritetaan ilman rekisteröidyn suostumusta, kun a) rekisteröity ei voi antaa suostumustaan käsittelyyn, b) ei voida kohtuudella odottaa, että rekisterinpitäjä hankkii rekisteröidyn suostumuksen käsittelyyn, c) käsittely on suoritettava ilman rekisteröidyn suostumusta, koska rekisteröidyn suostumuksen hankkiminen haittaisi 1 kohdan a alakohdassa tarkoitetun suojan tarjoamista.

([73]) Ks. vuoden 2018 tietosuojalain 41 §:n 1 momentti.

([74]) Ks. vuoden 2018 tietosuojalain 41 §:n 2 momentti.

([75]) Vuoden 2018 tietosuojalain 205 §:ssä olevan määritelmän mukaan termi "virheellinen" (inaccurate) tarkoittaa, että henkilötiedot ovat "virheellisiä tai harhaanjohtavia" (incorrect tai misleading). Yhdistyneen kuningaskunnan viranomaiset ovat selittäneet olevan tyypillistä, että rikostutkintaan liittyvät tiedot ovat usein epätäydellisiä, mutta että ne voivat silti olla paikkansapitäviä.

poistetaan tai oikaistaan viipymättä ([76]) käsittelyn ([77]) lainvalvontatarkoitus huomioiden, ja sen varmistamiseksi, että virheellisiä, puutteellisia tai vanhentuneita henkilötietoja ei siirretä tai aseteta saataville mitään lainvalvontatarkoitusta varten ([78]).

(46) Lisäksi Yhdistyneen kuningaskunnan tietosuojajärjestelmässä täsmennetään direktiivin (EU) 2016/680 7 artiklan tavoin, että tosiseikkoihin perustuvat henkilötiedot on mahdollisuuksien mukaan erotettava henkilökohtaisiin arvioihin perustuvista henkilötiedoista ([79]). Tarvittaessa ja mahdollisuuksien mukaan on erotettava selvästi toisistaan henkilötiedot, jotka koskevat eri ryhmiin kuuluvia rekisteröityjä, kuten epäiltyjä, rikoksesta tuomittuja henkilöitä, rikoksen uhreja ja todistajia ([80]).

2.4.4 *Säilyttämistä koskevat rajoitukset*

(47) Direktiivin (EU) 2016/680 5 artiklan mukaan tietoja olisi periaatteessa säilytettävä vain niin kauan, kuin on tarpeen niitä tarkoituksia varten, joita varten henkilötietoja käsitellään. Vuoden 2018 tietosuojalain 39 §:n ja samoin kuin mainitun direktiivin 5 artiklan mukaan henkilötietoja ei saa säilyttää mitään lainvalvontatarkoitusta varten pidempään, kuin on tarpeen sen tarkoituksen kannalta, jota varten niitä käsitellään. Yhdistyneen kuningaskunnan oikeudellisessa järjestelmässä edellytetään, että on vahvistettava asianmukaiset määräajat, joiden puitteissa tarkastellaan säännöllisesti uudelleen henkilötietojen säilyttämisen jatkamisen tarpeellisuutta lainvalvontatarkoituksia varten. Henkilötietojen säilyttämiseen liittyviä käytäntöjä ja sovellettavia määräaikoja koskevia lisäsääntöjä on vahvistettu asiaa koskevassa lainsäädännössä ja poliisin toimivaltuuksia ja toimintaa koskevissa ohjeissa. Esimerkiksi Englannissa ja Walesissa poliisiakatemian antama poliisin hallussa olevien tietojen hallintaa koskeva ohjesääntö yhdessä poliisin hallussa olevien tietojen hallintaa koskevien poliisin sisäisten ohjeiden kanssa muodostavat kehyksen, jolla varmistetaan johdonmukainen riskiperusteinen säilyttämis-, tarkistus- ja loppukäsittelyprosessi poliisin hallussa olevan operatiivisen tiedon hallinnointia varten ([81]). Tässä kehyksessä asetetaan kaikille yksiköille selkeät vaatimukset sille, miten tietoja olisi luotava, jaettava, käytettävä ja hallinnoitava yksittäisten poliisivoimien ja muiden virastojen sisällä ja niiden välillä ([82]). Poliisin odotetaan noudattavan ohjesääntöä, ja sen noudattamista valvoo Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ([83]).

(48) Pohjois-Irlannin poliisiviraston ei lain mukaan tarvitse noudattaa poliisin hallussa olevien tietojen hallintaa koskevaa ohjesääntöä. Vuonna 2011 hyväksyttyjä poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön puitteita täydennetään kuitenkin Pohjois-Irlannin poliisiviraston käsikirjalla ([84]), jossa esitetään toimintaperiaatteet ja menettelyt, kun poliisin hallussa olevien tietojen hallintaa koskevaa ohjesääntöä sovelletaan Pohjois-Irlannissa.

([76]) Vuoden 2018 tietosuojalain 38 §:n 1 momentin b kohta.

([77]) Yhdistyneen kuningaskunnan perustelut tietosuojan riittävyyttä koskevalle keskustelulle: "Näin varmistetaan, että sekä rekisteröityjen oikeudet että lainvalvontaviranomaisten operatiiviset tarpeet tunnustetaan. Edellä mainittua näkökohtaa tarkasteltiin huolellisesti tietosuojalakia laadittaessa, koska voi olla erityisiä ja rajallisia operatiivisia syitä, joiden vuoksi tietoja ei voida oikaista. Todennäköisimmin näin on silloin kun kyseessä olevat virheelliset henkilötiedot on säilytettävä alkuperäisessä muodossaan todistelua varten" (ks. UK Explanatory Framework for Adequacy Discussions, F jakso: Law Enforcement, s. 21, ks. alaviite 9).

([78]) Vuoden 2018 tietosuojalain 38 §:n 4 momentti. Lisäksi vuoden 2018 tietosuojalain 38 §:n 5 momentin mukaan kaikissa henkilötietojen siirroissa henkilötietojen laatu on tarkistettava ennen niiden siirtämistä tai asettamista saataville. Niihin on myös liitettävä tarpeelliset tiedot, joiden avulla vastaanottaja voi arvioida tietojen oikeellisuuden, täydellisyyden ja luotettavuuden sekä sen, missä määrin ne ovat ajan tasalla. Lisäksi jos henkilötietojen toimittamisen jälkeen ilmenee, että tiedot olivat virheellisiä tai että ne olivat lainvastaisia, vastaanottajalle on viipymättä ilmoitettava asiasta.

([79]) Vuoden 2018 tietosuojalain 38 §:n 2 momentti.

([80]) Vuoden 2018 tietosuojalain 38 §:n 3 momentti.

([81]) Näillä puitteilla varmistetaan hankittujen henkilötietojen yhdenmukainen säilyttäminen. Tarkastelujakso riippuu rikoksista, jotka on jaettu neljään ryhmään: 1) tietyt yleiseen suojeluun liittyvät asiat, 2) muut seksuaaliset väkivaltarikokset ja vakavat rikokset, 3) kaikki muut rikokset, 4) sekalaiset. Lisätietoja on saatavilla poliisin hallussa olevien tietojen hallintaa koskevissa poliisin sisäisissä ohjeissa (ks. alaviite 26).

([82]) Yhdistyneen kuningaskunnan viranomaisten toimittamien tietojen mukaan muut organisaatiot voivat vapaasti niin halutessaan noudattaa poliisin hallussa olevien tietojen hallintaa koskevaa ohjesääntöä, ja esimerkiksi vero- ja tullivirasto ja kansallinen rikosvirasto ovat vapaaehtoisesti hyväksyneet monia poliisin hallussa olevien tietojen hallintaa koskevan ohjesäännön periaatteita lainvalvonnan johdonmukaisuuden varmistamiseksi. Yleisesti useimmat organisaatiot antavat henkilöstölleen erityisiä toimintaohjeita ja opastusta siitä, miten henkilötietoja käsitellään osana henkilöstön tehtäviä ja mukautettuna kyseisen organisaation tarpeisiin. Tähän sisältyy yleensä myös pakollinen koulutus.

([83]) Poliisin hallussa olevien tietojen hallintaa koskeva ohjesääntö annettiin käyttäen vuoden 1996 poliisilain mukaisia valtuuksia, joiden nojalla poliisiakatemia voi antaa poliisin tehokkaaseen toimintaan liittyviä käytännesääntöjä. Poliisilain nojalla annettavilla ohjesäännöillä on oltava Secretary of Staten hyväksyntä, ja ne edellyttävät kansallisen rikosviraston kuulemista ennen kuin ne esitetään parlamentille. Vuoden 1996 poliisilain 39A §:n 7 momentissa edellytetään, että poliisi ottaa asianmukaisesti huomioon mainitun lain nojalla annetut säännöt.

([84]) Pohjois-Irlannin poliisiviraston poliisin hallussa olevien tietojen hallintaa koskevasta ohjesäännöstä annettu käsikirja (PSNI MOPI Handbook), luku 1–6.

(49) Skotlannin poliisivoimat tukeutuvat tietojen säilyttämistä koskevaan menettelyohjeeseen (Record Retention Standard Operating Procedure) ([85]), jossa vahvistetaan Skotlannin poliisiviraston tiedonhallinnan toimintalinjoja (Records Management Policy) ([86]). Menettelyohjeessa vahvistetaan erityiset Skotlannin poliisin hallussa olevien tietojen säilyttämistä koskevat säännöt.

(50) Sen lisäksi, että koko Yhdistyneessä kuningaskunnassa sovelletaan yleistä vaatimusta tarkistaa tietoja, paikallisissa säännöissä asetetaan yksityiskohtaisempia vaatimuksia. Esimerkiksi Englannin ja Walesin osalta poliisista ja rikosasioiden todistusaineistosta annetussa laissa, sellaisena kuin se on muutettuna vuonna 2012 vapauksien suojelusta annetulla lailla, säädetään sormenjälkien ja DNA-tunnisteiden säilyttämisestä sekä erityisestä järjestelmästä, jota sovelletaan henkilöihin, joita ei ole tuomittu ([87]). Vapauksien suojelusta annetulla lailla perustettiin myös biometristen materiaalien säilyttämisestä ja käytöstä vastaavan valtuutetun (Biometrics Commissioner) tehtävä ([88]). Pidätyskuvia koskevat säännöt annettiin vuoden 2017 pidätyskuvia koskevassa määräyksessä (Custody Image Review) ([89]). Skotlannissa vuoden 1995 rikosprosessilaissa säädetään sormenjälkien ja biologisten näytteiden hankkimisesta ja säilyttämisestä ([90]). Kuten Englannissa ja Walesissa, lainsäädännössä säännellään biometristen tietojen säilyttämistä eri tapauksissa ([91]).

2.4.5 *Tietoturva*

(51) Henkilötietoja on käsiteltävä tavalla, jolla varmistetaan niiden turvallisuus, mukaan lukien suojaaminen luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Tätä varten viranomaisten on toteutettava asianmukaisia teknisiä tai organisatorisia toimenpiteitä henkilötietojen suojaamiseksi mahdollisilta uhkilta. Näitä toimenpiteitä on arvioitava ottaen huomioon alan uusin tekniikka ja siihen liittyvät kustannukset.

(52) Nämä periaatteet on otettu huomioon vuoden 2018 tietosuojalain 40 §:ssä, jonka mukaan, samalla tavalla kuin direktiivin (EU) 2016/680 4 artiklan 1 kohdan f alakohdassa säädetään, lainvalvontatarkoituksia varten käsiteltyjä henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen tietoturva, asianmukaisia teknisiä tai organisatorisia toimenpiteitä hyödyntäen. Tähän sisältyy tietojen suojaaminen luvattomalta tai

([85]) Tietojen säilyttämistä koskeva menettelyohje, saatavilla seuraavassa osoitteessa: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) Lisätietoja tietojen hallinnasta on Skotlannin rekisteriviranomaisen (National Records of Scotland) verkkosivuilla seuraavassa osoitteessa: https://www.nrscotland.gov.uk/record-keeping/records-management

([87]) Säilytysajat vaihtelevat sen mukaan, onko henkilö tuomittu (vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annetun lain 63I–63KI §). Esimerkiksi rekisteriin merkittävästä rikoksesta (recordable offence) tuomitun aikuisen sormenjäljet ja DNA-tunnisteet voidaan säilyttää määräämättömän ajan (vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annetun lain 63I §:n 2 momentti), kun taas säilyttämisaika on rajattu, jos tuomittu on alle 18-vuotias, rikos on ”vähäinen” rekisteriin merkittävä rikos eikä henkilöä ole aiemmin tuomittu (lain 63K §). Kun henkilö on ollut pidätettynä tai syytettynä mutta häntä ei ole tuomittu, hänen tietojensa säilyttäminen on rajoitettu kolmeen vuoteen (vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annetun lain 63F §). Tämän säilyttämisajan pidentämiseen on saatava oikeusviranomaisen hyväksyntä (lain 63F §:n 7 momentti). Kun vähäisestä rikoksesta epäilty henkilö on ollut pidätettynä tai syytettynä mutta häntä ei ole tuomittu, tietoja ei saa säilyttää lainkaan (lain 63D § ja 63H §).

([88]) Vuonna 2012 vapauksien suojelusta annetun lain 20 §:ssä perustetaan biometristen materiaalien säilyttämisestä ja käytöstä vastaavan valtuutetun tehtävä. Biometristen materiaalien säilyttämisestä ja käytöstä vastaava valtuutettu päättää muun muassa, saako poliisi säilyttää DNA-tunnisteet ja sormenjäljet, jotka on otettu vakavasta rikoksesta (qualifying offence) epäillyltä henkilöltä, joka on pidätetty mutta jota vastaan ei ole nostettu syytettä (vuonna 1984 poliisista ja rikosasioiden todistusaineistosta annetun lain 63G §). Biometristen materiaalien säilyttämisestä ja käytöstä vastaavalla valtuutetulla on lisäksi yleinen vastuu valvoa DNA:n ja sormenjälkien säilyttämistä ja käyttöä sekä kansalliseen turvallisuuteen liittyvistä syistä tapahtuvaa säilyttämistä (vuonna 2012 poliisista ja rikosasioiden todistusaineistosta annetun lain 20 §:n 2 momentti). Biometristen materiaalien säilyttämisestä ja käytöstä vastaava valtuutettu nimitetään julkisia nimityksiä koskevien hallintosääntöjen nojalla (saatavilla seuraavassa osoitteessa: Governance Code for Public Appointments - GOV.UK (www.gov.uk) ja hänen toimeksiannostaan käy selvästi ilmi, että sisäasiainministeri voi erottaa hänet tehtävistään vain tarkoin määritellyissä olosuhteissa. Tällainen olosuhde voi olla esim. se, että hän on laiminlyönyt tehtäviensä hoidon kolmen kuukauden ajan, rikostuomio tai toimeksiannon ehtojen noudattamatta jättäminen.

([89]) Pidätyskuvien käyttöä ja säilyttämistä koskeva määräys (Review of the Use and Retention of Custody Images), saatavilla seuraavassa osoitteessa: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) Skotlannin vuoden 1995 rikosprosessilain 18 § ja sitä seuraavat pykälät.

([91]) Säilytysajat vaihtelevat sen mukaan, onko henkilö tuomittu (Skotlannin vuoden 1995 rikosprosessilain 18 §:n 3 momentti) tai onko hän alaikäinen. Kun kyse on alaikäisestä henkilöstä, säilytysaika on kolme vuotta lapsen kuulemismenettelyn yhteydessä annetusta tuomiosta (rikosprosessilain 18E §:n 8 momentti). Jos henkilö on ollut pidätettynä, mutta häntä ei ole tuomittu, tietoja ei voida säilyttää (rikosprosessilain 18 §:n 3 momentti), paitsi erityistapauksissa ja riippuen rikoksen vakavuudesta (rikosprosessilain 18A §). Skotlannin biometristen materiaalien säilyttämisestä ja käytöstä vastaavan valtuutetun tehtävä on perustettu vuonna 2020 biometristen materiaalien säilyttämisestä ja käytöstä vastaavasta valtuutetusta annetussa laissa (Scottish Biometrics Commissioner Act 2020, ks. https://www.legislation.gov.uk/asp/2020/8/contents). Valtuutetun tehtävänä on laatia ja tarkistaa (Skotlannin parlamentin hyväksymiä) käytännesääntöjä, jotka koskevat biometristen tietojen hankkimista, säilyttämistä, käyttöä ja tuhoamista rikosoikeudellisia tarkoituksia ja poliisia varten (mainitun lain 7 §).

laittomalta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta ([92]). Vuoden 2018 tietosuojalain 66 §:ssä täsmennetään lisäksi, että kunkin rekisterinpitäjän ja kunkin henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet varmistaakseen henkilötietojen käsittelystä aiheutuviin riskeihin nähden asianmukainen turvallisuustaso. Selittävien huomautusten mukaan rekisterinpitäjän on arvioitava riskit ja toteutettava sen perusteella asianmukaiset turvatoimenpiteet, kuten salaus tai tietoja käsittelevän henkilöstön erityiset turvallisuusselvityksen tasot ([93]). Arvioinnissa on otettava huomioon myös esimerkiksi käsiteltyjen tietojen luonne ja muut merkitykselliset tekijät tai olosuhteet, jotka voivat vaikuttaa käsittelyn turvallisuuteen.

(53) Tietoturvaperiaatteiden noudattamista koskeva järjestelmä on hyvin samankaltainen kuin direktiivin (EU) 2016/680 29–31 artiklalla perustettu järjestelmä. Erityisesti silloin, kun on kyse henkilötietojen tietoturvaloukkauksesta, josta rekisterinpitäjä on vastuussa, rekisterinpitäjän on vuoden 2018 tietosuojalain 67 §:n 1 momentin mukaan ilmoitettava tietoturvaloukkauksesta tietosuojavaltuutetulle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa tietoturvaloukkauksesta ([94]). Ilmoitusvelvollisuutta ei ole, jos henkilötietojen tietoturvaloukkaus ei todennäköisesti aiheuta riskiä yksilöiden oikeuksille ja vapauksille ([95]). Rekisterinpitäjän on dokumentoitava henkilötietojen tietoturvaloukkaukseen liittyvät tosiseikat, sen vaikutukset ja toteutetut korjaavat toimet siten, että tietosuojavaltuutettu voi varmistaa, onko tietosuojalakia noudatettu ([96]). Jos henkilötietojen käsittelijä saa tiedon tietoturvaloukkauksesta, sen on ilmoitettava siitä rekisterinpitäjälle ilman aiheetonta viivytystä ([97]).

(54) Vuoden 2018 tietosuojalain 68 §:n 1 momentissa säädetään, että jos henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin yksilöiden oikeuksille ja vapauksille, rekisterinpitäjän on ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä ([98]). Ilmoituksessa on oltava samat tiedot kuin johdanto-osan 53 kappaleessa selostetussa tietosuojavaltuutetun ilmoituksessa. Tätä velvoitetta ei sovelleta, jos rekisterinpitäjä oli toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet, joita sovellettiin henkilötietoihin, joita tietoturvaloukkaus koskee. Sitä ei sovelleta myöskään, jos rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että rekisteröityjen oikeuksiin ja vapauksiin kohdistuva suuri riski ei enää todennäköisesti toteudu. Rekisterinpitäjän ei myöskään tarvitse ilmoittaa rekisteröidylle, jos ilmoittaminen vaatisi kohtuutonta vaivaa ([99]). Tällöin tiedot on asetettava rekisteröidyn saataville muulla yhtä tehokkaalla tavalla, esimerkiksi julkisella tiedonannolla ([100]). Jos rekisterinpitäjä ei ole ilmoittanut rekisteröidylle tietoturvaloukkauksesta, tietosuojavaltuutettu voi tietosuojalain 67 §:n mukaisen ilmoituksen jälkeen ja arvioituaan, että tietoturvaloukkaus aiheuttaa suuren riskin, vaatia rekisterinpitäjää ilmoittamaan tietoturvaloukkauksesta rekisteröidylle ([101]).

([92]) Vuoden 2018 tietosuojalain selittävien huomautusten mukaisesti (ks. alaviite 45) rekisterinpitäjän on erityisesti suunniteltava ja järjestettävä turvallisuus siten, että se on oikeassa suhteessa hallussa olevien henkilötietojen luonteeseen ja tietoturvaloukkauksesta mahdollisesti aiheutuvaan haittaan; kerrottava selkeästi, kuka organisaatiossa vastaa tietoturvan varmistamisesta; varmistettava, että fyysinen ja tekninen turvallisuus ovat asianmukaisia, ja että niitä tuetaan vankoilla toimintalinjoilla ja menettelyillä sekä luotettavalla ja hyvin koulutetulla henkilöstöllä; ja oltava valmis reagoimaan nopeasti ja tehokkaasti kaikkiin tietoturvaloukkauksiin.

([93]) Vuoden 2018 tietosuojalain selittävien huomautusten 221 kohta (ks. alaviite 45).

([94]) Vuoden 2018 tietosuojalain 67 §:n 4 momentissa säädetään, että ilmoitukseen on sisällyttävä kuvaus henkilötietojen tietoturvaloukkauksen luonteesta (mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä kyseessä olevien henkilötietotietueiden ryhmät ja arvioidut määrät), yhteyspisteen nimi ja yhteystiedot, kuvaus henkilötietojen tietoturvaloukkauksen todennäköisistä seurauksista sekä kuvaus toimenpiteistä, jotka rekisterinpitäjä on toteuttanut tai aikoo toteuttaa henkilötietojen tietoturvaloukkauksen korjaamiseksi (mukaan lukien tarvittaessa toimenpiteet sen mahdollisten haittavaikutusten lieventämiseksi).

([95]) Vuoden 2018 tietosuojalain 67 §:n 2 momentti.

([96]) Vuoden 2018 tietosuojalain 67 §:n 6 momentti.

([97]) Vuoden 2018 tietosuojalain 67 §:n 9 momentti.

([98]) Vuoden 2018 tietosuojalain 68 §:n 7 momentin mukaan rekisterinpitäjä voi rajoittaa kokonaan tai osittain tietojen antamista rekisteröidylle siltä osin ja niin kauan kuin rajoittaminen on rekisteröidyn perusoikeudet ja oikeutetut edut huomioon ottaen välttämätön ja oikeasuhteinen toimenpide a) jotta vältetään estämästä virallisia tai laillisia tiedusteluja, tutkimuksia tai menettelyjä, b) jotta vältetään tuottamasta haittaa rikosten ennalta estämiselle, tutkimiselle ja paljastamiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle, c) yleisen turvallisuuden suojelemiseksi, d) kansallisen turvallisuuden suojelemiseksi, e) muiden henkilöiden oikeuksien ja vapauksien suojaamiseksi.

([99]) Vuoden 2018 tietosuojalain 68 §:n 3 momentti.

([100]) Vuoden 2018 tietosuojalain 68 §:n 5 momentti.

([101]) Vuoden 2018 tietosuojalain 68 §:n 6 momentti (vuoden 2018 tietosuojalain 68 §:n 8 momentissa säädetyin rajoituksin).

2.4.6 *Läpinäkyvyys*

(55) Rekisteröidyille on ilmoitettava heidän henkilötietojensa käsittelyn pääkohdat. Tämä tietosuojaperiaate on otettu huomioon vuoden 2018 tietosuojalain 44 §:ssä, jossa säädetään direktiivin (EU) 2016/680 13 artiklan tavoin, että rekisterinpitäjällä on yleinen velvollisuus antaa rekisteröityjen saataville tiedot heidän henkilötietojensa käsittelystä (joko asettamalla tiedot yleisesti yleisön saataville tai muulla tavoin) ([102]). Saataville asetettaviin tietoihin kuuluvat a) rekisterinpitäjän henkilöllisyys ja yhteystiedot, b) tapauksen mukaan tietosuojavastaavan yhteystiedot, c) tarkoitukset, joita varten rekisterinpitäjä käsittelee henkilötietoja, d) tieto siitä, että rekisteröidyillä on oikeus pyytää rekisterinpitäjältä pääsy henkilötietoihin sekä oikeus pyytää henkilötietojen oikaisemista tai poistamista tai henkilötietojen käsittelyn rajoittamista, ja e) tieto oikeudesta tehdä valitus tietosuojavaltuutetulle ja tietosuojavaltuutetun yhteystiedot ([103]).

(56) Rekisterinpitäjän on myös sellaisissa erityistapauksissa, joissa mahdollistetaan vuoden 2018 tietosuojalain mukaisten rekisteröidyn oikeuksien käyttäminen (esimerkiksi kun käsiteltävät henkilötiedot on kerätty rekisteröidyn tietämättä), annettava rekisteröidylle seuraavat tiedot: a) käsittelyn oikeusperusta, b) henkilötietojen säilytysaika tai, jos se ei ole mahdollista, tämän ajan määrittämiskriteerit, c) tarvittaessa tiedot henkilötietojen vastaanottajien ryhmistä (myös kolmansissa maissa tai kansainvälisissä järjestöissä olevista vastaanottajista), d) lisätiedot, jotka ovat rekisteröidylle tarpeen vuoden 2018 tietosuojalain 3 osan ([104]) mukaisten oikeuksien käyttämiseksi.

2.4.7 *Yksilön oikeudet*

(57) Rekisteröidyillä on oltava tiettyjä täytäntöönpanokelpoisia oikeuksia. Vuoden 2018 tietosuojalain 3 osan 3 luvussa annetaan yksilöille oikeus saada pääsy henkilötietoihin, oikaista ja poistaa niitä sekä rajoittaa niiden käyttöä ([105]). Nämä oikeudet ovat verrattavissa direktiivin (EU) 2016/680 3 luvussa säädettyihin oikeuksiin.

(58) Oikeudesta saada pääsy tietoihin säädetään vuoden 2018 tietosuojalain 45 §:ssä. Yksilöllä on oikeus saada rekisterinpitäjältä vahvistus siitä, käsitelläänkö hänen henkilötietojaan vai ei ([106]). Kun henkilötietoja käsitellään, rekisteröidyllä on myös oikeus saada pääsy kyseisiin tietoihin ja vastaanottaa seuraavat tiedot käsittelystä: a) käsittelyn tarkoitukset ja oikeusperustat, b) kyseessä olevat tietoryhmät, c) vastaanottaja, jolle tiedot on luovutettu, d) henkilötietojen säilytysaika, e) rekisteröidyn oikeus henkilötietojen oikaisemiseen ja poistamiseen, f) oikeus tehdä valitus ja g) mahdolliset tiedot kyseisten henkilötietojen alkuperästä ([107]).

(59) Vuoden 2018 tietosuojalain 46 §:n mukaan rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan häntä koskevat virheelliset henkilötiedot. Rekisterinpitäjän on oikaistava (tai jos tiedot ovat virheellisiä siksi, että ne ovat puutteellisia, täydennettävä) tiedot ilman aiheetonta viivytystä. Jos henkilötiedot on säilytettävä todistelua varten, rekisterinpitäjän on (henkilötietojen oikaisemisen sijaan) rajoitettava niiden käsittelyä ([108]).

([102]) Henkilötietojen käsittelyä lainvalvonnassa koskevissa ohjeissa annetaan seuraava esimerkki: ”Sivustollasi on yleinen tietosuojaseloste, joka sisältää perustiedot organisaatiosta, henkilötietojen käsittelyn tarkoituksesta, rekisteröidyn oikeuksista ja oikeudesta tehdä valitus tietosuojavaltuutetulle. Olet saanut tietää, että eräs henkilö oli läsnä rikoksen tapahtuessa. Kun henkilöä kuullaan ensimmäisen kerran, hänelle on toimitettava yleiset tiedot ja muut lisätiedot, jotta hän voi käyttää oikeuksiaan. Voit rajoittaa antamiasi asianmukaista käsittelyä koskevia tietoja vain, jos ne vaikuttavat kielteisesti suorittamaasi tutkintaan” (Guide to Law Enforcement Processing,”What information should we supply to an individual?”, saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Henkilötietojen käsittelyä lainvalvonnassa koskevissa ohjeissa todetaan, että henkilötietojen käsittelystä annettavien tietojen on oltava ytimekkäitä, ymmärrettäviä ja helposti saatavilla. Ne on kirjoitettava selkeällä ja yksinkertaisella kielellä, joka on mukautettu haavoittuvassa asemassa olevien henkilöiden, kuten lasten, tarpeisiin. Niiden on oltava myös maksuttomia (Guide to Law Enforcement Processing, ”How should we provide this information?”, saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Vuoden 2018 tietosuojalain 44 §:n 2 momentti.

([105]) Yksityiskohtainen analyysi rekisteröidyn oikeuksista: Guide to Law Enforcement Processing on individual rights, saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Vuoden 2018 tietosuojalain 45 §:n 1 momentti.

([107]) Vuoden 2018 tietosuojalain 45 §:n 2 momentti.

([108]) Vuoden 2018 tietosuojalain 46 §:n 4 momentti.

(60) Vuoden 2018 tietosuojalain 47 §:ssä annetaan yksityishenkilöille oikeus tietojen poistamiseen ja käsittelyn rajoittamiseen. Rekisterinpitäjän on poistettava ([109]) henkilötiedot ilman aiheetonta viivytystä, jos henkilötietojen käsittely rikkoisi tietosuojaperiaatteita, käsittelyn oikeudellisia perusteita tai arkistointia ja arkaluontoista käsittelyä koskevia suojatoimia. Rekisterinpitäjän on myös poistettava tiedot, jos siihen on lakisääteinen velvoite. Jos henkilötiedot on säilytettävä todistelua varten, rekisterinpitäjän on (henkilötietojen poistamisen sijaan) rajoitettava niiden käsittelyä ([110]). Rekisterinpitäjän on rajoitettava henkilötietojen käsittelyä, jos rekisteröity kiistää henkilötietojen paikkansapitävyyden, mutta tietojen oikeellisuutta ei voida varmistaa ([111]).

(61) Jos rekisteröity pyytää henkilötietojen oikaisemista tai poistamista tai niiden käsittelyn rajoittamista, rekisterinpitäjän on ilmoitettava rekisteröidylle kirjallisesti, onko pyyntöön suostuttu. Jos pyyntö on hylätty, sen on ilmoitettava rekisteröidylle kieltäytymisen syyt ja käytettävissä olevat oikeussuojakeinot (rekisteröidyn oikeus pyytää tietosuojavaltuutettua tutkimaan, onko rajoitusta sovellettu lainmukaisesti, oikeus tehdä valitus tietovaltuutetulle ja oikeus vaatia tuomioistuimelta lain noudattamista koskevan määräyksen antamista) ([112]).

(62) Jos rekisterinpitäjä oikaisee toiselta toimivaltaiselta viranomaiselta saatuja henkilötietoja, sen on ilmoitettava asiasta kyseiselle toiselle viranomaiselle ([113]). Jos rekisterinpitäjä oikaisee tai poistaa luovuttamiaan henkilötietoja tai rajoittaa niiden käsittelyä, rekisterinpitäjän on ilmoitettava tästä vastaanottajille, ja vastaanottajien on vastaavasti oikaistava tai poistettava henkilötietoja tai rajoitettava niiden käsittelyä (siltä osin kuin he ovat edelleen vastuussa henkilötietojen käsittelystä) ([114]).

(63) Lisäksi rekisteröidyllä on oikeus saada rekisterinpitäjältä ilman aiheetonta viivytystä tieto henkilötietojen tietoturvaloukkauksesta, jos se todennäköisesti aiheuttaa suuren riskin yksilöiden oikeuksille ja vapauksille ([115]).

(64) Kaikkien näiden rekisteröidyn oikeuksien osalta ja samoin kuin direktiivin (EU) 2016/680 12 artiklassa säädetään, rekisterinpitäjällä on velvollisuus varmistaa, että kaikki rekisteröidylle annettavat tiedot toimitetaan tiiviisti esitetyssä, ymmärrettävässä ja helposti saatavilla olevassa muodossa ([116]) ja mahdollisuuksien mukaan samassa muodossa kuin pyyntö ([117]). Rekisterinpitäjän on noudatettava rekisteröidyn pyyntöä ilman aiheetonta viivytystä tai joka tapauksessa periaatteessa kuukauden kuluessa pyynnön esittämisestä ([118]). Jos rekisterinpitäjällä on perusteltua aihetta epäillä pyytäjän henkilöllisyyttä, hän voi pyytää lisätietoja ja viivyttää pyynnön käsittelyä, kunnes henkilöllisyys on varmistettu. Rekisterinpitäjä voi vaatia kohtuullista maksua tai kieltäytyä toimimasta, jos se katsoo pyynnön ilmeisen perusteettomaksi ([119]). Tietosuojavaltuutettu on antanut ohjeita siitä, milloin pyyntö katsotaan ilmeisen perusteettomaksi tai kohtuuttomaksi ja milloin maksua voidaan vaatia ([120]).

(65) Lisäksi vuoden 2018 tietosuojalain 53 §:n 4 momentin mukaan Secretary of State voi vahvistaa maksun enimmäismäärän asetuksella.

([109]) Rekisteröity voi pyytää rekisterinpitäjää poistamaan henkilötiedot tai rajoittamaan niiden käsittelyä (mutta rekisterinpitäjän velvollisuuksia poistaa tiedot tai rajoittaa niiden käsittelyä sovelletaan riippumatta siitä, onko tällainen pyyntö esitetty vai ei).

([110]) Vuoden 2018 tietosuojalain 46 §:n 4 momentti ja 47 §:n 2 momentti.

([111]) Vuoden 2018 tietosuojalain 47 §:n 3 momentti.

([112]) Vuoden 2018 tietosuojalain 48 §:n 1 momentti.

([113]) Vuoden 2018 tietosuojalain 48 §:n 7 momentti.

([114]) Vuoden 2018 tietosuojalain 48 §:n 9 momentti.

([115]) Vuoden 2018 tietosuojalain 68 §.

([116]) Vuoden 2018 tietosuojalain 52 §:n 1 momentti.

([117]) Vuoden 2018 tietosuojalain 52 §:n 3 momentti.

([118]) Vuoden 2018 tietosuojalain 54 §:ssä määritellään 'sovellettava ajanjakso', jolla tarkoitetaan yhden kuukauden ajanjaksoa tai asetuksissa mahdollisesti määriteltyä pidempää ajanjaksoa, joka alkaa tietystä ajankohdasta (siitä kun rekisterinpitäjä vastaanottaa pyynnön, kun rekisterinpitäjä saa tietosuojalain 52 §:n 4 momentin mukaisen pyynnön yhteydessä pyydetyt tiedot (jos sellaisia on) tai kun (mahdollinen) tietosuojalain 53 §:n mukaisen pyynnön yhteydessä perittävä maksu suoritetaan.

([119]) Vuoden 2018 tietosuojalain 53 §:n 1 momentti.

([120]) Tietosuojavaltuutetun ohjeiden mukaan rekisterinpitäjä voi päättää veloittaa rekisteröidyltä maksun, jos pyyntö on ilmeisen perusteeton tai kohtuuton, mutta rekisterinpitäjä päättää silti vastata siihen. Maksun on oltava kohtuullinen ja sellainen, että se voi toimia kustannusten perusteena. Henkilötietojen käsittelyä lainvalvonnassa koskevat ohjeet ilmeisen perusteettomaksi tai kohtuuttomaksi katsottavien pyyntöjen osalta, saatavilla seuraavassa osoitteessa: 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 Rekisteröidyn oikeuksien rajoitukset ja läpinäkyvyyttä koskevat velvoitteet

(66) Toimivaltainen viranomainen voi tietyissä olosuhteissa rajoittaa rekisteröidyn oikeuksia, kuten oikeutta saada pääsy tietoihin ([121]), saada tieto ([122]), tietää henkilötietojen tietoturvaloukkauksesta ([123]) ja saada tieto siitä, miksi oikaisu- tai poistamispyyntö on hylätty ([124]). Samalla tavalla kuin direktiivin (EU) 2016/680 III luvussa tarkoitetussa järjestelmässä, toimivaltainen viranomainen voi soveltaa rajoitusta vain, jos se on rekisteröidyn perusoikeudet ja oikeutetut edut huomioon ottaen välttämätöntä ja oikeasuhteista, a) jotta vältetään virallisen tai laillisen tiedustelun, tutkimuksen tai menettelyn estäminen b) jotta vältetään tuottamasta haittaa rikosten ennalta estämiselle, tutkimiselle ja paljastamiselle tai rikoksiin liittyville syytetoimille taikka rikosoikeudellisten seuraamusten täytäntöönpanolle, c) yleisen turvallisuuden suojelemiseksi, d) kansallisen turvallisuuden suojelemiseksi, e) muiden henkilöiden oikeuksien ja vapauksien suojaamiseksi.

(67) Tietosuojavaltuutettu on antanut ohjeita näiden rajoitusten soveltamisesta. Rekisterinpitäjien on tehtävä näiden ohjeiden mukaan tapauskohtainen analyysi, jossa otetaan tasapuolisesti huomioon yksilön oikeudet ja tietojen luovuttamisesta aiheutuva haitta. Niiden on erityisesti perusteltava kaikki tarpeellisina ja oikeasuhteisina sovelletut rajoitukset, ja ne voivat rajoittaa sitä, mitä on luovutettu, ainoastaan, jos se haittaisi edellä mainittuja tarkoituksia ([125]).

(68) On myös useita muita toimivaltaisten viranomaisten antamia ohjeita, joissa annetaan yksityiskohtaista tietoa tietosuojalainsäädännön eri näkökohdista, muun muassa rekisteröityjen oikeuksia koskevien rajoitusten soveltamisesta ([126]). Esimerkiksi kansallisen poliisipäälliköiden neuvoston tietosuojakäsikirjassa (Data Protection Manual of the National Police Chief's Counsel) todetaan 45 §:n 4 momentin osalta seuraavaa: ”On tärkeää huomata, että rajoituksia voidaan soveltaa vain siinä määrin ja niin kauan, kuin on tarpeen. Näin ollen rajoituksen yleinen soveltaminen kaikkiin hakijan henkilötietoihin tai rajoituksen pysyvä soveltaminen ei ole sallittua. Viimeksi mainitun seikan osalta on usein niin, että henkilötiedot, jotka on kerätty tutkinnan kohteena olevan rekisteröidyn tietämättä, on ensin suojattava paljastamiselta hänelle, jotta ei aiheuteta haittaa tutkinnalle sen aikana, mutta myöhemmin tietojen ilmaiseminen ei olisi vahingollista, jos henkilötiedot olisi luovutettu henkilölle puhuttelun aikana. Poliisivoimien on otettava käyttöön menettelyt, joilla varmistetaan, että näiden rajoitusten soveltaminen on välttämätöntä ja kestää vain tarvittavan ajan.” ([127]) Näissä ohjeissa annetaan myös esimerkkejä siitä, milloin kutakin rajoitusta todennäköisesti sovelletaan ([128]).

(69) Lisäksi voidaan todeta mahdollisuudesta rajoittaa näiden edellä mainittujen oikeuksien soveltamista ”kansallisen turvallisuuden” suojelemiseksi, että rekisterinpitäjä voi pyytää kabinettiministerin tai oikeuskanslerin (Attorney General) (tai Skotlannin oikeuskanslerin) allekirjoittamaa todistusta siitä, että tällaisten oikeuksien rajoittaminen on välttämätön ja oikeasuhteinen toimenpide kansallisen turvallisuuden suojelemiseksi ([129]). Yhdistyneen kuningaskunnan hallitus on antanut ohjeita kansallista turvallisuutta koskevan todistuksen osalta vuoden 2018 tietosuojalain nojalla. Ohjeissa korostetaan erityisesti, että kaikkien kansalliseen turvallisuuteen liittyvien rekisteröityjen oikeuksien rajoitusten on oltava oikeasuhteisia ja välttämättömiä ([130]) (ks. lisätietoja kansallista turvallisuutta koskevasta todistuksesta johdanto-osan 131–134 kappale).

([121]) Vuoden 2018 tietosuojalain 45 §:n 4 momentti.
([122]) Vuoden 2018 tietosuojalain 44 §:n 4 momentti.
([123]) Vuoden 2018 tietosuojalain 68 §:n 7 momentti.
([124]) Vuoden 2018 tietosuojalain 48 §:n 3 momentti.
([125]) Ks. esimerkiksi henkilötietojen käsittelyä lainvalvonnassa koskevat ohjeet sen osalta, miten yksilöllä on oikeus saada pääsy tietoihin, saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) Ks. esim. Data Protection Manual for Police Data Protection Professional issued by the National Police Chief Counsel (ks. alaviite 27) tai törkeiden petosten torjuntaviraston ohjeet, saatavilla seuraavassa osoitteessa: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) Data protection Manual of the National Police Chief Counsel, s. 140 (ks. alaviite 27).
([128]) Em. tietosuojakäsikirjan mukaan ”virallisen tai laillisen tiedustelun, tutkimuksen tai menettelyn” estämisen välttämisellä on todennäköisesti merkitystä henkilötietojen käsittelylle, kun kyse on tutkinnasta, perheoikeudenkäynneistä, muista kuin rikosoikeudellisista sisäisistä kurinpitomenettelyistä ja sellaisista tutkinnoista kuin lapsen seksuaalista hyväksikäyttöä koskevasta riippumattomasta tutkinnasta. Sen sijaan ”muiden henkilöiden oikeuksien ja vapauksien” suojaaminen liittyy henkilötietoihin, jotka koskisivat myös muita henkilöitä ja hakijaa (Data protection Manual of the National Police Chief Counsel, s. 140, ks. alaviite 27).
([129]) Vuoden 2018 tietosuojalain 79 §.
([130]) UK Government Guidance on National Security Certificates, saatavilla seuraavassa osoitteessa: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

(70) Lisäksi jos rekisteröidyn oikeuksia rajoitetaan, toimivaltaisen viranomaisen on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä oikeuksien rajoittamisesta, rajoituksen syistä ja käytettävissä olevista oikeussuojakeinoista, paitsi jos näiden tietojen antaminen heikentäisi sitä perustetta, jolla rajoitusta sovelletaan ([131]). Rajoitusten väärinkäyttöä estävänä ylimääräisenä suojatoimena rekisterinpitäjän on kirjattava syyt tietojen rajoittamiseen ja annettava tiedot pyydettäessä tietosuojavaltuutetun käyttöön ([132]).

(71) Jos rekisterinpitäjä kieltäytyy antamasta läpinäkyvyyteen liittyviä lisätietoja tai antamasta pääsyn tietoihin taikka hylkää oikaisua, poistamista tai käsittelyn rajoittamista koskevan pyynnön, henkilö voi pyytää tietosuojavaltuutettua tutkimaan, onko rekisterinpitäjä käyttänyt rajoitusta lainmukaisesti ([133]). Asianomainen henkilö voi myös tehdä valituksen tietosuojavaltuutetulle tai pyytää tuomioistuinta määräämään rekisterinpitäjän noudattamaan pyyntöä ([134]).

2.4.7.2 Automatisoidut päätökset

(72) Vuoden 2018 tietosuojalain 49 ja 50 § kattavat automatisoituun päätöksentekoon liittyvät oikeudet ja sovellettavat suojatoimet ([135]). Rekisterinpitäjä voi tehdä merkittävän päätöksen, joka perustuu pelkästään henkilötietojen automatisoituun käsittelyyn, jos sitä edellytetään tai se sallitaan laissa, kuten myös direktiivin (EU) 2016/680 11 artiklassa säädetään ([136]). Päätös on merkittävä, jos sillä olisi rekisteröityä koskevia kielteisiä oikeusvaikutuksia tai jos se vaikuttaisi merkittävästi rekisteröityyn ([137]).

(73) Jos rekisterinpitäjän on lain mukaan tehtävä merkittävä päätös tai sillä on lupa tehdä merkittävä päätös, vuoden 2018 tietosuojalain 50 §:ssä säädetään suojatoimista, joita sovelletaan tällaiseen päätökseen (joka määritellään ”vaatimukset täyttäväksi merkittäväksi päätökseksi”). Rekisterinpitäjän on mahdollisimman pian ilmoitettava rekisteröidylle, että tällainen päätös on tehty. Rekisteröity voi kuukauden kuluessa pyytää rekisterinpitäjää harkitsemaan päätöstä uudelleen tai tekemään uuden päätöksen, joka ei perustu pelkästään automatisoituun käsittelyyn. Rekisterinpitäjän on tarkasteltava pyyntöä ja ilmoitettava rekisteröidylle käsittelyn tuloksesta. Vuoden 2018 tietosuojalaissa annetaan Secretary of Statelle valtuudet antaa asetuksia täydentävistä suojatoimista ([138]). Tällaisia asetuksia ei ole vielä annettu.

2.4.8 *Tietojen siirtäminen edelleen*

(74) Jäsenvaltion lainvalvontaviranomaiselta Yhdistyneen kuningaskunnan lainvalvontaviranomaiselle siirrettyjen henkilötietojen suojan tasoa ei saa heikentää, kun näitä tietoja siirretään edelleen kolmannessa maassa sijaitseville vastaanottajille. Tällaiset ”jatkosiirrot”, jotka Yhdistyneen kuningaskunnan lainvalvontaviranomaisen näkökulmasta ovat luonteeltaan Yhdistyneestä kuningaskunnasta tapahtuvia kansainvälisiä siirtoja, olisi sallittava vain siinä tapauksessa, että kyseiseen Yhdistyneen kuningaskunnan ulkopuolella toimivaan vastaanottajaan sovelletaan sääntöjä, joilla varmistetaan, että suojelun taso vastaa Yhdistyneen kuningaskunnan oikeusjärjestyksessä taattua suojelun tasoa.

([131]) Vuoden 2018 tietosuojalain 44 §:n 5 ja 6 momentti, 45 §:n 5 ja 6 momentti ja 48 §:n 4 momentti.
([132]) Vuoden 2018 tietosuojalain 44 §:n 7 momentti, 45 §:n 7 momentti ja 48 §:n 6 momentti.
([133]) Vuoden 2018 tietosuojalain 51 §.
([134]) Vuoden 2018 tietosuojalain 167 §.
([135]) Vuoden 2018 tietosuojalain selittävissä huomautuksissa todetaan automatisoidun käsittelyn soveltamisalasta seuraavaa: ”Nämä säännökset liittyvät täysin automatisoituun päätöksentekoon, mutta eivät automatisoituun käsittelyyn. Automatisoitu käsittely (profilointi mukaan luettuna) tarkoittaa, että tietoja käsitellään ilman ihmisen työpanosta. Sitä käytetään lainvalvonnassa säännöllisesti suurten tietokokonaisuuksien suodattamiseksi ihmisen hallittavissa oleviin määriin. Automatisoitu päätöksenteko on yksi automatisoidun käsittelyn muoto, ja se edellyttää, että lopullinen päätös tehdään ilman ihmisen puuttumista asiaan.” (Tietosuojalain selittävät huomautukset 204 kohta, ks. alaviite 45).
([136]) Tietosuojalaissa säädetyn suojan lisäksi Yhdistyneen kuningaskunnan oikeudellisessa kehyksessä on muita lainsäädännöllisiä rajoituksia, joita sovelletaan lainvalvontaviranomaisiin ja joilla estetään laittomaan syrjintään johtava automatisoitu käsittely (profilointi mukaan luettuna). Euroopan ihmisoikeussopimukseen sisältyvät oikeudet, myös 14 artiklaan sisältyvä syrjintäkielto, on saatettu osaksi Yhdistyneen kuningaskunnan lainsäädäntöä vuoden 1998 ihmisoikeuslailla. Vuoden 2010 tasa-arvolaissa kielletään vastaavasti syrjimästä henkilöitä, joilla on suojattuja ominaisuuksia (muun muassa sukupuoli, rotu, vammaisuus jne.).
([137]) Vuoden 2018 tietosuojalain 49 §:n 2 momentti.
([138]) Vuoden 2018 tietosuojalain 50 §:n 4 momentti.

(75) Kansainvälisiä siirtoja koskevaa Yhdistyneen kuningaskunnan järjestelmää säännellään vuoden 2018 tietosuojalain 3 osan 5 luvussa ([139]), ja se vastaa direktiivin (EU) 2016/680 V luvussa omaksuttua lähestymistapaa. Jotta henkilötietoja voidaan siirtää kolmanteen maahan, toimivaltaisen viranomaisen on erityisesti täytettävä seuraavat kolme edellytystä: a) siirron on oltava tarpeen lainvalvontatarkoitusta varten; b) siirron on perustuttava i) kolmannen maan osalta tietosuojan riittävyyttä koskevaan asetukseen, ii) jos se ei perustu tietosuojan riittävyyttä koskevaan asetukseen, asianmukaisten suojatoimien olemassaoloon tai iii) jos se ei perustu tietosuojan riittävyyttä koskevaan päätökseen tai asianmukaisiin suojatoimiin, sen on perustuttava erityisiin olosuhteisiin; ja c) siirron vastaanottajan on oltava i) kolmannen maan asiaankuuluva viranomainen (eli toimivaltaista viranomaista vastaava viranomainen); ii) ”asianomainen kansainvälinen järjestö”, esimerkiksi kansainvälinen elin, joka suorittaa tehtäviä, jotka vastaavat mitä tahansa lainvalvontatarkoitusta; tai iii) muu henkilö kuin asiaankuuluva viranomainen, mutta vain jos siirto on ehdottoman välttämätön jonkin lainvalvontatarkoituksen suorittamiseksi; asianomaisen rekisteröidyn perusoikeudet ja -vapaudet eivät syrjäytä yleistä etua, jonka perusteella siirto on tarpeen; henkilötietojen siirtäminen kolmannen maan asianomaiselle viranomaiselle olisi tehotonta tai epätarkoituksenmukaista; ja vastaanottajalle ilmoitetaan tarkoitukset, joita varten tietoja voidaan käsitellä ([140]).

(76) Secretary of State antaa kolmanteen maahan, kolmannen maan alueeseen tai sektoriin tai kansainväliseen järjestöön sovellettavat tietosuojan riittävyyttä koskevat määräykset tai tällaisen maan, alueen, sektorin tai järjestön kuvauksen ([141]). Secretary of Staten on arvioitava, takaako kyseinen alue/ala/organisaatio henkilötietojen suojan riittävän tason. Vuoden 2018 tietosuojalain 74A §:n 4 momentissa täsmennetään, että tätä varten Secretary of Staten on otettava huomioon useita direktiivin (EU) 2016/680 36 artiklassa lueteltujen kaltaisia seikkoja ([142]). Tältä osin vuoden 2018 tietosuojalain 3 osa on siirtymäkauden päättymisestä lähtien ollut ”EU-oikeudesta johdettua sisäistä lainsäädäntöä”, jota Yhdistyneen kuningaskunnan tuomioistuimet tulkitsevat, kuten selitettiin, asiaa koskevan unionin tuomioistuimen sellaisen oikeuskäytännön mukaisesti, joka on annettu ennen Yhdistyneen kuningaskunnan eroa unionista, ja unionin oikeuden yleisten periaatteiden mukaisesti, koska ne olivat voimassa välittömästi ennen siirtymäkauden päättymistä. Tämä sisältää ”olennaisen vastaavuuden” vaatimuksen, jota sovelletaan Yhdistyneen kuningaskunnan viranomaisten suorittamiin riittävyysarviointeihin.

(77) Menettelyn osalta asetuksiin sovelletaan vuoden 2018 tietosuojalain 182 §:ssä säädettyjä ”yleisiä” menettelyvaatimuksia. Menettelyn mukaan Secretary of Staten on kuultava tietosuojavaltuutettua ennen tietosuojan riittävyyttä

([139]) Tämä uusi järjestelmä otettiin käyttöön siirtymäkauden päättyessä, ja se sisältää Secretary of Statelle annetun toimivallan antaa tietosuojan riittävyyttä koskevia asetuksia. Tietosuojaa, yksityisyydensuojaa ja sähköistä viestintää koskevassa säädöksessä, (erityisesti sen liitteessä 21 olevassa 10–12 kohdassa, joka mainitulla säädöksellä sisällytetään vuoden 2018 tietosuojalakiin) säädetään kuitenkin, että tiettyjä henkilötietojen siirtoja siirtymäkauden päättyessä ja sen jälkeen käsitellään, ikään kuin ne perustuisivat tietosuojan riittävyyttä koskeviin asetuksiin. Näihin siirtoihin kuuluvat siirrot kolmansiin maihin, joista EU on tehnyt tietosuojan riittävyyttä koskevan päätöksen siirtymäkauden päättyessä, sekä EU:n jäsenvaltioihin, EFTA-valtioihin ja Gibraltarin alueeseen, koska ne soveltavat lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annettua direktiiviä lainvalvontatarkoituksessa suoritettavaan tietojen käsittelyyn (EFTA-valtiot soveltavat direktiiviä (EU) 2016/680 Schengenin säännöstöön perustuvien velvoitteidensa vuoksi). Tämä tarkoittaa sitä, että siirtymäkauden päättyessä siirrot näihin maihin voivat jatkua samaan tapaan kuin ennen EU:sta eroamista. Siirtymäkauden päättymisen jälkeen Secretary of Staten on tarkasteltava tietosuojan riittävyyttä uudelleen neljän vuoden kuluessa.

([140]) Vuoden 2018 tietosuojalain 73 ja 77 §.

([141]) Yhdistyneen kuningaskunnan viranomaiset ovat selittäneet, että maan tai kansainvälisen järjestön kuvauksella tarkoitetaan tilannetta, jossa tietosuojan riittävyys olisi tarpeen määritellä erityisellä ja osittaisella tavalla, johon sisältyy kohdennettuja rajoituksia (esimerkiksi niin, että tietosuojan riittävyyttä koskeva asetus koskisi vain tietyntyyppisiä tiedonsiirtoja).

([142]) Ks. vuoden 2018 tietosuojalain 74A §:n 4 momentti, jossa säädetään, että kun arvioidaan tietosuojan riittävyyttä, ”Secretary of Staten on erityisesti otettava huomioon a) oikeusvaltioperiaate, ihmisoikeuksien ja perusvapauksien kunnioitus, sekä yleinen että alakohtainen asiaankuuluva lainsäädäntö, joka koskee muun muassa yleistä turvallisuutta, puolustusta, kansallista turvallisuutta ja rikosoikeutta sekä viranomaisten pääsyä henkilötietoihin, sekä tällaisen lainsäädännön täytäntöönpano, tietosuojaa koskevat säännöt, ammatilliset säännöt ja turvatoimet, mukaan lukien asianomaisessa kolmannessa maassa tai kansainvälisessä järjestössä noudatettavat säännöt henkilötietojen siirtämisestä edelleen muuhun kolmanteen maahan tai muulle kansainväliselle järjestölle, oikeuskäytäntö sekä rekisteröidyille kuuluvat tehokkaat ja täytäntöönpanokelpoiset oikeudet ja tehokkaat hallinnolliset ja oikeudelliset muutoksenhakukeinot niitä rekisteröityjä varten, joiden henkilötietoja siirretään, b) se, onko kyseisessä kolmannessa maassa tai siinä kolmannessa maassa, jonka alaisuuteen kansainvälinen järjestö kuuluu, vähintään yksi tehokkaasti toimiva riippumaton valvontaviranomainen, joka vastaa tietosuojasääntöjen noudattamisen varmistamisesta ja täytäntöönpanosta, kuten riittävistä valvontavaltuuksista, oikeuksien käyttämistä koskevan avun ja neuvojen tarjoamisesta rekisteröidyille sekä yhteistyön tekemisestä tietosuojavaltuutetun kanssa, ja c) kyseisen kolmannen maan tai kansainvälisen järjestön tekemät kansainväliset sitoumukset tai muut oikeudellisesti sitovista yleissopimuksista tai välineistä sekä monenvälisiin tai alueellisiin järjestelmiin osallistumisesta johtuvat velvoitteet, jotka koskevat erityisesti henkilötietojen suojaamista.”

koskevien Yhdistyneen kuningaskunnan tulevien asetusten ehdottamista ([143]). Kun Secretary of State on hyväksynyt asetukset, ne toimitetaan parlamenttiin sekä ylä- että alahuoneen käsiteltäväksi ns. negatiivisessa päätöslauselmamenettelyssä (negative resolution procedure). Tämä tarkoittaa, että asetus tulee voimaan, jollei kummallekaan kamarille esitetä vaatimusta sen hylkäämisestä 40 päivän kuluessa ([144]).

(78) Vuoden 2018 tietosuojalain 74B §:n 1 momentin mukaan tietosuojan riittävyyttä koskevia asetuksia on tarkasteltava uudelleen enintään neljän vuoden välein, ja Secretary of Staten on jatkuvasti seurattava kolmansissa maissa ja kansainvälisissä järjestöissä tapahtuvaa kehitystä, joka voisi vaikuttaa päätökseen tehdä tällaisia asetuksia tai niiden muuttamiseen tai kumoamiseen. Jos Secretary of State saa tietoonsa, että jokin maa tai järjestö ei enää takaa henkilötietojen riittävää tietosuojaa, hänen on tarvittaessa muutettava asetuksia tai kumottava ne ja aloitettava kyseisen kolmannen maan tai kansainvälisen järjestön kanssa neuvottelut tietosuojaan liittyvien puutteiden korjaamiseksi.

(79) Samoin kuin direktiivin (EU) 2016/680 37 artiklassa säädetään, tietosuojan riittävyyttä koskevan asetuksen puuttuessa henkilötietojen siirto lainvalvonta-alalla olisi mahdollista, kun asianmukaiset suojatoimet on toteutettu. Tällaiset suojatoimet varmistetaan joko a) oikeudellisesti sitovalla välineellä, joka sisältää asianmukaiset suojatoimet henkilötietojen suojaamiseksi tai b) rekisterinpitäjän suorittamalla arvioinnilla, jossa se kaikki siirtoon liittyvät olosuhteet arvioituaan päätyy siihen, että henkilötietojen suojaamiseksi on olemassa asianmukaiset suojatoimet ([145]). Lisäksi kun siirrot perustuvat asianmukaisiin suojatoimiin, vuoden 2018 tietosuojalaissa säädetään, että tietosuojavaltuutetun tavanomaisen valvontatehtävän lisäksi toimivaltaisten viranomaisten on annettava tarkat tiedot siirroista tietosuojavaltuutetulle ([146]).

(80) Jos siirto ei perustu tietosuojan riittävyyttä koskevaan päätökseen tai asianmukaisiin suojatoimiin, se voidaan toteuttaa vain tietyissä olosuhteissa, joista käytetään nimitystä ”erityiset olosuhteet” ([147]). Näin on silloin, kun siirto on tarpeen a) rekisteröidyn tai toisen henkilön elintärkeiden etujen suojaamiseksi; b) rekisteröidyn oikeutettujen etujen turvaamiseksi; c) kolmannen maan yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhan ehkäisemiseksi; d) yksittäistapauksissa jotakin lainvalvontatarkoitusta varten; tai e) yksittäistapauksissa jotakin oikeudellista tarkoitusta varten (esimerkiksi oikeudenkäyntiä tai oikeudellisen neuvonnan saamista varten) ([148]). Todettakoon, että d ja e alakohtaa ei sovelleta, jos rekisteröidyn oikeudet ja vapaudet syrjäyttävät siirtoon liittyvän yleisen edun ([149]). Nämä olosuhteet vastaavat niitä erityistilanteita ja -edellytyksiä, joita voidaan pitää direktiivin (EU) 2016/680 38 artiklassa tarkoitettuina ”poikkeuksina”.

(81) Näissä olosuhteissa siirron päivämäärä, kellonaika ja perustelut, vastaanottajan nimi ja muut merkitykselliset tiedot sekä siirrettyjen henkilötietojen kuvaus on dokumentoitava ja toimitettava pyynnöstä tietosuojavaltuutetulle ([150]).

(82) Vuoden 2018 tietosuojalain 78 §:ssä säädetään myöhemmistä siirroista eli tilanteesta, jossa Yhdistyneestä kuningaskunnasta kolmanteen maahan siirretyt henkilötiedot siirretään myöhemmin toiseen kolmanteen maahan tai kansainväliselle järjestölle. Lain 78 §:n 1 momentin mukaan Yhdistyneen kuningaskunnan siirtävän rekisterinpitäjän on asetettava siirron ehdoksi, että tietoja ei siirretä edelleen kolmanteen maahan ilman siirtävän rekisterinpitäjän lupaa. Lisäksi 78 §:n 3 momentin mukaan ja samoin kuin direktiivin (EU) 2016/680 35 artiklan 1

([143]) Ks. Memorandum of Understanding between the Secretary of State for the Department for Digital, Culture, Media and Sport and the Information's Commissioner's Office on the role of the ICO in relation to new United Kingdom adequacy assessment, saatavilla seuraavassa osoitteessa https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Tämän 40 päivän jakson aikana parlamentin kummallakin kamarilla on halutessaan mahdollisuus äänestää sääntöjä vastaan ja jos vaatimus asetuksen hylkäämisestä menee läpi äänestyksessä, asetuksella ei ole viime kädessä lainkaan oikeusvaikutuksia.

([145]) Vuoden 2018 tietosuojalain 75 §.

([146]) Vuoden 2018 tietosuojalain 75 §:n 3 momentissa säädetään, että kun tietojen siirto tapahtuu asianmukaisten suojatoimien avulla, a) siirto on dokumentoitava, b) asiakirjat on toimitettava tietosuojavaltuutetulle pyynnöstä ja c) asiakirjoissa on oltava erityisesti i) siirron päivämäärä ja kellonaika, ii) vastaanottajan nimi ja muut asiaankuuluvat tiedot, iii) siirron perustelut ja iv) siirrettyjen henkilötietojen kuvaus.

([147]) Henkilötietojen käsittelyä lainvalvonnassa koskevat ohjeet erityisten olosuhteiden osalta, saatavilla seuraavassa osoitteessa: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Vuoden 2018 tietosuojalain 76 §.

([149]) Vuoden 2018 tietosuojalain 76 §.

([150]) Vuoden 2018 tietosuojalain 76 §:n 3 momentti.

kohdan e alakohdassa säädetään, jos tällainen lupa vaaditaan, sovelletaan useita aineellisia vaatimuksia. Tarkemmin sanottuna toimivaltaisen viranomaisen on siirron hyväksymisestä päättäessään varmistettava, että siirto on tarpeen lainvalvontatarkoituksessa, ja otettava huomioon muun muassa a) lupapyyntöön johtaneiden olosuhteiden vakavuus, b) tarkoitus, jota varten henkilötiedot alun perin siirrettiin, ja c) henkilötietojen suojaa koskevat vaatimukset, joita sovelletaan siinä kolmannessa maassa tai kansainvälisessä järjestössä, johon henkilötiedot siirrettäisiin.

(83) Lisäksi silloin, kun Yhdistyneestä kuningaskunnasta edelleen siirrettävät tiedot oli alun perin siirretty Euroopan unionista, sovelletaan ylimääräisiä suojatoimia.

(84) Ensinnäkin vuoden 2018 tietosuojalain 73 §:n 1 momentin b kohdassa – samoin kuin direktiivin (EU) 2016/680 35 artiklan 1 kohdan c alakohdassa – säädetään, että jos jäsenvaltio on alun perin siirtänyt henkilötiedot rekisterinpitäjälle tai muulle toimivaltaiselle viranomaiselle tai asettanut ne muutoin rekisterinpitäjälle tai muulle toimivaltaiselle viranomaiselle, kyseisen jäsenvaltion tai tähän jäsenvaltioon sijoittautuneen henkilön, joka on direktiivissä (EU) 2016/680 tarkoitettu toimivaltainen viranomainen, jäsenvaltion lainsäädännön mukaisesti siirtoon antama lupa on edellytyksenä.

(85) Samoin kuin direktiivin (EU) 2016/680 35 artiklan 2 kohdassa säädetään, tällaista lupaa ei kuitenkaan vaadita, jos a) siirto on tarpeen joko jäsenvaltion tai kolmannen maan yleiseen turvallisuuteen tai jäsenvaltion olennaisiin etuihin kohdistuvan välittömän ja vakavan uhan estämiseksi ja b) lupaa ei voida saada ajoissa. Tässä tapauksessa sen jäsenvaltion viranomaiselle, joka olisi ollut vastuussa siirron hyväksymisestä, on ilmoitettava asiasta viipymättä ([151]).

(86) Toiseksi samaa lähestymistapaa sovelletaan silloin, kun tiedot on alun perin siirretty Euroopan unionista Yhdistyneeseen kuningaskuntaan, minkä jälkeen Yhdistynyt kuningaskunta on siirtänyt ne edelleen kolmanteen maahan, joka myöhemmin siirtää ne edelleen kolmanteen maahan. Tässä tapauksessa Yhdistyneen kuningaskunnan toimivaltainen viranomainen ei voi 78 §:n 4 momentin nojalla antaa lupaa jälkimmäiselle siirrolle 78 §:n 1 momentin nojalla, paitsi jos jäsenvaltio, joka on alun perin siirtänyt kyseiset tiedot, tai tähän jäsenvaltioon sijoittautunut henkilö, joka on lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annetussa direktiivissä tarkoitettu toimivaltainen viranomainen, on antanut siirtoon luvan jäsenvaltion lainsäädännön mukaisesti. Nämä suojatoimet ovat tärkeitä, koska ne antavat jäsenvaltioiden viranomaisille mahdollisuuden varmistaa suojan jatkuvuus EU:n tietosuojalainsäädäntöä noudattaen koko siirtoketjun ajan.

(87) Kansainvälisiä siirtoja koskevien uusien puitteiden soveltaminen alkoi siirtymäkauden päätyttyä ([152]). Liitteessä 21 olevassa 10–12 kohdassa (otettu käyttöön DPPC-säädöksellä) kuitenkin säädetään, että siirtymäkauden päättymisestä lähtien tiettyjä henkilötietojen siirtoja kohdellaan, ikään kuin ne perustuisivat tietosuojan riittävyyttä koskeviin asetuksiin. Näihin siirtoihin kuuluvat siirrot jäsenvaltioon, EFTA-valtioon, kolmanteen maahan, josta EU on tehnyt tietosuojan tason riittävyyttä koskevan päätöksen siirtymäkauden päättyessä, sekä Gibraltarin alueelle. Siirtoja näihin maihin voidaan jatkaa samalla tavoin kuin ennen Yhdistyneen kuningaskunnan eroamista unionista. Siirtymäkauden päättymisen jälkeen Secretary of Staten on tarkasteltava tietosuojan riittävyyttä uudelleen neljän vuoden jälkeen eli joulukuun 2024 loppuun mennessä. Yhdistyneen kuningaskunnan viranomaiset ovat selittäneet, että vaikka Secretary of Staten on toteutettava tällainen uudelleentarkastelu joulukuun 2024 loppuun mennessä, siirtymäsäännöksiin ei sisälly raukeamissäännöstä, joten niiden oikeusvaikutus ei lakkaa automaattisesti, vaikka tarkastelu ei olisikaan saatettu päätökseen joulukuun 2024 loppuun mennessä.

2.4.9 *Vastuuvelvollisuus*

(88) Vastuuvelvollisuutta koskevan periaatteen mukaisesti tietoja käsittelevien viranomaisten on otettava käyttöön asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta ne voivat tehokkaasti noudattaa tietosuojavelvoitteitaan ja myös osoittaa sen erityisesti toimivaltaiselle valvontaviranomaiselle.

(89) Tämä periaate on otettu huomioon vuoden 2018 tietosuojalain 56 §:ssä, jossa asetetaan rekisterinpitäjälle yleinen vastuuvelvollisuus eli velvoite toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet sen varmistamiseksi ja osoittamiseksi, että henkilötietojen käsittely on vuoden 2018 tietosuojalain 3 osan vaatimusten mukaista. Toteutettuja toimenpiteitä on tarkasteltava uudelleen ja päivitettävä tarvittaessa, ja jos se on oikeasuhteista käsittelyyn nähden, toteutettava asianmukaiset tietosuojaperiaatteet.

([151]) Vuoden 2018 tietosuojalain 73 §:n 5 momentti.

([152]) Tämän uuden kehyksen soveltamista on tarkasteltava Euroopan unionin ja Euroopan atomienergiayhteisön sekä Ison-Britannian ja Pohjois-Irlannin yhdistyneen kuningaskunnan välillä tehdyn kauppa- ja yhteistyösopimuksen, jäljempänä 'kauppa- ja yhteistyösopimus', 782 artiklan valossa. Sopimus (EUVL L 444, 31.12.2020, s. 14) on saatavilla seuraavassa osoitteessa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:22020A1231(01)&from=FI

(90) Samoin kuin direktiivin (EU) 2016/680 IV luvussa, vuoden 2018 tietosuojalain 55–71 §:ssä säädetään erilaisista mekanismeista, joilla varmistetaan vastuuvelvollisuus ja annetaan rekisterinpitäjille ja henkilötietojen käsittelijöille mahdollisuus osoittaa vaatimustenmukaisuus. Rekisterinpitäjien on erityisesti toteutettava sisäänrakennettu ja oletusarvoinen tietosuoja eli varmistettava, että tietosuojaperiaatteet pannaan tehokkaasti täytäntöön. Niiden on myös pidettävä kirjaa kaikista rekisterinpitäjän vastuulla olevista käsittelytoimien luokista (mukaan lukien rekisterinpitäjän henkilöllisyys, tietosuojavastaavan yhteystiedot, käsittelyn tarkoitukset, tietojen vastaanottajien ryhmät, kuvaus rekisteröityjen ryhmistä ja henkilötiedot) ja pidettävä nämä tiedot pyynnöstä tietosuojavaltuutetun saatavilla. Rekisterinpitäjän ja henkilötietojen käsittelijän on myös säilytettävä lokitiedot tietyistä käsittelytoimista ja annettava ne tietosuojavaltuutetun käyttöön ([153]). Rekisterinpitäjien on myös avustettava tietosuojavaltuutettua hänen tehtäviensä hoitamisessa.

(91) Vuoden 2018 tietosuojalaissa asetetaan myös lisävaatimuksia käsittelylle, joka todennäköisesti aiheuttaa suuren riskin yksilöiden oikeuksille ja vapauksille. Näihin kuuluu velvollisuus tehdä tietosuojaa koskevia vaikutustenarviointeja ja kuulla tietosuojavaltuutettua ennen käsittelyä, jos tällainen arviointi osoittaa, että käsittely aiheuttaisi suuren riskin yksilöiden oikeuksille ja vapauksille (jos ei ryhdytä toimiin riskin lieventämiseksi).

(92) Rekisterinpitäjien on lisäksi nimitettävä tietosuojavastaava, paitsi jos rekisterinpitäjä on tuomioistuin tai muu oikeusviranomainen, joka toimii lainkäyttötehtävissä ([154]). Rekisterinpitäjän on varmistettava, että tietosuojavastaava osallistuu kaikkien henkilötietojen suojaan liittyvien kysymysten käsittelyyn, että hänellä on tarvittavat resurssit ja pääsy henkilötietoihin ja käsittelytoimiin ja että hän voi suorittaa tehtävänsä riippumattomasti. Tietosuojavastaavan tehtävistä säädetään vuoden 2018 tietosuojalain 71 §:ssä, ja niihin kuuluvat tietojen ja neuvojen antaminen, tietosuojasääntöjen noudattamisen valvonta sekä yhteistyö tietosuojavaltuutetun kanssa ja yhteyspisteenä toimiminen. Tehtäviään suorittaessaan tietosuojavastaavan on tutkittava käsittelytoimiin liittyvät riskit ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset.

2.5 **Valvonta ja täytäntöönpano**

2.5.1 *Riippumaton valvonta*

(93) Sen varmistamiseksi, että tietosuojan riittävä taso taataan myös käytännössä, on oltava riippumaton valvontaviranomainen, jonka tehtävänä on valvoa tietosuojasääntöjen noudattamista ja varmistaa niiden täytäntöönpano. Kyseisen viranomaisen on toimittava riippumattomasti ja puolueettomasti tehtäviään suorittaessaan ja toimivaltuuksiaan käyttäessään.

(94) Yhdistyneen kuningaskunnan yleisen tietosuoja-asetuksen ja vuoden 2018 tietosuojalain noudattamisen valvonnasta ja täytäntöönpanosta vastaa tietosuojavaltuutettu (Information Commissioner) ([155]). Tietosuojavaltuutettu valvoo myös toimivaltaisten viranomaisten vuoden 2018 tietosuojalain 3 osan nojalla suorittamaa henkilötietojen käsittelyä ([156]). Tietosuojavaltuutettu on ns. Corporation Sole eli itsenäinen oikeushenkilö, jonka tehtävää hoitaa yksi luonnollinen henkilö. Tietosuojavaltuutettua avustaa hänen työssään toimisto. Tietosuojavaltuutetun toimiston vakinaisten työntekijöiden määrä 31. maaliskuuta 2020 oli 768 ([157]). Tietosuojavaltuutettu toimii digitaaliasiain-, kulttuuri-, media- ja urheiluministeriön alaisuudessa ([158]).

([153]) Vuoden 2018 tietosuojalain 62 §.
([154]) Vuoden 2018 tietosuojalain 69 §.
([155]) Direktiivin (EU) 2016/680 36 artiklan 2 kohdan b alakohta.
([156]) Vuoden 2018 tietosuojalain 116 §.
([157]) Tietosuojavaltuutetun vuosikertomus ja varainhoitovuoden 2019–2020 tilinpäätös ovat saatavilla seuraavassa osoitteessa: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf
([158]) Niiden keskinäisiä suhteita säännellään hallinnointisopimuksella. Vastuuministeriön keskeisenä tehtävänä on muun muassa varmistaa, että tietosuojavaltuutetulla on käytössään riittävä rahoitus ja henkilöstö; edustaa tietosuojavaltuutettua parlamentissa ja muissa hallintoelimissä; varmistaa, että käytössä on vankka kansallinen tietosuojakehys; ja antaa tietosuojavaltuutetulle ohjeita ja tukea esimerkiksi kiinteistö-, vuokraus- ja hankintakysymyksissä (vuosien 2018–2021 hallinnointisopimus (Management Agreement) on saatavilla seuraavassa osoitteessa: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Tietosuojavaltuutetun riippumattomuus vahvistetaan nimenomaisesti Yhdistyneen kuningaskunnan yleisen tietosuoja-asetuksen 52 artiklassa, jossa otetaan huomioon Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 ([159]) 52 artiklan 1–3 kohdassa säädetyt vaatimukset. Tietosuojavaltuutetun tulee toimia täysin riippumattomasti hoitaessaan tehtäviään ja käyttäessään hänelle Yhdistyneen kuningaskunnan yleisen tietosuoja-asetuksen mukaisesti annettuja valtuuksia. Häneen ei saa vaikuttaa ulkopuolelta suoraan eikä välillisesti hänen hoitaessaan tehtäviään ja käyttäessään valtuuksiaan, eikä hän saa pyytää eikä ottaa ohjeita miltään taholta. Tietosuojavaltuutetun on myös pidättäydyttävä kaikesta toiminnasta, joka ei sovi yhteen hänen tehtäviensä hoitamisen kanssa, eikä hän saa toimikautensa aikana harjoittaa palkallista tai palkatonta yhteensopimatonta ammattitoimintaa.

(96) Tietosuojavaltuutetun nimittämistä ja erottamista koskevat ehdot esitetään vuoden 2018 tietosuojalain liitteessä 12. Kuningatar nimittää tietosuojavaltuutetun oikeudenmukaisen ja läpinäkyvän kilpailun perusteella laaditun hallituksen suosituksen mukaisesti. Hakijoilla on oltava asianmukainen tutkinto, osaaminen ja pätevyys. Neuvoa-antava arviointilautakunta laatii luettelon hyväksytyistä hakijoista julkisia nimityksiä koskevien hallintosääntöjen ([160]) mukaisesti. Secretary of State tekee päätöksensä sen jälkeen, kun asianomainen parlamentin erityisvaliokunta on suorittanut ennakkotarkastelun. Valiokunnan lausunto julkaistaan ([161]).

(97) Tietosuojavaltuutetun toimikausi on enintään seitsemän vuotta. Hänen Majesteettinsa voi erottaa tietosuojavaltuutetun parlamentin molempien kamarien esityksen (Address) perusteella ([162]). Ehdotusta tietosuojavaltuutetun erottamisesta ei voida esittää kummallekaan parlamentin kamarille, ellei ministeri ole esittänyt kyseiselle kamarille selvitystä, jossa hän katsoo, että tietosuojavaltuutettu on syyllistynyt vakavaan väärinkäytökseen ja/tai hän ei enää täytä tietosuojavaltuutetun tehtävien hoitamiselle asetettuja edellytyksiä ([163]).

(98) Tietosuojavaltuutetun rahoitus on peräisin kolmesta lähteestä: i) rekisterinpitäjien maksamat tietosuojamaksut, jotka vahvistetaan Secretary of Staten asetuksella ([164]) ja joilla katetaan 85–90 prosenttia toimiston vuosibudjetista ([165]); ii) avustus, jonka hallitus voi maksaa tietosuojavaltuutetulle ja jolla rahoitetaan pääasiassa muista kuin tietosuojaan liittyvistä tehtävistä aiheutuvat tietosuojavaltuutetun toimintakustannukset ([166]); iii) palveluista perittävät maksut ([167]). Tällä hetkellä tällaisia maksuja ei peritä.

(99) Tietosuojavaltuutetun yleiset tehtävät, jotka koskevat vuoden 2018 tietosuojalain 3 osan soveltamisalaan kuuluvien henkilötietojen käsittelyä, vahvistetaan vuoden 2018 tietosuojalain liitteessä 13. Tehtäviin kuuluu vuoden 2018 tietosuojalain 3 osan seuranta ja täytäntöönpano, yleisen tietoisuuden lisääminen, parlamentin, hallituksen ja muiden toimielinten avustaminen lainsäädännöllisissä ja hallinnollisissa toimenpiteissä, rekisterinpitäjien ja

([159]) Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (EUVL L 119, 4.5.2016, s. 1).

([160]) Julkisia nimityksiä koskevat hallintosäännöt ovat saatavilla seuraavassa osoitteessa: https://www.gov.uk/government/publications/governance-code-for-public-appointments

([161]) Second Report of Session 2015–2016 of the Culture, Media and Sports Committee at the House of Commons, saatavilla seuraavassa osoitteessa: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) ”Address” on parlamentille osoitettava esitys, jonka tarkoituksena on saattaa monarkin tietoon parlamentin näkemys tietystä kysymyksestä.

([163]) Vuoden 2018 tietosuojalain liitteessä 12 oleva 3 kohta.

([164]) Vuoden 2018 tietosuojalain 137 §.

([165]) Vuoden 2018 tietosuojalain 137 ja 138 §:ssä vahvistetaan erilaisia suojatoimia sen varmistamiseksi, että maksut asetetaan asianmukaiselle tasolle. Erityisesti vuoden 2018 tietosuojalain 137 §:n 4 kohdassa luetellaan seikat, jotka Secretary of Staten on otettava huomioon antaessaan asetuksia eri organisaatioilta perittävien maksujen määrittämiseksi. Vuoden 2018 tietosuojalain 138 §:n 1 momentissa ja 182 §:ssä asetetaan Secretary of Statelle oikeudellinen velvoite kuulla ennen asetusten antamista tietosuojavaltuutettua ja muita sellaisten henkilöiden edustajia, joihin asetukset todennäköisesti vaikuttavat, jotta heidän näkemyksensä voidaan ottaa huomioon. Lisäksi tietosuojavaltuutetun on vuoden 2018 tietosuojalain 138 §:n 2 momentin nojalla seurattava maksuasetuksen (Charges Regulations) toimintaa ja esitettävä tarvittaessa Secretary of Statelle ehdotus sen muuttamiseksi. Maksuasetuksiin sovelletaan ns. myönteistä päätöslauselmamenettelyä (affirmative resolution procedure), jonka mukaan ne voidaan hyväksyä vasta kun kumpikin parlamentin kamari on antanut niistä myönteisen päätöslauselman. (Jos asetuksella kuitenkin vain otetaan huomioon vähittäishintaindeksin nousu, sovelletaan negatiivista päätöslauselmamenettelyä.)

([166]) Hallinnointisopimuksen mukaan Secretary of State voi suorittaa tietosuojavaltuutetulle maksuja varoista, jotka parlamentti on myöntänyt tähän tarkoitukseen vuoden 2018 tietosuojalain liitteessä 12 olevan 9 kohdan nojalla. Tietosuojavaltuutettua kuultuaan ministeri maksaa tietosuojavaltuutetulle asianmukaisen tukimäärän hallintomenoihin ja mm. tiedonvapauteen liittyvien tietosuojavaltuutetun erityistehtävien hoitamista varten (hallinnointisopimus 2018–2021, 1.12 kohta, ks. alaviite158).

([167]) Vuoden 2018 tietosuojalain 134 §.

henkilötietojen käsittelijöiden velvollisuuksia koskevan tietoisuuden edistäminen, rekisteröidyn oikeuksien käyttämistä koskevien tietojen antaminen rekisteröidylle ja tutkimusten suorittaminen. Oikeuslaitoksen riippumattomuuden takaamiseksi henkilötietojen käsittelyyn liittyviä tietosuojavaltuutetun tehtäviä ei voi hoitaa henkilö eikä tuomioistuin, joka suorittaa lainkäyttötehtäviä. Oikeuslaitoksen valvonta on osoitettu erityisille elimille, kuten jäljempänä esitetään.

2.5.1.1 Täytäntöönpanon valvonta, ml. seuraamukset

(100) Tietosuojavaltuutetulla on yleiset tutkintavaltuudet, korjaavat toimivaltuudet sekä hyväksymis- ja neuvontavaltuudet, kun on kyse vuoden 2018 tietosuojalain 3 osan soveltamisalaan kuuluvien henkilötietojen käsittelystä. Tietosuojavaltuutetulla on valtuudet ilmoittaa rekisterinpitäjälle tai henkilötietojen käsittelijälle väitetystä 3 osan rikkomisesta, antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle varoitus siitä, että aiotut käsittelytoimet todennäköisesti rikkovat 3 osan säännöksiä, ja antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle huomautus, jos käsittelytoimet ovat rikkoneet 3 osan säännöksiä. Lisäksi tietosuojavaltuutettu voi omasta aloitteestaan tai pyynnöstä antaa lausuntoja Yhdistyneen kuningaskunnan parlamentille, hallitukselle tai muille toimielimille ja elimille sekä yleisölle kaikista henkilötietojen suojaan liittyvistä kysymyksistä ([168]).

(101) Tietosuojavaltuutetulla on erityisesti toimivalta

— määrätä rekisterinpitäjä ja henkilötietojen käsittelijä (ja tietyissä tapauksissa kuka tahansa muu henkilö) toimittamaan tarvittavat tiedot ns. tiedonantomääräyksellä (information notice) ([169]);

— suorittaa tutkimuksia ja tarkastuksia antamalla ns. tarkastusmääräys (assessment notice), jonka nojalla rekisterinpitäjää tai henkilötietojen käsittelijää voidaan vaatia antamaan tietosuojavaltuutetulle pääsy tiettyihin tiloihin ja oikeus tarkastaa tai tutkia asiakirjoja tai laitteita sekä kuulla henkilöitä, jotka käsittelevät henkilötietoja rekisterinpitäjän puolesta ([170]);

— hankkia muulla tavoin pääsy rekisterinpitäjien ja henkilötietojen käsittelijöiden asiakirjoihin ja niiden tiloihin vuoden 2018 tietosuojalain 154 §:n mukaisesti (”pääsy- ja tarkastusvaltuudet”);

— käyttää korjaavia toimivaltuuksia esittämällä varoituksia ja huomautuksia tai antamalla täytäntöönpanomääräyksiä (enforcement notice), joissa rekisterinpitäjät / henkilötietojen käsittelijät määrätään toteuttamaan tai kielletään niitä toteuttamasta tiettyjä toimenpiteitä ([171]); sekä

— määrätä hallinnollisia sakkoja ns. seuraamusmääräyksellä (penalty notice) ([172]).

(102) Tietosuojavaltuutetun sääntelytoimia koskevissa toimintaperiaatteissa (Regulatory Action Policy) esitetään, missä olosuhteissa tietosuojavaltuutettu voi antaa em. ilmoituksia ja määräyksiä ([173]). Täytäntöönpanomääräyksessä voidaan asettaa vaatimuksia, joita tietosuojavaltuutettu pitää asianmukaisina puutteen korjaamiseksi. Seuraamusmääräyksessä vaaditaan henkilöä maksamaan tietosuojavaltuutetulle määräyksessä esitetty määrä. Seuraamusmääräys voidaan antaa, jos vuoden 2018 tietosuojalain ([174]) tiettyjä säännöksiä ei ole noudatettu, tai se voidaan antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle, joka ei ole noudattanut tiedonanto-, tarkastus- tai täytäntöönpanopäätöstä.

(103) Tarkemmin sanottuna päättäessään seuraamusmääräyksen antamisesta rekisterinpitäjälle tai henkilötietojen käsittelijälle ja seuraamuksen määrästä tietosuojavaltuutetun on otettava huomioon vuoden 2018 tietosuojalain 155 §:n 3 momentissa luetellut seikat, mukaan lukien laiminlyönnin luonne ja vakavuus, laiminlyönnin tahallisuus tai tuottamuksellisuus, rekisterinpitäjän tai henkilötietojen käsittelijän toteuttamat toimet rekisteröidyn kärsimän

([168]) Vuoden 2018 tietosuojalain liitteessä 13 oleva 2 kohta.
([169]) Vuoden 2018 tietosuojalain 142 § (vuoden 2018 tietosuojalain 143 §:ssä säädetyin rajoituksin) .
([170]) Vuoden 2018 tietosuojalain 146 § (vuoden 2018 tietosuojalain 147 §:ssä säädetyin rajoituksin).
([171]) Vuoden 2018 tietosuojalain 149–151 § (vuoden 2018 tietosuojalain 152 §:ssä säädetyin rajoituksin).
([172]) Vuoden 2018 tietosuojalain 155 § (vuoden 2018 tietosuojalain 156 §:ssä säädetyin rajoituksin).
([173]) Sääntelytoimia koskevat toimintaperiaatteet (Regulatory Action Policy) ovat saatavilla seuraavassa osoitteessa: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) Tietosuojavaltuutettu voi antaa seuraamusmääräyksen erityisesti vuoden 2018 tietosuojalain 149 §:n 2, 3, 4 tai 5 momentissa tarkoitetun noudattamatta jättämisen vuoksi.

vahingon lieventämiseksi, rekisterinpitäjän tai henkilötietojen käsittelijän vastuun aste (ottaen huomioon rekisterinpitäjän tai henkilötietojen käsittelijän toteuttamat tekniset ja organisatoriset toimenpiteet), rekisterinpitäjän tai henkilötietojen käsittelijän mahdolliset aiemmat laiminlyönnit, henkilötietojen ryhmät, joita laiminlyönti koskee, ja se, olisiko seuraamus tehokas, oikeasuhteinen ja varoittava.

(104) Seuraamusmääräyksellä määrättävän seuraamuksen enimmäismäärä on 17 500 000 puntaa, kun kyse on tietosuojaperiaatteiden (vuoden 2018 tietosuojalain 35, 36, 37 §, 38 §:n 1 momentti, 39 §:n 1 momentti ja 40 §), läpinäkyvyyttä koskevien velvoitteiden ja yksilön oikeuksien (vuoden 2018 tietosuojalain 44, 45, 46, 47, 48, 49, 52 ja 53 §) tai kansainvälisten henkilötietojen siirtoa koskevien periaatteiden (vuoden 2018 tietosuojalain 73, 75, 76, 77 ja 78 §) noudattamatta jättämisestä. Muussa tapauksessa seuraamuksen enimmäismäärä on 8 700 000 puntaa ([175]). Tiedonanto-, arviointi- tai täytäntöönpanomääräyksen noudattamatta jättämisen vuoksi voidaan määrätä seuraamusmääräyksellä sakkoa enintään 17 500 000 puntaa.

(105) Viimeisimpien vuosikertomustensa (2018–2019 ([176]), 2019–2020 ([177])) mukaan tietosuojavaltuutettu on suorittanut useita tutkimuksia, jotka koskevat rikosoikeudellisten lainvalvontaviranomaisten suorittamaa henkilötietojen käsittelyä. Esimerkiksi lokakuussa 2019 tietosuojavaltuutettu julkaisi tutkimustensa perusteella lausunnon, joka koskee kasvojentunnistusteknologian käyttöä julkisilla paikoilla lainvalvontatarkoituksia varten. Tutkimuksessa keskityttiin erityisesti siihen, miten Etelä-Walesin poliisi (South Wales Police) ja suur-Lontoon poliisi (Metropolitan Police Services) käyttävät reaaliaikaista kasvojentunnistusta. Tietosuojavaltuutettu on tutkinut myös suur-Lontoon poliisin jengitietokantaa (Gangs matrix) ([178]) ja todennut, että siihen liittyy useita vakavia tietosuojalainsäädännön rikkomisia, jotka todennäköisesti heikentäisivät yleisön luottamusta tietokantaan ja siihen, miten tietoja käytetään.

(106) Marraskuussa 2018 tietosuojavaltuutettu antoi täytäntöönpanomääräyksen, jonka nojalla suur-Lontoon poliisi toteutti tarvittavat toimet turvallisuuden ja vastuuvelvollisuuden lisäämiseksi ja sen varmistamiseksi, että tietoja käytetään oikeasuhteisesti.

(107) Toinen esimerkki viimeaikaisista täytäntöönpanotoimista tällä alalla on tietosuojavaltuutetun toukokuussa 2018 määräämä 325 000 punnan sakko kruunun syyttäjäyksikölle poliisikuulustelujen tallenteita sisältävien salaamattomien DVD-levyjen katoamisen vuoksi. Tietosuojavaltuutettu on lisäksi tutkinut yleisempiä aiheita, kuten vuoden 2020 alkupuoliskolla matkapuhelintietojen käyttöä poliisitoiminnassa ja uhrien tietojen käsittelyä poliisin toimesta.

(108) Koska eräät tietosuojalainsäädännön loukkaukset ovat rikoksia, niiden perusteella voidaan määrätä myös rikosoikeudellisia seuraamuksia sen lisäksi, että niihin sovelletaan tietosuojavaltuutetun täytäntöönpanovaltuuksia (vuoden 2018 tietosuojalain 196 §). Tämä koskee esimerkiksi henkilötietojen hankkimista tai luovuttamista ilman rekisterinpitäjän suostumusta ja luovutettujen henkilötietojen toimittamista toiselle henkilölle ilman rekisterinpitäjän suostumusta ([179]); anonymisoitujen henkilötietojen tunnistetietojen palauttamista ilman anonymisoinnista vastaavan rekisterinpitäjän suostumusta ([180]); tahallista toimintaa, jolla estetään tietosuojavaltuutettua käyttämästä toimivaltaansa henkilötietojen tarkastamiseksi kansainvälisten velvoitteiden mukaisesti ([181]), väärien lausuntojen antamista tiedonantomääräyksen perusteella tai tietojen tuhoamista tiedonanto- ja arviointimääräysten yhteydessä ([182]).

(109) Tietosuojavaltuutetulla on myös vuoden 2018 tietosuojalain 139 §:n nojalla velvollisuus antaa kummallekin parlamentin kamarille yleiskertomus lakisääteisten tehtäviensä hoitamisesta ([183]).

([175]) Vuoden 2018 tietosuojalain 157 §.

([176]) Tietosuojavaltuutetun vuosikertomus ja varainhoitovuoden 2018–2019 tilinpäätös ovat saatavilla seuraavassa osoitteessa: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) Tietosuojavaltuutetun vuosikertomus 2019–2020 (ks. alaviite 157).

([178]) Tietokantaan talletetaan tiedustelutietoa oletetuista jengien jäsenistä ja jengirikollisuuden uhreista.

([179]) Vuoden 2018 tietosuojalain 170 §.

([180]) Vuoden 2018 tietosuojalain 171 §.

([181]) Vuoden 2018 tietosuojalain 119 §.

([182]) Vuoden 2018 tietosuojalain 144 ja 148 §.

([183]) Kuten hallinnointisopimuksessa määrätään, vuosikertomuksessa on i) käsiteltävä kaikki tietosuojavaltuutetun määräysvallassa olevat yhtiöt, tytäryhtiöt tai yhteisyritykset; ii) noudatettava valtionkassan tilinpäätöskäsikirjaa (Treasury's Financial Reporting Manual); iii) oltava hallintotapaselvitys (governance statement), jossa esitetään, miten tilinpitäjä on hallinnoinut ja valvonut organisaatiossa käytettyjä resursseja kuluneen vuoden aikana, ja jossa osoitetaan, kuinka hyvin organisaatio hallitsee tavoitteidensa ja päämääriensä saavuttamiseen kohdistuvia riskejä; ja iv) esitettävä pääpiirteittäin edellisen varainhoitovuoden tärkeimmät toimet ja tulokset sekä esitettävä yhteenveto tulevista suunnitelmista (hallinnointisopimus 2018–2021, kohta 3.26, ks. alaviite 158).

2.5.2 *Oikeuslaitoksen valvonta*

(110) Tuomioistuinten ja oikeuslaitoksen suorittamaan henkilötietojen käsittelyyn sovelletaan kahta eri valvontamenettelyä. Silloin kun oikeuslaitoksen virkamies tai tuomioistuin ei toimi lainkäyttötehtävissä, valvonnasta vastaa tietosuojavaltuutettu. Sen sijaan silloin kun rekisterinpitäjä toimii lainkäyttötehtävissä, tietosuojavaltuutettu ei voi hoitaa valvontatehtäväänsä ([184]), vaan se on osoitettu erityisille elimille. Lähestymistapa on sama kuin direktiivin (EU) 2016/680 32 artiklassa.

(111) Jälkimmäisessä tilanteessa valvonnasta vastaa Englannin ja Walesin tuomioistuinten (courts, First-tier ja Upper Tribunals) osalta oikeuslaitoksen tietosuojalautakunta (Judicial Data Protection Panel) ([185]). Lisäksi Englannin ja Walesin korkeimman oikeuden presidentti (Lord Chief Justice) on laatinut tietosuojaselosteen (Privacy Notice) ([186]), jossa kerrotaan, miten Englannin ja Walesin tuomioistuimet käsittelevät henkilötietoja lainkäyttötehtäviä varten. Vastaavan tietosuojaselosteen ovat antaneet myös Pohjois-Irlannin ([187]) ja Skotlannin ([188]) oikeusviranomaiset.

(112) Lisäksi Pohjois-Irlannin Lord Chief Justice on nimittänyt yhden High Court -tuomioistuimen tuomarin tietosuojaa valvovaksi tuomariksi ([189]). Pohjois-Irlannin oikeuslaitokselle on myös laadittu ohjeet siitä, miten on toimittava tietojen (mahdollisen) menetyksen yhteydessä ja miten tästä mahdollisesti aiheutuvia ongelmia on käsiteltävä ([190]).

(113) Skotlannin ylin tuomari Lord President on nimittänyt tietosuojaa valvovan tuomarin (Data Supervisory Judge), jonka tehtävänä on tutkia tietosuojaa koskevia valituksia. Tästä säädetään oikeussuojakeinoja koskevissa säännöissä, jotka vastaavat Englannin ja Walesin osalta vahvistettuja sääntöjä ([191]).

(114) Lisäksi yksi korkeimman oikeuden (Supreme Court) tuomareista on nimitetty valvomaan tietosuojaa.

([184]) Vuoden 2018 tietosuojalain 117 §.

([185]) Lautakunnan tehtävänä on antaa oikeuslaitokselle ohjausta ja koulutusta. Lisäksi se käsittelee rekisteröityjen tekemiä valituksia, jotka koskevat tuomioistuinten ja lainkäyttötehtäviä hoitavien henkilöiden suorittamaa henkilötietojen käsittelyä. Lautakunta pyrkii löytämään ratkaisun kaikkiin valituksiin. Jos valituksen tekijä ei ole tyytyväinen lautakunnan päätökseen ja esittää lisänäyttöä, lautakunta voi harkita päätöstään uudelleen. Lautakunta ei itse määrää taloudellisia seuraamuksia, mutta jos se katsoo, että vuoden 2018 tietosuojalakia on rikottu riittävän vakavasti, se voi viedä valituksen oikeuslaitoksen tutkintalautakunnan (Judicial Conduct Investigation) käsiteltäväksi. Jos valitus todetaan aiheelliseksi, lordikansleri (oikeusministeri) ja Lord Chief Justice (tai tehtävään valtuutettu vanhempi tuomari) päättävät, mitä toimia viranhaltijaa vastaan olisi toteutettava. Näitä voivat olla vakavuusjärjestyksessä virallinen muistutus, virallinen varoitus, huomautus ja viime kädessä erottaminen virasta. Jos yksityishenkilö on tyytymätön tapaan, jolla tutkintalautakunta on tutkinut asiaa, hän voi valittaa asiasta edelleen tuomarien nimityksistä ja viranhoidosta vastaavalle oikeusasiamiehelle (Judicial Appointments and Conduct Ombudsman; ks. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Oikeusasiamiehellä on valtuudet pyytää tutkintalautakuntaa tutkimaan valitus uudelleen ja ehdottaa, että valituksen tekijälle maksetaan korvaus, jos hänen katsotaan kärsineen vahinkoa hallinnollisen väärinkäytöksen vuoksi.

([186]) Lord Chief Justicen ja tuomioistuinten ylimmän presidentin laatima tietosuojaseloste on saatavilla seuraavassa osoitteessa: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([187]) Pohjois-Irlannin Lord Chief Justicen laatima tietosuojaseloste on saatavilla seuraavassa osoitteessa: https://judiciaryni.uk/data-privacy

([188]) Skotlannin tuomioistuinten tietosuojaseloste on saatavilla seuraavassa osoitteessa: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([189]) Tietosuojaa valvova tuomari laatii ohjeita oikeuslaitokselle ja tutkii tietoturvaloukkauksia ja/tai valituksia, jotka koskevat tuomioistuinten tai lainkäyttötehtäviä hoitavien henkilöiden suorittamaa henkilötietojen käsittelyä.

([190]) Jos valitus tai tietoturvaloukkaus katsotaan vakavaksi, se toimitetaan edelleen oikeuslaitoksen oikeusasiamiehen (Judicial Complaints Officer) tutkittavaksi Pohjois-Irlannin Lord Chief Justicen laatiman valituksia koskevien käytännesääntöjen (Code of Practice on Complaints) mukaisesti. Valituksen ratkaisu voi olla jokin seuraavista: ei aiheuta toimenpiteitä, muistutus, koulutus tai mentorointi, epävirallinen varoitus, virallinen varoitus, lopullinen varoitus, ammatinharjoittamisen rajoitus tai käsittelyn siirtäminen lakisääteiseen tuomioistuimeen. Pohjois-Irlannin Lord Chief Justicen laatimat valituksia koskevat käytännesäännöt ovat saatavilla seuraavassa osoitteessa: 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]) Tietosuojaa valvovan tuomarin tutkimuksissa aiheelliseksi todettu valitus saatetaan Lord Presidentin käsiteltäväksi. Hänellä on toimivalta määrätä annettavaksi muistutus, virallinen varoitus tai huomautus, jos hän katsoo sen tarpeelliseksi (vastaavat tuomioistuinten jäseniä koskevat säännöt ovat saatavilla seuraavassa osoitteessa: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3 *Oikeussuojakeinot*

(115) Jotta voidaan varmistaa yksilön oikeuksien asianmukainen suojelu ja täytäntöönpano, rekisteröidyllä olisi oltava tehokkaat hallinnolliset ja oikeudelliset oikeussuojakeinot ja myös oikeus saada vahingonkorvausta.

(116) Ensinnäkin rekisteröidyllä on oikeus tehdä tietosuojavaltuutetulle valitus, jos hän katsoo, että hänen henkilötietojensa käsittelyssä on rikottu vuoden 2018 tietosuojalain 3 osan säännöksiä ([192]). Kuten johdanto-osan 100 ja 109 kappaleessa todetaan, tietosuojavaltuutetulla on toimivalta arvioida, ovatko rekisterinpitäjä ja henkilötietojen käsittelijä noudattaneet vuoden 2018 tietosuojalakia, ja jos näin ei ole, vaatia niitä toteuttamaan tarvittavat toimet tai pidättymään tietyistä toimista ja määrätä sakkoja.

(117) Toiseksi vuoden 2018 tietosuojalaissa säädetään oikeudesta käyttää oikeussuojakeinoja tietosuojavaltuutettua vastaan. Jos tietosuojavaltuutettu ei ”edistä” ([193]) rekisteröidyn tekemän valituksen käsittelyä, tämä voi hakea oikeussuojaa tuomioistuimelta pyytämällä, että First Tier Tribunal -tuomioistuin ([194]) määrää tietosuojavaltuutetun toteuttamaan valituksen johdosta asianmukaiset toimenpiteet tai ilmoittamaan valituksen tekijälle sitä koskevan tutkinnan etenemisestä ([195]). Lisäksi kuka tahansa henkilö, jolle tietosuojavaltuutettu on antanut jonkin edellä mainituista määräyksistä (tiedonanto-, arviointi-, täytäntöönpano- tai seuraamusmääräys), voi hakea siihen muutosta First Tier Tribunal -tuomioistuimessa. Jos tuomioistuin katsoo, että tietosuojavaltuutetun päätös ei ole lainmukainen tai että tietosuojavaltuutetun olisi pitänyt käyttää harkintavaltaansa eri tavalla, tuomioistuimen on hyväksyttävä muutoksenhakemus tai korvattava annettu määräys toisella määräyksellä tai päätöksellä, jonka tietosuojavaltuutettu olisi voinut antaa tai tehdä ([196]).

(118) Kolmanneksi yksilöt voivat vedota oikeudellisiin oikeussuojakeinoihin rekisterinpitäjiä ja henkilötietojen käsittelijöitä vastaan suoraan tuomioistuimissa vuoden 2018 tietosuojalain 167 §:n nojalla. Jos tuomioistuin katsoo rekisteröidyn hakemuksen perusteella, että tietosuojalainsäädäntöön perustuvia rekisteröidyn oikeuksia on loukattu, se voi määrätä käsittelystä vastaavan rekisterinpitäjän tai tämän puolesta toimivan henkilötietojen käsittelijän toteuttamaan määräyksessä yksilöidyt toimenpiteet tai pidättymään siinä yksilöidyistä toimenpiteistä. Lisäksi vuoden 2018 tietosuojalain 169 §:ssä säädetään, että henkilö, joka kärsii vahinkoa jonkin tietosuojalainsäädännössä (ml. vuoden 2018 tietosuojalain 3 osa, mutta pois lukien Yhdistyneen kuningaskunnan yleinen tietosuoja-asetus) vahvistetun oikeuden loukkaamisen vuoksi, on oikeutettu saamaan tällaisesta vahingosta korvauksen rekisterinpitäjältä tai henkilötietojen käsittelijältä, paitsi jos nämä voivat osoittaa, etteivät ole millään tavoin vastuussa vahingon aiheuttaneesta tapahtumasta. Vahingolla tarkoitetaan tässä sekä taloudellista menetystä että esimerkiksi kärsimystä.

(119) Neljänneksi henkilö, joka katsoo, että viranomaiset ovat loukanneet hänen oikeuksiaan, mukaan lukien oikeutta yksityisyyteen ja tietosuojaan, voi viedä asian Yhdistyneen kuningaskunnan tuomioistuimiin vuoden 1998 ihmisoikeuslain nojalla. Vuoden 2018 tietosuojalain 3 osan mukaiset rekisterinpitäjät eli toimivaltaiset viranomaiset ovat aina viranomaisia vuoden 1998 ihmisoikeuslaissa tarkoitetussa merkityksessä. Henkilö, joka väittää, että viranomainen on toiminut (tai aikoo toimia) tavalla, joka on ristiriidassa jonkin ihmisoikeussopimukseen perustuvan oikeuden kanssa ja siten vuoden 1998 ihmisoikeuslain 6 §:n 1 momentin nojalla lainvastainen, voi nostaa kanteen kyseistä viranomaista vastaan toimivaltaisessa tuomioistuimessa tai vedota asianomaisiin oikeuksiin missä tahansa oikeudenkäynnissä, kun hän on (tai olisi) lainvastaisen teon uhri ([197]).

([192]) Vuoden 2018 tietosuojalain 165 §.

([193]) Vuoden 2018 tietosuojalain 166 §:ssä viitataan nimenomaisesti seuraaviin tilanteisiin: a) tietosuojavaltuutettu ei ole toteuttanut asianmukaisia toimenpiteitä valitukseen vastaamiseksi, b) tietosuojavaltuutettu ei ole antanut valituksen tekijälle tietoja tutkinnan etenemisestä tai sen tuloksesta kolmen kuukauden kuluessa siitä kun tietosuojavaltuutettu on vastaanottanut valituksen, tai c) jos tietosuojavaltuutettu ei tee valituksen perusteella ratkaisua tai ei anna valituksen tekijälle tutkintaa koskevia tietoja em. kolmen kuukauden määräajan kuluessa.

([194]) First Tier Tribunal -tuomioistuin on toimivaltainen käsittelemään hallituksen sääntelyelinten päätöksiä koskevat muutoksenhaut. Kun muutoksenhaku koskee tietosuojavaltuutetun päätöstä, toimivaltainen jaosto on ”yleinen sääntelyjaosto” (General Regulatory Chamber), joka on toimivaltainen koko Yhdistyneessä kuningaskunnassa.

([195]) Vuoden 2018 tietosuojalain 166 §.

([196]) Vuoden 2018 tietosuojalain 161 ja 162 §.

([197]) Ks. asia Brown v. Commissioner of Police of the Metropolis 2016, jossa tuomioistuin myönsi kantajalle korvauksen tietosuojan alalla poliisia vastaan nostetussa asiassa. Tuomioistuin hyväksyi kantajan vaatimukset, jotka koskivat vuoden 1998 tietosuojalain velvoitteiden rikkomista, vuoden 1998 ihmisoikeuslain (ja siihen liittyvän Euroopan ihmisoikeussopimuksen 8 artiklan mukaisen oikeuden) rikkomista sekä yksityisten tietojen väärinkäyttöä (vastaaja myönsi lopulta tietosuojalain ja Euroopan ihmisoikeussopimuksen rikkomisen, joten tuomiossa keskityttiin siihen, mikä oli asianmukainen oikeussuojakeino). Näiden rikkomisten seurauksena tuomioistuin määräsi kantajalle maksettavan rahallisen korvauksen.

(120) Jos tuomioistuin toteaa, että jokin viranomaisen toimi on lainvastainen, se voi toimivaltuuksiensa puitteissa hyväksyä sellaisen vaatimuksen tai oikeussuojakeinon tai antaa sellaisen määräyksen, jonka se katsoo kohtuulliseksi ja asianmukaiseksi ([198]). Tuomioistuin voi myös todeta, että jokin primaarioikeuden säännös ei sovi yhteen jonkin ihmisoikeussopimuksessa taatun oikeuden kanssa.

(121) Sen jälkeen kun kansalliset oikeussuojakeinot on käytetty loppuun, yksilö voi myös käyttää oikeussuojakeinoja Euroopan ihmisoikeustuomioistuimessa, jos Euroopan ihmisoikeussopimuksessa taattuja oikeuksia on loukattu.

2.6 **Tietojen edelleen jakaminen**

(122) Yhdistyneen kuningaskunnan lainsäädännön mukaan lainvalvontaviranomainen voi jakaa tietoja toisille Yhdistyneen kuningaskunnan viranomaisille muita kuin niitä tarkoituksia varten, johon ne alun perin kerättiin, jäljempänä 'tietojen edelleen jakaminen', vain tiettyjen edellytysten täyttyessä.

(123) Samoin kuin direktiivin (EU) 2016/680 4 artiklan 2 kohdassa, vuoden 2018 tietosuojalain 36 §:n 3 momentissa sallitaan toimivaltaisen viranomaisen lainvalvontatarkoituksia varten keräämien henkilötietojen myöhempi käsittely (joko alkuperäisen rekisterinpitäjän tai toisen rekisterinpitäjän toimesta) muuta kuin alkuperäistä lainvalvontatarkoitusta varten, sikäli kuin rekisterinpitäjällä on lupa käsitellä tällaisia henkilötietoja tällaista muuta tarkoitusta varten ja käsittely on tarpeellista ja oikeasuhteista ([199]). Tässä tapauksessa vastaanottavan viranomaisen suorittamaan käsittelyyn sovelletaan kaikkia vuoden 2018 tietosuojalain 3 osassa säädettyjä ja edellä käsiteltyjä suojatoimia.

(124) Yhdistyneen kuningaskunnan oikeusjärjestyksessä tietojen edelleen jakaminen sallitaan nimenomaisesti eri laeissa. Muun muassa i) vuonna 2017 digitaalitaloudesta annetussa laissa (Digital Economy Act 2017) sallitaan tietojen jakaminen viranomaisten kesken eri tarkoituksia varten, esimerkiksi jos on kyse julkiseen sektoriin kohdistuvasta petoksesta, joka aiheuttaisi viranomaisille menetyksiä tai menetysten riskin ([200]) tai jos kyseessä on velka viranomaiselle tai valtiolle (the Crown) ([201]); ii) vuonna 2013 rikoksista ja tuomioistuimista annetussa laissa sallitaan tietojen jakaminen kansallisen rikosviraston ([202]) kanssa vakavan ja järjestäytyneen rikollisuuden torjuntaa, tutkintaa ja syytteeseenpanoa varten; iii) vuonna 2007 vakavasta rikollisuudesta annetussa laissa (Serious Crime Act 2007) sallitaan viranomaisten paljastaa tietoja petostentorjunnasta vastaaville organisaatioille petostentorjuntaa varten ([203]).

(125) Näissä laeissa säädetään nimenomaisesti, että tietojen jakamisessa on noudatettava vuoden 2018 tietosuojalaissa vahvistettuja sääntöjä. Lisäksi poliisiakatemia on antanut tietojen jakamista koskevia sisäisiä ohjeita (Authorised Professional Practice on Information Sharing) ([204]), joiden tarkoituksena on auttaa poliisia noudattamaan Yhdistyneen kuningaskunnan yleiseen tietosuoja-asetukseen, tietosuojalakiin ja vuoden 1998 ihmisoikeuslakiin perustuvia tietosuojavelvoitteitaan. Tuomioistuinvalvonnan avulla voidaan varmistaa, että tietojen jakamisen yhteydessä noudatetaan sovellettavaa tietosuojaa koskevaa oikeudellista kehystä ([205]).

(126) Samoin kuin direktiivin (EU) 2016/680 9 artiklassa, vuoden 2018 tietosuojalaissa säädetään lisäksi, että lainvalvontatarkoitusta varten kerättyjä henkilötietoja voidaan käsitellä muussa kuin lainvalvontatarkoituksessa vain, jos tällainen käsittely sallitaan laissa ([206]). Tällainen jakaminen kattaa kaksi eri tapausta: 1) rikoslain täytäntöönpanon valvonnasta vastaava viranomainen jakaa tietoja jonkin muun viranomaisen kanssa, tiedustelupalvelua lukuun

([198]) Vuoden 1998 ihmisoikeuslain 8 §:n 1 momentti.

([199]) Vuoden 2018 tietosuojalain 36 §:n 3 momentti.

([200]) Vuonna 2017 digitaalitaloudesta annetun lain 56 §, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2017/30/contents

([201]) Vuonna 2017 digitaalitaloudesta annetun lain 48 §.

([202]) Vuonna 2013 rikoksista ja tuomioistuimista annetun lain 7 §, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2013/22/contents

([203]) Vuonna 2007 vakavasta rikollisuudesta annetun lain 68 §, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2007/27/contents

([204]) Authorised Professional Practice on Information Sharing, saatavilla seuraavassa osoitteessa: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

([205]) Ks. esimerkiksi asia M, R v. the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), jossa High Court -tuomioistuinta pyydettiin tarkastelemaan tietojen jakamista poliisin ja rikollisuuden vähentämistä edistävän yrityskumppanuusorganisaation Business Crime Reduction Partnership (BCRP) välillä; organisaatiolla oli valtuudet hallinnoida määräyksiä (exclusion notice), joilla tietyiltä henkilöiltä evättiin pääsy organisaation jäsenten liiketiloihin. Tuomioistuin totesi tarkastelunsa yhteydessä, että tietojen jakaminen perustui sopimukseen, jonka tarkoituksena oli suojella yleisöä ja ehkäistä rikollisuutta, ja katsoi lopulta, että se tapahtui valtaosaksi lainmukaisesti, eräitä arkaluontoisia tietoja lukuun ottamatta. Toinen esimerkki on asia Cooper v. NCA [2019] EWCA Civ 16, jossa muutoksenhakutuomioistuin Court of Appeal hyväksyi tietojen jakamisen poliisin ja vakavaa järjestäytynyttä rikollisuutta käsittelevän viraston (Serious Organised Crime Agency, SOCA) välillä; tämä lainvalvontavirasto on nykyään osa kansallista rikosvirastoa (NCA).

([206]) Vuoden 2018 tietosuojalain 36 §:n 4 momentti.

ottamatta (eli esimerkiksi finanssivalvonta- tai veroviranomaisen, kilpailuviranomaisen tai lastensuojeluviranomaisen kanssa); ja 2) rikoslain täytäntöönpanon valvonnasta vastaava viranomainen jakaa tietoja tiedustelupalvelun kanssa. Ensimmäisessä tapauksessa henkilötietojen käsittely kuuluu sekä Yhdistyneen kuningaskunnan yleisen tietosuoja-asetuksen että vuoden 2018 tietosuojalain 2 osan soveltamisalaan. Kuten asetuksen (EU) 2016/679 nojalla annetussa päätöksessä täsmennetään, Yhdistyneen kuningaskunnan yleisessä tietosuoja-asetuksessa ja vuoden 2018 tietosuojalain 2 osassa säädetyt tietosuojatakeet tarjoavat pohjimmiltaan unionissa tarjotun tasoisen suojan ([207]).

(127) Toisessa tapauksessa rikoslain täytäntöönpanon valvonnasta vastaava viranomainen jakaa keräämiään tietoja tiedustelupalvelun kanssa kansallisen turvallisuuden suojelemiseksi. Sovellettava oikeusperusta on tällöin vuoden 2008 terrorismintorjuntalaki (Counter Terrorism Act 2008) ([208]). Vuoden 2008 terrorismintorjuntalain nojalla kuka tahansa voi antaa tietoja mille tahansa tiedustelupalvelun yksikölle minkä tahansa kyseiselle yksikölle kuuluvan tehtävän suorittamista varten, ”kansallinen turvallisuus” mukaan lukien.

(128) Edellytyksistä, joiden mukaan tietoja voidaan jakaa kansallisen turvallisuuden suojelemiseksi, säädetään tiedustelupalvelulaissa (Intelligence Services Act) ja turvallisuuspalvelulaissa (Security Services Act). Niissä rajoitetaan tiedustelupalvelujen oikeus saada tietoja siihen, mikä on tarpeen niiden lakisääteisten tehtävien hoitamista varten. Jos vuoden 2018 tietosuojalain 3 osan soveltamisalaan kuuluvat lainvalvontavirastot haluavat jakaa tietoja tiedustelupalvelujen kanssa, niiden on otettava huomioon useita tekijöitä/rajoituksia niiden virastojen lakisääteisten tehtävien lisäksi, joista säädetään tiedustelupalvelulaissa ja turvallisuuspalvelulaissa ([209]). Vuoden 2008 terrorismintorjuntalain 20 §:ssä selvennetään, että jaettaessa tietoja mainitun lain 19 §:n nojalla on silti noudatettava tietosuojalainsäädäntöä, mikä tarkoittaa, että kaikkia vuoden 2018 tietosuojalaissa säädettyjä rajoituksia ja vaatimuksia sovelletaan. Lisäksi lainvalvontaviranomaiset ja tiedustelupalvelut ovat vuoden 1998 ihmisoikeuslaissa tarkoitettuja viranomaisia, joten niiden on varmistettava, että ne noudattavat toiminnassaan Euroopan ihmisoikeussopimuksessa ja erityisesti sen 8 artiklassa taattuja oikeuksia. Toisin sanoen nämä vaatimukset merkitsevät sitä, että kaikessa lainvalvontavirastojen ja tiedustelupalvelujen välisessä tietojen jakamisessa noudatetaan tietosuojalainsäädäntöä ja ihmisoikeussopimusta.

(129) Kun tiedustelupalvelut käsittelevät henkilötietoja, jotka on saatu lainvalvontaviranomaisilta kansallista turvallisuutta koskeviin tarkoituksiin, käsittelyyn sovelletaan useita edellytyksiä ja suojatoimia ([210]). Vuoden 2018 tietosuojalain 4 osaa sovelletaan kaikkeen tiedustelupalvelujen suorittamaan tai niiden puolesta tapahtuvaan

([207]) Yhdistyneen kuningaskunnan tarjoaman henkilötietojen suojan riittävyydestä Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 mukaisesti annettu komission täytäntöönpanopäätös C(2021)4800.

([208]) Vuoden 2008 terrorismintorjuntalain 19 §, saatavilla seuraavassa osoitteessa: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([209]) Vuoden 1994 tiedustelupalvelulain (ks. https://www.legislation.gov.uk/ukpga/1994/13/contents) 2 §:n 2 momentin mukaan ”Tiedustelupalvelun päällikkö vastaa palvelun tehokkuudesta, ja hänen velvollisuutensa on varmistaa, – a) että käytössä on järjestelyt sen varmistamiseksi, että tiedustelupalvelu hankkii tietoja yksinomaan siltä osin, kuin ne ovat tarpeen sen tehtävien hoitamiseksi, ja että se ei paljasta mitään tietoja muutoin kuin siltä osin kuin se on tarpeen – i) kyseistä tarkoitusta varten; ii) kansallisen turvallisuuden vuoksi; iii) vakavan rikollisuuden ehkäisemiseksi tai paljastamiseksi; tai iv) rikosasian käsittelyä varten; ja b) että tiedustelupalvelu ei ryhdy mihinkään toimiin minkään Yhdistyneen kuningaskunnan poliittisen puolueen etujen edistämiseksi”. Vuoden 1989 turvallisuuspalveluja koskevan lain (ks. https://www.legislation.gov.uk/ukpga/1989/5/contents) 2 §:n 2 momentin mukaan taas ”Pääjohtaja vastaa palvelun tehokkuudesta, ja hänen velvollisuutensa on varmistaa, – a) että käytössä on järjestelyt sen varmistamiseksi, että tiedustelupalvelu hankkii tietoja yksinomaan siltä osin kuin ne ovat tarpeen sen tehtävien hoitamiseksi ja että se paljastaa tietoja vain siltä osin kuin se on tarpeen kyseistä tarkoitusta varten tai vakavan rikollisuuden ehkäisemiseksi tai paljastamiseksi tai rikosasian käsittelyä varten; ja b) että palvelu ei ryhdy mihinkään toimiin minkään poliittisen puolueen etujen edistämiseksi; ja c) että kansallisen rikosviraston johtajan kanssa on sovittu järjestelyistä, joilla tämän lain 1 §:n 4 momentin nojalla suoritettavia palvelun toimia koordinoidaan poliisin, kansallisen rikosviraston ja muiden lainvalvontavirastojen toimien kanssa”.

([210]) Tiedustelupalvelujen valtuuksia koskevista suojatoimista ja rajoituksista säädetään myös vuonna 2016 tutkintavaltuuksista annetussa laissa, joka yhdessä tutkintavaltuuksia koskevien asetusten (Englannin, Walesin ja Pohjois-Irlannin osalta Regulation of Investigatory Powers Act 2000 ja Skotlannin osalta Regulation of Investigatory Powers (Scotland) Act 2000) kanssa muodostaa oikeusperustan tällaisten valtuuksien käytölle. Näillä valtuuksilla ei kuitenkaan ole merkitystä ”tietojen edelleen jakamisen” yhteydessä, koska ne koskevat tiedustelupalvelujen suorittamaa henkilötietojen suoraa keruuta. Tutkintavaltuuksia koskevan lain nojalla tiedustelupalveluille myönnettyjen valtuuksien arvioinnista ks. Yhdistyneen kuningaskunnan tarjoaman henkilötietojen suojan riittävyydestä Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/679 mukaisesti annettu komission täytäntöönpanopäätös C(2021) 4800.

käsittelyyn. Siinä esitetään tärkeimmät tietosuojaperiaatteet (lainmukaisuus, kohtuullisuus ja läpinäkyvyys ([211]); käyttötarkoituksen rajoittaminen ([212]); tietojen minimointi ([213]); täsmällisyys ([214]); säilyttämisen rajoittaminen ([215]) ja turvallisuus ([216])), asetetaan edellytykset erityisten tietoryhmien käsittelylle ([217]), säädetään rekisteröityjen oikeuksista ([218]), edellytetään sisäänrakennettua tietosuojaa ([219]) ja säännellään henkilötietojen kansainvälisiä siirtoja ([220]).

(130) Toisaalta vuoden 2018 tietosuojalain 110 §:ssä säädetään sen 4 osan tiettyjä säännöksiä koskevasta poikkeuksesta silloin, kun se on tarpeen kansallisen turvallisuuden takaamiseksi. Vuoden 2018 tietosuojalain 110 §:n 2 momentissa luetellaan säännökset, joista poikkeaminen sallitaan. Näitä ovat muun muassa tietosuojaperiaatteet (lainmukaisuusperiaatetta lukuun ottamatta), rekisteröidyn oikeudet, velvollisuus ilmoittaa tietoturvaloukkauksesta tietosuojavaltuutetulle, kansainvälisten velvoitteiden mukaiset tietosuojavaltuutetun tarkastusvaltuudet ja tietyt tietosuojavaltuutetun täytäntöönpanovaltuudet, säännökset joiden nojalla tietyt tietosuojaloukkaukset kriminalisoidaan sekä säännökset, jotka liittyvät erityisiin käsittelytarkoituksiin, kuten käsittely journalistisia, akateemisia tai taiteellisia tarkoituksia varten. Poikkeukseen voidaan vedota tapauskohtaisen analyysin perusteella ([221]). Kuten Yhdistyneen kuningaskunnan viranomaiset ovat selvittäneet ja sen oikeuskäytännössä on vahvistettu, ”rekisterinpitäjän on otettava huomioon, mitä tosiasiallisia seurauksia asianomaisten tietosuojasääntöjen noudattamisesta aiheutuisi kansalliselle turvallisuudelle tai puolustukselle, ja olisiko niiden kohtuudella mahdollista noudattaa tavanomaisia sääntöjä ilman, että siitä aiheutuisi seurauksia kansalliselle turvallisuudelle tai puolustukselle” ([222]). Sen, onko poikkeusta sovellettu asianmukaisella tavalla, ratkaisee tietosuojavaltuutettu ([223]).

([211]) Vuoden 2018 tietosuojalain 86 §:n 6 momentin mukaan käsittelyn kohtuullisuuden ja läpinäkyvyyden määrittämiseksi on tarkasteltava menetelmää, jonka avulla tiedot on saatu. Sen mukaan kohtuullisuutta ja läpinäkyvyyttä koskevat vaatimukset täyttyvät, jos tiedot saadaan henkilöltä, jolla on laillinen valtuutus tai velvollisuus toimittaa ne.

([212]) Vuoden 2018 tietosuojalain 87 §:n nojalla käsittelyn tarkoituksen on oltava tietty, nimenomainen ja laillinen. Tietoja ei saa käsitellä tavalla, joka on yhteensopimaton sen tarkoituksen kanssa, jota varten ne on kerätty. Lain 87 §:n 3 momentin nojalla henkilötietojen myöhempi käsittely voidaan sallia vain, jos rekisterinpitäjällä on lakisääteinen valtuutus käsitellä tietoja kyseistä tarkoitusta varten ja jos käsittely on välttämätöntä ja oikeasuhteista tähän muuhun tarkoitukseen nähden. Käsittelyn olisi katsottava olevan sääntöjen mukaista, jos se tehdään yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ja siihen sovelletaan asianmukaisia suojatoimia (vuoden 2018 tietosuojalain 87 §:n 4 momentti).

([213]) Henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja (vuoden 2018 tietosuojalain 88 §).

([214]) Henkilötietojen on oltava täsmällisiä ja ajantasaisia (vuoden 2018 tietosuojalain 89 §).

([215]) Henkilötietoja ei saa säilyttää pidempään kuin on tarpeen (vuoden 2018 tietosuojalain 90 §).

([216]) Kuudennen tietosuojaperiaatteen mukaan henkilötietoja on käsiteltävä ottaen huomioon henkilötietojen käsittelystä aiheutuvien riskien edellyttämät asianmukaiset turvatoimenpiteet. Näitä riskejä ovat esimerkiksi vahingossa tapahtuva tai lainvastainen pääsy henkilötietoihin tai niiden tuhoaminen, häviäminen, käyttäminen, muuttaminen tai luovuttaminen (vuoden 2018 tietosuojalain 91 §). Lain 107 §:ssä myös edellytetään, että 1) jokaisen rekisterinpitäjän on toteutettava henkilötietojen käsittelystä aiheutuvien riskien edellyttämät asianmukaiset turvatoimenpiteet, ja 2) jos kyseessä on automaattinen käsittely, jokaisen rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskinarviointiin perustuvia ehkäiseviä tai lieventäviä toimenpiteitä.

([217]) Vuoden 2018 tietosuojalain liite 10 ja 86 §:n 2 momentin b kohta.

([218]) Vuoden 2018 tietosuojalain 4 osan 3 luku ja erityisesti oikeus tutustua tietoihin ja oikaista tai poistaa ne, oikeus vastustaa tietojen käsittelyä ja oikeus olla joutumatta automaattisen päätöksenteon kohteeksi, oikeus puuttua automatisoituun päätöksentekoon ja saada tieto päätöksenteosta. Rekisterinpitäjän on myös annettava rekisteröidylle tietoa hänen henkilötietojensa käsittelystä.

([219]) Vuoden 2018 tietosuojalain 103 §.

([220]) Vuoden 2018 tietosuojalain 109 §. Henkilötietojen siirrot kansainvälisille järjestöille tai Yhdistyneen kuningaskunnan ulkopuolisille mailla ovat mahdollisia, jos siirto on välttämätön ja oikeasuhteinen toimenpide ja se toteutetaan rekisterinpitäjän lakisääteisiä tehtäviä varten tai muita sellaisia tarkoituksia varten, joista säädetään vuoden 1989 turvallisuuspalvelulain (Security Service Act 1989) ja vuoden 1994 tiedustelupalvelulain (Intelligence Services Act 1994) asiaa koskevissa säännöksissä.

([221]) Ks. asia Baker v. Secretary of State for the Home Department [2001] UKIT NSA2 (’Baker v. Secretary of State’).

([222]) UK Explanatory Framework for Adequacy Discussion, H jakso: National Security Data Protection and Investigatory Powers Framework, s. 15–16, saatavilla seuraavassa osoitteessa: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf Ks. myös Baker v. Secretary of State (ks. edellä alaviite 220), jossa tuomioistuin kumosi sisäasiainministerin antaman kansallista turvallisuutta koskevan todistuksen ja vahvisti kansallista turvallisuutta koskevan poikkeuksen soveltamisen, koska se katsoi, ettei ollut syytä säätää yleisestä poikkeuksesta tiedonsaantioikeuteen vastaamista koskevaan velvollisuuteen, vaan että tällaisen poikkeuksen hyväksyminen kaikissa olosuhteissa ilman tapauskohtaista analyysiä ylittäisi sen, mikä on välttämätöntä ja oikeasuhteista kansallisen turvallisuuden suojaamiseksi.

([223]) Ks. tietosuojavaltuutetun ja Yhdistyneen kuningaskunnan tiedusteluyhteisön (UK Intelligence Community, UKIC) välinen yhteisymmärryspöytäkirja, jonka mukaan ”sen jälkeen kun tietosuojavaltuutettu on saanut rekisteröidyn tekemän valituksen, hän haluaa varmistua siitä, että asia on käsitelty oikein, ja tarvittaessa siitä, että mahdollista poikkeusta on sovellettu asianmukaisella tavalla” (tietosuojavaltuutetun toimiston ja Yhdistyneen kuningaskunnan tiedusteluyhteisön yhteisymmärryspöytäkirja, kohta 16; saatavilla seuraavassa osoitteessa: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Mahdollisuudesta rajoittaa näiden edellä mainittujen oikeuksien soveltamista ”kansallisen turvallisuuden” suojelemiseksi vuoden 2018 tietosuojalain 79 §:ssä säädetään lisäksi, että rekisterinpitäjä voi pyytää kabinettiministerin tai oikeuskanslerin (Attorney General) allekirjoittamaa todistusta siitä, että tällaisten oikeuksien rajoittaminen on tai kyseiseen aikaan oli välttämätön ja oikeasuhteinen toimenpide kansallisen turvallisuuden suojelemiseksi ([224]). Yhdistyneen kuningaskunnan hallitus on antanut ohjeita vuoden 2018 tietosuojalain mukaisista kansallista turvallisuutta koskevista todistuksista. Ohjeissa korostetaan erityisesti, että kaikkien kansalliseen turvallisuuteen liittyvien rekisteröityjen oikeuksien rajoitusten on oltava oikeasuhteisia ja välttämättömiä ([225]). Kaikki kansallista turvallisuutta koskevat todistukset on julkaistava tietosuojavaltuutetun verkkosivuilla ([226]).

(132) Todistuksen olisi oltava voimassa määrätyn ajan ja enintään viisi vuotta, jotta toimeenpanovallan käyttäjä voi tarkastella sitä säännöllisesti uudelleen ([227]). Todistuksessa on yksilöitävä ne henkilötiedot tai henkilötietoryhmät, joihin poikkeusta sovelletaan, sekä ne vuoden 2018 tietosuojalain säännökset, joista poikkeaminen sallitaan ([228]).

(133) On huomattava, että kansallista turvallisuutta koskevat todistukset eivät muodosta lisäperustetta tietosuojaoikeuksien rajoittamiselle kansalliseen turvallisuuteen liittyvien syiden vuoksi. Toisin sanoen rekisterinpitäjä tai henkilötietojen käsittelijä voi vedota todistukseen vain, jos se on katsonut tarpeelliseksi vedota kansallista turvallisuutta koskevaan poikkeukseen, jota on sovellettava tapauskohtaisesti. Vaikka asiaan sovellettaisiin kansallista turvallisuutta koskevaa todistusta, tietosuojavaltuutettu voi tutkia, oliko vetoaminen siinä myönnettyyn poikkeukseen kyseisessä tapauksessa perusteltua ([229]).

(134) Jokainen, jota todistuksen antaminen suoraan koskee, voi hakea Upper Tribunal -tuomioistuimessa ([230]) muutosta todistukseen ([231]), tai jos tiedot esitetään todistuksessa yleisellä tasolla, vastustaa todistuksen soveltamista määrättyihin tietoihin ([232]).

(135) Tuomioistuin tutkii todistuksen antamista koskevan päätöksen ja päättää, oliko sen antamiseen perusteltu syy ([233]). Tuomioistuin voi tarkastella tätä varten erilaisia seikkoja, kuten tarpeellisuutta, oikeasuhteisuutta ja lainmukaisuutta, ottaen huomioon todistuksen vaikutukset rekisteröityjen oikeuksiin ja tasapainottaen niitä suhteessa tarpeeseen varmistaa kansallinen turvallisuus. Tämän perusteella tuomioistuin voi päättää, että todistusta ei sovelleta muutoksenhaun kohteena oleviin henkilötietoihin ([234]).

([224]) Vuoden 2018 tietosuojalaissa on kumottu mahdollisuus myöntää tällainen todistus vuoden 1998 tietosuojalain 28 §:n 2 momentin nojalla. Edelleen on kuitenkin mahdollista antaa ”vanhoja todistuksia” vuoden 1998 lain nojalla (ks. vuoden 2018 tietosuojalain liitteessä 20 olevan 5 osan 17 kohta). Tämä mahdollisuus vaikuttaa kuitenkin hyvin harvinaiselta ja sitä voidaan soveltaa vain rajoitetuissa tapauksissa, jos rekisteröity riitauttaa kansalliseen turvallisuuteen perustuvan poikkeuksen käytön tilanteessa, jossa viranomainen on suorittanut käsittelytoimia vuoden 1998 lain nojalla. Huomattakoon, että tällaisissa tapauksissa sovelletaan vuoden 1998 tietosuojalain 28 §:ää kokonaisuudessaan, eli rekisteröidyllä on mahdollisuus riitauttaa todistus. Tällä hetkellä ei ole yhtään vuoden 1998 tietosuojalain nojalla annettua kansallista turvallisuutta koskevaa todistusta.

([225]) United Kingdom Government Guidance on National Security Certificates under the Data Protection Act 2018, saatavilla seuraavassa osoitteessa: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

([226]) Vuoden 2018 tietosuojalain 130 §:n mukaan tietosuojavaltuutettu voi päättää olla julkaisematta todistuksen tekstiä tai sen osaa, jos julkaiseminen olisi kansalliseen turvallisuuteen liittyvän tai yleisen edun vastaista tai jos se voisi vaarantaa kenen tahansa henkilön turvallisuuden. Tällaisissa tapauksissa tietosuojavaltuutettu julkaisee kuitenkin tiedon siitä, että todistus on myönnetty.

([227]) United Kingdom Government Guidance on National Security Certificates, kohta 15, ks. alaviite 225.

([228]) United Kingdom Government Guidance on National Security Certificates, kohta 5, ks. alaviite 225.

([229]) Vuoden 2018 tietosuojalain 102 §:n mukaan rekisterinpitäjän on pystyttävä osoittamaan, että se on noudattanut vuoden 2018 tietosuojalakia. Tämä merkitsee sitä, että tiedustelupalvelun olisi osoitettava tietosuojavaltuutetulle, että se on poikkeukseen vedotessaan ottanut huomioon tapaukseen liittyvät erityisolosuhteet. Tietosuojavaltuutettu myös julkaisee tiedot kansallista turvallisuutta koskevista todistuksista seuraavassa osoitteessa: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/

([230]) Upper Tribunal -tuomioistuimella on toimivalta käsitellä alempien hallintotuomioistuinten päätöksiä koskevat muutoksenhaut, ja sillä on erityinen toimivalta käsitellä tiettyjen hallintoelinten päätöksiä koskevat suorat muutoksenhaut.

([231]) Vuoden 2018 tietosuojalain 111 §:n 3 momentti.

([232]) Vuoden 2018 tietosuojalain 111 §:n 5 momentti.

([233]) Asiassa Baker v. Secretary of State (ks. alaviite 221) antamassaan tuomiossa Information Tribunal -tuomioistuin kumosi sisäasiainministerin antaman kansallista turvallisuutta koskevan todistuksen, koska se katsoi, ettei ollut syytä säätää yleisestä poikkeuksesta tiedonsaantioikeuteen vastaamista koskevaan velvollisuuteen, vaan että tällaisen poikkeuksen hyväksyminen kaikissa olosuhteissa ilman tapauskohtaista analyysiä ylittäisi sen, mikä on välttämätöntä ja oikeasuhteista kansallisen turvallisuuden suojaamiseksi.

([234]) United Kingdom Government Guidance on National Security Certificates, kohta 25, ks. alaviite 225.

(136) Muita mahdollisia rajoituksia voidaan soveltaa vuoden 2018 tietosuojalain liitteen 11 nojalla tiettyihin tietosuojalain 4 osan säännöksiin ([235]) muiden yleisen edun mukaisten tärkeiden tavoitteiden tai sellaisten suojattujen etujen turvaamiseksi kuin esimerkiksi parlamentaarinen koskemattomuus, asianajosalaisuus, oikeudenkäynnin kulku tai asevoimien toimintakyky. Näiden säännösten soveltaminen on joko vapautettu tiettyjen tietoryhmien osalta (”luokitusperusteinen vapautus”) tai siltä osin, kuin niiden soveltaminen todennäköisesti vahingoittaisi kyseistä suojattua etua (”vahinkoperusteinen vapautus”) ([236]). Vahinkoperusteisiin vapautuksiin voidaan vedota vain siltä osin, kuin säännöksessä lueteltujen tietosuojasäännösten soveltaminen todennäköisesti vahingoittaisi kyseessä olevaa etua. Tämä tarkoittaa, että vapautuksen soveltaminen on aina perusteltava viittaamalla vahinkoon, jonka sen soveltaminen kyseisessä yksittäisessä tapauksessa todennäköisesti aiheuttaisi. Luokitusperusteisiin vapautuksiin voidaan vedota vain niiden rajoitettujen tietoryhmien osalta, joiden osalta vapautus myönnetään. Nämä ovat tarkoitukseltaan ja vaikutuksiltaan samantapaisia kuin monet Yhdistyneen kuningaskunnan yleiseen tietosuoja-asetukseen (vuoden 2018 tietosuojalain liitteen 2 nojalla) sovellettavat poikkeukset, jotka puolestaan vastaavat EU:n tietosuoja-asetuksen 23 artiklan säännöksiä.

(137) Edellä esitetystä seuraa, että Yhdistyneen kuningaskunnan sovellettavien säännösten nojalla käytössä on rajoituksia ja ehtoja, joita myös tuomioistuimet ja tietosuojavaltuutettu tulkitsevat, sen varmistamiseksi, että näitä poikkeuksia ja rajoituksia sovelletaan vain siltä osin, kuin se on välttämätöntä ja oikeasuhteista kansallisen turvallisuuden suojelemiseksi.

(138) Tietosuojavaltuutettu valvoo tiedustelupalvelujen vuoden 2018 tietosuojalain 4 osan mukaisesti suorittamaa henkilötietojen käsittelyä ([237]).

(139) Tietosuojavaltuutetun yleiset tehtävät, jotka koskevat vuoden 2018 tietosuojalain 4 osan soveltamisalaan kuuluvaa tiedustelupalvelujen suorittamaa henkilötietojen käsittelyä, vahvistetaan vuoden 2018 tietosuojalain liitteessä 13. Tehtäviin kuuluvat erityisesti esimerkiksi vuoden 2018 tietosuojalain 4 osan seuranta ja täytäntöönpano, yleisen tietoisuuden lisääminen, parlamentin, hallituksen ja muiden toimielinten avustaminen lainsäädännöllisissä ja hallinnollisissa toimenpiteissä, rekisterinpitäjien ja henkilötietojen käsittelijöiden velvollisuuksia koskevan tietoisuuden edistäminen, rekisteröidyn oikeuksien käyttämistä koskevien tietojen antaminen rekisteröidylle ja tutkimusten suorittaminen.

(140) Tietosuojavaltuutetulla on vuoden 2018 tietosuojalain 3 osan osalta valtuudet ilmoittaa rekisterinpitäjille väitetystä rikkomisesta ja antaa varoituksia siitä, että käsittely todennäköisesti rikkoo sääntöjä, ja antaa huomautus vahvistetun rikkomisen johdosta. Se voi myös antaa täytäntöönpano- ja seuraamusmääräyksiä tiettyjen lain säännösten rikkomisen vuoksi ([238]). Toisin kuin vuoden 2018 tietosuojalain muiden osien yhteydessä, tietosuojavaltuutettu ei kuitenkaan voi antaa arviointimääräystä kansallisesta turvallisuudesta vastaavalle elimelle ([239]).

(141) Lisäksi vuoden 2018 tietosuojalain 110 §:ssä säädetään poikkeuksesta tietosuojavaltuutetun tiettyjen valtuuksien käyttöön silloin, kun se on tarpeen kansallisen turvallisuuden suojaamiseksi. Tähän sisältyvät tietosuojavaltuutetun valtuudet antaa (kaikentyyppisiä) tietosuojalain mukaisia määräyksiä (tiedonanto-, arviointi-, täytäntöönpano- ja seuraamusmääräykset), valtuudet suorittaa tarkastuksia kansainvälisten velvoitteiden mukaisesti, pääsy- ja tarkastus-

([235]) Tämä kattaa seuraavat: i) 4 osan tietosuojaperiaatteet, lukuun ottamatta ensimmäisen periaatteen yhteydessä mainittua käsittelyn lainmukaisuutta koskevaa vaatimusta ja sitä, että käsittelyn on täytettävä jokin liitteissä 9 ja 10 säädetyistä ehdoista; ii) rekisteröityjen oikeudet; ja iii) velvollisuudet, jotka koskevat tietoturvaloukkauksista ilmoittamista tietosuojavaltuutetulle.

([236]) Tietosuojan riittävyyttä koskevien perustelujen (UK Explanatory Framework) mukaan luokitusperusteisia poikkeuksia ovat: i) kruunun kunnianosoitusten ja kunniamerkkien myöntämistä koskevat tiedot; ii) asianajosalaisuus; iii) työsuhteeseen tai koulutukseen liittyvät luottamukselliset tiedot; ja iv) koepaperit ja arvosanat. Vahinkoperusteiset poikkeukset koskevat seuraavia seikkoja: i) rikosten ennalta estäminen tai paljastaminen; rikoksentekijöiden kiinniotto ja syytteeseenpano; ii) parlamentaarinen koskemattomuus; iii) oikeudenkäyntimenettelyt; iv) kruunun asevoimien taistelukyky; v) Yhdistyneen kuningaskunnan taloudellinen hyvinvointi; vi) rekisteröidyn kanssa käydyt neuvottelut; vii) tieteellinen tai historiallinen tutkimus tai tilastolliset tarkoitukset; viii) yleisen edun mukainen arkistointi. UK Explanatory Framework for Adequacy Discussion, H jakso: National Security, sivu 13, ks. alaviite 222.

([237]) Vuoden 2018 tietosuojalain 116 §.

([238]) Vuoden 2018 tietosuojalain 149 §:n 2 momentin ja 155 §:n, joita olisi tarkasteltava yhdessä, mukaan rekisterinpitäjälle tai henkilötietojen käsittelijälle voidaan antaa täytäntöönpano- ja seuraamusmääräys, jos ne ovat rikkoneet vuoden 2018 tietosuojalain 4 osan 2 luvun säännöksiä (käsittelyperiaatteet), vuoden 2018 tietosuojalain 4 osan säännöstä, jolla rekisteröidylle annetaan oikeuksia, vuoden 2018 tietosuojalain 108 §:n mukaista velvoitetta ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojavaltuutetulle ja vuoden 2018 tietosuojalain 109 §:ssä vahvistettuja periaatteita, jotka koskevat henkilötietojen siirtoa kolmansiin maihin, ihmisoikeussopimuksen ulkopuolisiin maihin ja kansainvälisille järjestöille. (Ks. lisätietoja täytäntöönpano- ja seuraamusmääräyksistä johdanto-osan 102–103 kappale).

([239]) Vuoden 2018 tietosuojalain 147 §:n 6 momentin mukaan tietosuojavaltuutettu ei voi antaa arviointimääräystä vuoden 2000 tiedonvapauslain 23 §:n 3 momentissa tarkoitetulle elimelle. Näihin kuuluvat turvallisuuspalvelu (MI5), salainen tiedustelupalvelu (MI6) ja tiedustelupalvelu.

valtuudet sekä rikoksia koskevat säännöt ([240]). Kuten johdanto-osan 136 kappaleessa selitetään, näitä poikkeuksia sovelletaan tapauskohtaisesti ja vain, jos se on välttämätöntä ja oikeasuhteista. Tuomioistuinvalvonnan avulla voidaan varmistaa näiden poikkeusten soveltaminen ([241]).

(142) Tietosuojavaltuutettu ja Yhdistyneen kuningaskunnan tiedustelupalvelut ovat allekirjoittaneet yhteisymmärryspöytäkirjan ([242]), jossa vahvistetaan puitteet muun muassa tietoturvaloukkauksia koskevien ilmoitusten ja rekisteröityjen tekemien valituksien käsittelyyn liittyvää yhteistyötä varten. Siinä määrätään erityisesti, että saatuaan valituksen tietosuojavaltuutettu tarkistaa, että mahdollista kansalliseen turvallisuuteen liittyvää poikkeusta on sovellettu asianmukaisesti. Kun tietosuojavaltuutettu pyytää tietoja yksityishenkilön tekemän valituksen tutkinnan yhteydessä, asianomaisen elimen (United Kingdom Government Guidance on National Security Certificates under the Data Protection Act) on vastattava 20 työpäivän kuluessa käyttäen asianmukaisia suojattuja kanavia, jos vastaus sisältää turvallisuusluokiteltuja tietoja. Tietosuojavaltuutettu on saanut huhtikuusta 2018 alkaen 21 yksityishenkilöiden tekemää valitusta, jotka koskevat tiedustelupalveluja. Kaikki valitukset on tutkittu, ja niiden tulos on ilmoitettu asianomaiselle rekisteröidylle ([243]).

(143) Lisäksi tiedustelu- ja turvallisuusvaliokunta (Intelligence and Security Committee) vastaa tiedustelupalvelujen suorittaman tietojenkäsittelyn parlamentaarisesta valvonnasta. Valiokunnan oikeusperustana on vuoden 2013 oikeus- ja turvallisuuslaki (Justice and Security Act 2013) ([244]). Lain mukaan tiedustelu- ja turvallisuusvaliokunta on Yhdistyneen kuningaskunnan parlamentin valiokunta. Sen jäsenet kuuluvat joko parlamentin ala- tai ylähuoneeseen, ja pääministeri nimittää heidät opposition johtajaa kuultuaan ([245]). Valiokunta esittää parlamentille vuosittain kertomuksen tehtäviensä hoitamisesta ja muita kertomuksia sen mukaan, kuin se katsoo tarpeelliseksi ([246]).

(144) Valiokunta sai vuonna 2013 laajemmat valtuudet mm. valvoa turvallisuuspalvelujen operatiivista toimintaa. Vuoden 2013 oikeus- ja turvallisuuslain 2 §:n nojalla valiokunnan tehtävänä on valvoa kansallisten turvallisuusvirastojen menoja, hallintoa, toimintaperiaatteita ja operaatioita. Laissa täsmennetään, että valiokunta voi suorittaa

([240]) Säännökset, joihin voidaan soveltaa poikkeusta, ovat seuraavat: 108 § (henkilötietojen tietoturvaloukkauksesta ilmoittaminen tietosuojavaltuutetulle), 119 § (kansainvälisten velvoitteiden mukainen tarkastus); 142–154 § ja liite 15 (tietosuojavaltuutetun määräykset sekä pääsy- ja tarkastusvaltuudet); ja 170–173 § (henkilötietoihin liittyvät rikokset). Lisäksi liitteessä 13 (tietosuojavaltuutetun muut yleiset tehtävät) olevan 1 kohdan a ja g alakohta ja 2 kohta, kun kyse on tiedustelupalvelujen suorittamasta käsittelystä.

([241]) Ks. esim. asia Baker v. Secretary of State for the Home Department (ks. alaviite 221).

([242]) Tietosuojavaltuutetun ja Yhdistyneen kuningaskunnan tiedusteluyhteisön välinen yhteisymmärryspöytäkirja, ks. alaviite 231.

([243]) Seitsemässä näistä tapauksista tietosuojavaltuutettu neuvoi valittajaa viemään asian rekisterinpitäjän käsiteltäväksi (näin toimitaan silloin kun valitus olisi alun perin pitänyt tehdä ensin rekisterinpitäjälle eikä tietosuojavaltuutetulle), yhdessä tapauksessa tietosuojavaltuutettu antoi rekisterinpitäjälle yleisiä neuvoja (näin tehdään silloin kun rekisterinpitäjän toiminta ei vaikuta rikkoneen lainsäädäntöä, mutta käytäntöjä muuttamalla olisi voitu välttää asian vieminen tietosuojavaltuutetun käsiteltäväksi), ja muissa 13 tapauksessa tietosuojavaltuutetun toimet eivät olleet tarpeen (näin on silloin kun valituksen aihe kuuluu vuoden 2018 tietosuojalain soveltamisalaan, koska se liittyy henkilötietojen käsittelyyn, mutta annettujen tietojen perusteella ei vaikuta siltä, että rekisterinpitäjä olisi rikkonut lainsäädäntöä).

([244]) Yhdistyneen kuningaskunnan viranomaisten selvityksen mukaan lailla laajennettiin valiokunnan toimeksiantoa niin, että se kattaa koko tiedusteluyhteisön valvonnan myös kolmen tiedusteluviraston ulkopuolella ja mahdollistaa virastojen operatiivisen toiminnan takautuvan valvonnan silloin kun asialla on huomattava kansallinen merkitys.

([245]) Vuoden 2013 oikeus- ja turvallisuuslain 1 §. Ministerit eivät voi olla valiokunnan jäseniä. Valiokunnan jäsenyys jatkuu jäsenen nimittämisen jälkeen kyseisen parlamentin toimikauden päättymiseen asti. Valiokunnan jäsen voidaan erottaa hänet nimittäneen parlamentin päätöslauselmalla, tai jos hän lakkaa olemasta parlamentin jäsen tai jos hänestä tulee ministeri. Jäsen voi myös erota tehtävästään.

([246]) Valiokunnan kertomukset ja lausunnot ovat saatavilla verkossa seuraavassa osoitteessa: http://isc.independent.gov.uk/committee-reports. Valiokunta antoi vuonna 2015 yksityisyydensuojaa ja turvallisuutta koskevaa lainsäädäntöä käsittelevän kertomuksen "Privacy and Security: A modern and transparent legal framework" (ks: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf). Kertomuksessa se tarkasteli tiedustelupalvelujen käyttämiä valvontatekniikoita koskevaa lainsäädäntöä ja antoi joukon suosituksia, jotka harkinnan jälkeen sisällytettiin tutkintavaltuuksia koskevaan lakiesitykseen, joka sittemmin vahvistettiin vuonna 2016 tutkintavaltuuksista annetuksi laiksi. Hallituksen vastaus yksityisyydensuojaa ja turvallisuutta koskevaan kertomukseen on saatavilla seuraavassa osoitteessa: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

tutkimuksia operatiivisista asioista silloin, kun ne eivät liity käynnissä oleviin operaatioihin ([247]). Pääministerin ja valiokunnan välisessä yhteisymmärryspöytäkirjassa ([248]) täsmennetään yksityiskohtaisesti seikat, jotka on otettava huomioon sen määrittämiseksi, onko jokin toiminta osa käynnissä olevaa operaatiota ([249]). Pääministeri voi myös pyytää valiokuntaa tutkimaan käynnissä olevia operaatioita, minkä lisäksi valiokunta voi tarkastella virastojen vapaaehtoisesti toimittamia tietoja.

(145) Vuoden 2013 oikeus- ja turvallisuuslain liitteen 1 nojalla tiedustelu- ja turvallisuusvaliokunta voi pyytää minkä tahansa kolmen tiedustelupalvelun johtajaa luovuttamaan mitä tahansa tietoja. Tiedustelupalvelujen on annettava nämä tiedot saataville, ellei Secretary of State vastusta sitä veto-oikeudellaan ([250]). Yhdistyneen kuningaskunnan viranomaiset selittivät, että valiokunnalta salataan käytännössä hyvin vähän tietoja ([251]).

(146) Oikeussuojakeinojen osalta vuoden 2018 tietosuojalain 165 §:n 2 momentin mukaan rekisteröidyllä on oikeus tehdä tietosuojavaltuutetulle valitus, jos hän katsoo, että hänen henkilötietojensa käsittelyssä on rikottu vuoden 2018 tietosuojalain 4 osan säännöksiä, mukaan lukien kansallista turvallisuutta koskevien poikkeusten ja rajoitusten väärinkäyttö.

(147) Vuoden 2018 tietosuojalain 4 osan nojalla rekisteröidyillä on lisäksi oikeus pyytää High Court -tuomioistuimelta (Skotlannissa Court of Session) määräys, jolla rekisterinpitäjä velvoitetaan noudattamaan tiedonsaantia koskevia oikeuksia ([252]), oikeutta vastustaa tietojen käsittelyä ([253]) ja oikeutta oikaista tai poistaa tiedot.

(148) Rekisteröidyillä on myös oikeus vaatia rekisterinpitäjältä tai henkilötietojen käsittelijältä korvausta vahingosta, joka on aiheutunut vuoden 2018 tietosuojalain 4 osassa säädettyjen vaatimusten rikkomisesta ([254]). Vahingolla tarkoitetaan tässä sekä taloudellista menetystä että esimerkiksi kärsimystä ([255]).

(149) Yksityishenkilö voi myös tehdä valituksen tutkintavaltuuksia käsittelevään tuomioistuimeen Yhdistyneen kuningaskunnan tiedusteluviranomaisten tai niiden puolesta suoritetuista toimista ([256]).Tutkintavaltuuksia käsittelevä tuomioistuin on perustettu tutkintavaltuuksia koskevilla asetuksilla (Englannin, Walesin ja Pohjois-Irlannin osalta Regulation of Investigatory Powers Act 2000 ja Skotlannin osalta Regulation of Investigatory Powers (Scotland) Act 2000), ja se on riippumaton toimeenpanovallan käyttäjästä ([257]). Vuonna 2000 tutkintavaltuuksista annetun asetuksen 65 §:n mukaan Hänen Majesteettinsa nimittää tuomioistuimen jäsenet viiden vuoden toimikaudeksi.

(150) Hänen Majesteettinsa voi erottaa tuomioistuimen jäsenen parlamentin molempien kamarien esityksen (Address) ([258]) perusteella ([259]).

(151) Vuonna 2000 tutkintavaltuuksista annetun asetuksen 65 §:n mukaan rekisteröidyllä on oikeus viedä asiansa Investigatory Powers Tribunal -tuomioistuimen käsiteltäväksi (”asiavaltuus”), jos hän uskoo, i) että tiedustelupalvelun toiminta kohdistuu häneen tai hänen omaisuuteensa tai hänen lähettämäänsä tai hänelle lähetettyyn tai hänelle tarkoitettuun viestintään tai hänen käyttämäänsä postipalveluun, televiestintäjärjestelmään tai televiestintäpalveluun ([260]) ja ii) että

([247]) Vuoden 2013 oikeus- ja turvallisuuslain 2 §.
([248]) Memorandum of Understanding between the Prime minister and the ISC, saatavilla seuraavassa osoitteessa: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) Memorandum of Understanding between the Prime minister and the ISC, 14 kohta, ks. alaviite 248.
([250]) Secretary of State voi veto-oikeudellaan kieltää tietojen luovuttamisen vain kahdella perusteella: tiedot ovat arkaluontoisia, eikä niitä pitäisi luovuttaa valiokunnalle kansallisen turvallisuuden vuoksi; tai tiedot ovat luonteeltaan sellaisia, että jos Secretary of Statea vaadittaisiin esittämään ne jossakin alahuoneen erityisvaliokunnassa, hän ei katsoisi sitä asianmukaiseksi (myös muista kuin kansalliseen turvallisuuteen liittyvistä syistä) (ks. vuoden 2013 oikeus- ja turvallisuuslain liitteessä 1 oleva 4 kohdan 2 alakohta).
([251]) UK Explanatory Framework – H jakso: National Security, s. 43.
([252]) Vuoden 2018 tietosuojalain 94 §:n 11 momentti.
([253]) Vuoden 2018 tietosuojalain 99 §:n 4 momentti.
([254]) Vuoden 2018 tietosuojalain 169 §:ssä säädetään, että ”henkilö, joka kärsii vahinkoa jonkin tietosuojalainsäädännössä vahvistetun oikeuden loukkaamisen vuoksi, on oikeutettu saamaan tällaisesta vahingosta korvauksen”.
([255]) Vuoden 2018 tietosuojalain 169 §:n 5 momentti.
([256]) Ks. vuonna 2000 tutkintavaltuuksista annetun asetuksen 65 §:n 2 momentin b kohta.
([257]) Asetuksen liitteen 3 nojalla tuomioistuimen jäsenillä on oltava tietty oikeusalan kokemus, ja heidät voidaan nimittää tehtäväänsä uudelleen.
([258]) ”Esityksen” (Address) käsitteestä ks. alaviite 183.
([259]) Vuonna 2000 tutkintavaltuuksista annetun asetuksen liitteessä 3 olevan 1 kohdan 5 alakohta.
([260]) Vuonna 2000 tutkintavaltuuksista annetun asetuksen 65 §:n 4 momentti.

toiminta on tapahtunut ”olosuhteissa, jotka on mahdollista kiistää” ([261]) tai että se on toteutettu tiedustelupalvelujen toimesta tai niiden puolesta ([262]). Koska etenkin tätä ”uskomista” koskevaa edellytystä on tulkittu varsin väljästi ([263]), asian vieminen tämän tuomioistuimen käsiteltäväksi ei edellytä erityistä asiavaltuutta.

(152) Kun kyseinen tuomioistuin käsittelee sille tehtyä valitusta, sen velvollisuutena on tutkia, ovatko henkilöt, joita koskevia väitteitä valituksessa esitetään, olleet jollakin tavoin tekemisissä valittajan kanssa, ja onko viranomainen, jonka väitetään osallistuneen oikeudenloukkauksiin, toteuttanut väitetyt toimet ([264]). Jos tuomioistuin ottaa asian käsiteltäväksi, sen on sovellettava ratkaisussaan samoja periaatteita kuin ne, joita mikä tahansa tuomioistuin soveltaisi oikeudellista uudelleentarkastelua koskevaan hakemukseen ([265]).

(153) Investigatory Powers Tribunal -tuomioistuimen on ilmoitettava valittajalle, onko asia ratkaistu hänen hyväkseen vai ei ([266]). Vuonna 2000 tutkintavaltuuksista annetun asetuksen 67 §:n 6 ja 7 momentin nojalla tuomioistuimella on toimivalta antaa väliaikaisia määräyksiä ja myöntää sopivaksi katsomiaan vahingonkorvauksia tai antaa muita määräyksiä ([267]). Vuonna 2000 tutkintavaltuuksista annetun asetuksen 67A §:n mukaan Investigatory Powers Tribunal -tuomioistuimen ratkaisuun on mahdollista hakea muutosta, ellei sen tai asianomaisen muutoksenhakutuomioistuimen myöntämästä luvasta muuta johdu.

(154) Yksityishenkilöt voivat nostaa kanteen ja hakea oikeussuojaa Investigatory Powers Tribunal -tuomioistuimesta, jos he katsovat, että viranomainen on toiminut (tai aikoo toimia) tavalla, joka on ristiriidassa esimerkiksi yksityisyyttä ja tietosuojaa koskevien Euroopan ihmisoikeussopimuksen mukaisten oikeuksien kanssa ja siten vuoden 1998 ihmisoikeuslain 6 §:n 1 momentin nojalla lainvastaista. Investigatory Powers Tribunal -tuomioistuimella on yksinomainen toimivalta käsitellä ihmisoikeuslakiin liittyviä kanteita, joissa on kysymys tiedustelupalveluista. Kuten High Court on todennut, tämä tarkoittaa, että kysymys siitä, onko jossakin tietyssä tapauksessa siihen liittyvien tosiseikkojen perusteella rikottu ihmisoikeuslakia, voidaan periaatteessa saattaa sellaisen riippumattoman tuomioistuimen tutkittavaksi, jolla on oikeus tutustua kaikkeen asiaa koskevaan aineistoon, myös salaiseen aineistoon. High Courtin mukaan tässä yhteydessä on myös muistettava, että myös kyseisellä tuomioistuimella on mahdollisuus hakea muutosta asianomaisesta muutoksenhakutuomioistuimesta (Englannissa ja Walesissa Court of Appeal), ja että Supreme Court on äskettäin päättänyt, että Investigatory Powers Tribunal on periaatteessa tuomioistuinvalvonnan alainen: ks. R (Privacy International) v. Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219 ([268]). Jos tuomioistuin toteaa, että jokin viranomaisen toimi on lainvastainen, se voi toimivaltuuksiensa puitteissa hyväksyä sellaisen vaatimuksen tai oikeussuojakeinon tai antaa sellaisen määräyksen, jonka se katsoo kohtuulliseksi ja asianmukaiseksi ([269]).

([261]) Tämä viittaa olosuhteisiin, joissa viranomaisten toiminta perustuu toimivaltaan (esim. viestintätietojen hankintaa koskevaan määräykseen tai lupaan), tai siihen, että kyseisissä olosuhteissa (toimivallasta riippumatta) toiminnan toteuttaminen ei olisi ollut asianmukaista ilman kyseistä toimivaltaa, tai ainakaan ilman että olisi perusteellisesti harkittu, pitäisikö tällaista toimivaltaa hakea. Kun toiminta on toteutettu oikeusvaltuutetun valtuutuksella, sen katsotaan tapahtuneen olosuhteissa, jotka on mahdollista kiistää (vuonna 2000 tutkintavaltuuksista annetun asetuksen 65 §:n 7ZA momentti). Sen sijaan muut toimet, jotka on toteutettu lainkäyttötehtävää hoitavan henkilön luvalla, katsotaan toteutetun olosuhteissa, joita ei voida kiistää (vuonna 2000 tutkintavaltuuksista annetun asetuksen 65 §:n 7 ja 8 momentti).

([262]) Yhdistyneen kuningaskunnan viranomaisten antamien tietojen mukaan se, että valituksen tekemisen kynnys on matala, johtaa siihen, että tuomioistuin katsoo tutkintansa perusteella varsin usein, että valittaja ei itse asiassa ollut milloinkaan viranomaisten tutkinnan kohteena. Investigatory Powers Tribunal -tuomioistuimen tuoreimman tilastoraportin mukaan tuomioistuimelle vuonna 2016 tehdystä 209 valituksesta 52 prosenttia katsottiin aiheettomiksi tai haitantekotarkoituksessa tehdyiksi ja 25 prosenttia päätettiin ratkaisemattomana (”no determination”). Yhdistyneen kuningaskunnan viranomaisten mukaan tämä tarkoittaa joko sitä, että valittajan suhteen ei käytetty peitetoimintaa tai sitä koskevia valtuuksia tai että tällaisia tekniikoita käytettiin, mutta tuomioistuin katsoi toiminnan olleen lainmukaista. Lisäksi 11 prosenttia tapauksista jäi tuomioistuimen toimivallan ulkopuolelle tai ne peruttiin tai niitä ei voitu ottaa tutkittavaksi, 5 prosenttia katsottiin vanhentuneiksi ja 7 prosenttia ratkaistiin valittajan eduksi. Statistical Report of the Investigatory Powers Tribunal 2016, saatavilla seuraavassa osoitteessa: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) Ks. asia Human Rights Watch v. Secretary of State [2016] UKIPTrib15_165-CH. Kyseisessä asiassa Investigatory Powers Tribunal katsoi Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön viitaten, että sellaisen väitteen todenperäisyyttä, jonka mukaan henkilö uskoo, että jokin tiedustelupalveluista on suorittanut tai että sen puolesta on suoritettu jotakin sellaista vuonna 2000 tutkintavaltuuksista annetun asetuksen 68 §:n 5 momentin soveltamisalaan kuuluvaa toimintaa, jonka vuoksi kyseinen henkilö voi väittää joutuneensa pelkästä salaisten toimenpiteiden tai salaiset toimenpiteet mahdollistavan lainsäädännön olemassaolosta johtuvan oikeudenloukkauksen uhriksi, voidaan arvioida asianmukaisesti vain jos kyseinen henkilö kykenee osoittamaan, että hänellä on henkilökohtaisen tilanteensa vuoksi voinut olla riski joutua tällaisten toimenpiteiden kohteeksi (ks. Human Rights Watch v. Secretary of State, 41 kohta).

([264]) Vuonna 2000 tutkintavaltuuksista annetun asetuksen 67 §:n 3 momentti.

([265]) Vuonna 2000 tutkintavaltuuksista annetun asetuksen 67 §:n 2 momentti.

([266]) Vuonna 2000 tutkintavaltuuksista annetun asetuksen 68 §:n 4 momentti.

([267]) Tähän voi sisältyä määräys, joka koskee minkä tahansa viranomaisen hallussa olevien ja ketä tahansa henkilöä koskevien tietojen tuhoamista.

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

([269]) Vuoden 1998 ihmisoikeuslain 8 §:n 1 momentti.

(155) Sen jälkeen kun kaikki kansalliset oikeussuojakeinot on käytetty, yksilö voi myös käyttää oikeussuojakeinoja Euroopan ihmisoikeustuomioistuimessa, jos esimerkiksi yksityisyyttä ja tietosuojaa koskevia Euroopan ihmisoikeussopimuksessa taattuja oikeuksia on loukattu.

(156) Edellä esitetystä seuraa, että kun Yhdistyneen kuningaskunnan rikosoikeudelliset lainvalvontaviranomaiset jakavat tämän päätöksen nojalla siirrettyjä tietoja muille viranomaisille, myös tiedustelupalveluille, sovelletaan rajoituksia ja ehtoja, joilla varmistetaan, että edelleen jakaminen on välttämätöntä ja oikeasuhteista ja että siihen sovelletaan vuoden 2018 tietosuojalain erityisiä tietosuojatakeita. Lisäksi asianomaisten viranomaisten suorittamaa henkilötietojen käsittelyä valvovat riippumattomat elimet, ja asianomaisilla henkilöillä on käytettävissään tehokkaat oikeussuojakeinot.

3. PÄÄTELMÄT

(157) Komissio katsoo, että vuoden 2018 tietosuojalain 3 osassa varmistetaan unionin toimivaltaisilta viranomaisilta Yhdistyneen kuningaskunnan toimivaltaisille viranomaisille rikosoikeudellisia lainvalvontatarkoituksia varten siirrettyjen henkilötietojen suojan taso, joka vastaa olennaisilta osin direktiivissä (EU) 2016/680 taattua tasoa.

(158) Lisäksi komissio katsoo, että Yhdistyneen kuningaskunnan lainsäädäntöön sisältyvät valvontamekanismit ja oikeussuojakeinot kokonaisuutena mahdollistavat sen, että henkilötietoja käsittelevän toiminnanharjoittajan tekemät rikkomukset voidaan havaita ja niistä voidaan käytännössä antaa rangaistus. Ne tarjoavat myös rekisteröidylle oikeussuojakeinoja, jotta hän voi tutustua itseään koskeviin henkilötietoihin ja korjata tai poistaa kyseiset tiedot.

(159) Yhdistyneen kuningaskunnan oikeusjärjestystä koskevien käytettävissä olevien tietojen perusteella komissio katsoo, että Yhdistyneen kuningaskunnan viranomaisten puuttuminen erityisesti lainvalvontaan ja kansalliseen turvallisuuteen liittyvissä tarkoituksissa niiden yksilöiden perusoikeuksiin, joiden henkilötietoja siirretään Euroopan unionista Yhdistyneeseen kuningaskuntaan, myös silloin, kun on kyse henkilötietojen jakamisesta lainvalvontaviranomaisten ja kansallisten turvallisuuselinten ja muiden viranomaisten välillä, tulee rajatuksi siihen, mikä on ehdottoman välttämätöntä kyseessä olevan lainmukaisen tavoitteen saavuttamiseksi, ja että tällaista puuttumista vastaan on olemassa tehokas oikeussuoja.

(160) Olisi sen vuoksi päätettävä, että Yhdistynyt kuningaskunta tarjoaa riittävän tietosuojan tason, sellaisena kuin siitä säädetään direktiivin (EU) 2016/680 36 artiklan 2 kohdassa, tulkittuna perusoikeuskirjan pohjalta.

(161) Tämä päätelmä perustuu sekä Yhdistyneen kuningaskunnan kansalliseen järjestelmään että sen kansainvälisiin sitoumuksiin, ja erityisesti siihen, että maa on liittynyt Euroopan ihmisoikeussopimukseen ja kuuluu Euroopan ihmisoikeustuomioistuimen toimivallan piiriin. Mainittujen välineiden jatkuva noudattaminen on näin ollen erityisen tärkeä osa tässä päätöksessä arvioitavaa oikeudellista kehystä.

4. TÄMÄN PÄÄTÖKSEN VAIKUTUKSET JA TIETOSUOJAVIRANOMAISTEN TOIMET

(162) Jäsenvaltioiden ja niiden elinten on toteutettava tarvittavat toimenpiteet unionin toimielinten säädösten noudattamiseksi, sillä säädösten oletetaan olevan lainmukaisia ja niillä on näin ollen oikeusvaikutuksia siihen saakka, kunnes ne perutaan, kumotaan kumoamiskanteen johdosta tai julistetaan pätemättömiksi ennakkoratkaisupyynnön tai lainvastaisuusväitteen perusteella.

(163) Näin ollen direktiivin (EU) 2016/680 36 artiklan 3 kohdan mukainen tietosuojan riittävyyttä koskeva komission päätös sitoo kaikkia elimiä jäsenvaltioissa, joille se on osoitettu, mukaan lukien niiden riippumattomat valvontaviranomaiset. Tämä tarkoittaa erityisesti sitä, että tämän päätöksen soveltamisaikana siirtoja unionin rekisterinpitäjältä tai henkilötietojen käsittelijältä Yhdistyneen kuningaskunnan rekisterinpitäjälle tai henkilötietojen käsittelijälle voidaan tehdä ilman erillistä lupaa.

(164) Samalla on kuitenkin muistettava, kuten direktiivin (EU) 2016/680 47 artiklan 5 kohdassa tunnustetaan ja unionin tuomioistuimen asiassa Schrems antamassa tuomiossa selostetaan, että jos kansallinen tietosuojaviranomainen esimerkiksi valituksen käsittelyn yhteydessä asettaa kyseenalaiseksi sen, onko tietosuojan riittävyyttä koskeva komission päätös yksityisyydensuojaa ja tietosuojaa koskevan perusoikeuden mukainen, kansallisessa lainsäädännössä on säädettävä oikeussuojakeinoista, joiden avulla viranomainen voi esittää väitteensä kansallisessa tuomioistuimessa, jonka on tarvittaessa pyydettävä unionin tuomioistuimelta ennakkoratkaisua ([270]).

([270]) Tuomio asiassa Schrems, 65 kohta.

5. TÄMÄN PÄÄTÖKSEN SEURANTA, SEN SOVELTAMISEN KESKEYTTÄMINEN TAI PÄÄTÖKSEN KUMOAMINEN TAI MUUTTAMINEN

(165) Direktiivin (EU) 2016/680 36 artiklan 4 kohdan nojalla komissio seuraa jatkuvasti asian kannalta merkityksellistä kehitystä Yhdistyneessä kuningaskunnassa tämän päätöksen hyväksymisen jälkeen voidakseen arvioida, takaako se edelleen olennaisilta osin vastaavan suojan tason. Tällainen seuranta on erityisen tärkeää tässä tapauksessa, koska Yhdistynyt kuningaskunta hallinnoi, soveltaa ja panee täytäntöön uutta tietosuojajärjestelmää, joka ei enää kuulu unionin oikeuden soveltamisalaan ja voi muuttua. Tältä osin kiinnitetään erityistä huomiota siihen, miten henkilötietojen siirtoa kolmansiin maihin koskevia Yhdistyneen kuningaskunnan sääntöjä sovelletaan käytännössä, myös tekemällä kansainvälisiä sopimuksia. Erityistä huomiota kiinnitetään myös vaikutuksiin, joita soveltamisella voi olla tämän päätöksen nojalla siirrettävien tietojen suojan tasoon, ja yksilön oikeuksien täytäntöönpanon tehokkuuteen tämän päätöksen kattamilla aloilla. Komissio hyödyntää seurannassaan muun muassa oikeuskäytännön kehitystä ja tietosuojavaltuutetun ja muiden riippumattomien elinten suorittamaa valvontaa.

(166) Seurannan helpottamiseksi Yhdistyneen kuningaskunnan viranomaisten olisi viipymättä ja säännöllisesti ilmoitettava komissiolle kaikista Yhdistyneen kuningaskunnan oikeusjärjestyksen olennaisista muutoksista, jotka vaikuttavat tämän päätöksen kohteena olevaan oikeudelliseen kehykseen, sekä tässä päätöksessä arvioitujen, henkilötietojen käsittelyä koskevien käytäntöjen muutoksista erityisesti johdanto-osan 165 kappaleessa mainittujen seikkojen osalta.

(167) Jotta komissio voisi harjoittaa tehokkaasti valvontatehtäväänsä, jäsenvaltioiden olisi lisäksi ilmoitettava komissiolle kaikista kansallisten tietosuojaviranomaisten toteuttamista asiaankuuluvista toimista, varsinkin siinä tapauksessa, että ne liittyvät EU:n rekisteröityjen esittämiin kysymyksiin tai valituksiin, jotka koskevat henkilötietojen siirtoa Euroopan unionista Yhdistyneen kuningaskunnan toimivaltaisille viranomaisille. Komissiolle olisi myös ilmoitettava havainnoista, joiden mukaan rikosten ennalta estämisestä, tutkimisesta, paljastamisesta tai rikoksiin liittyvistä syytetoimista vastaavat Yhdistyneen kuningaskunnan viranomaiset, mukaan lukien valvontaelimet, eivät varmista vaadittua suojan tasoa.

(168) Jos käytettävissä olevat tiedot, erityisesti tämän päätöksen seurannasta saatavat tiedot tai Yhdistyneen kuningaskunnan tai jäsenvaltioiden viranomaisten toimittamat tiedot, osoittavat, että Yhdistyneen kuningaskunnan takaama tietosuojan taso ei mahdollisesti ole enää riittävä, komission olisi viipymättä ilmoitettava asiasta Yhdistyneen kuningaskunnan toimivaltaisille viranomaisille ja vaadittava asianmukaisten toimenpiteiden toteuttamista tietyn ajan kuluessa, joka ei voi ylittää kolmea kuukautta. Tätä määräaikaa voidaan tarvittaessa pidentää tietyksi ajaksi käsillä olevan asian ja/tai toteutettavien toimenpiteiden luonteen mukaan.

(169) Jos Yhdistyneen kuningaskunnan toimivaltaiset viranomaiset eivät kyseisen määräajan päättyessä ole toteuttaneet näitä toimenpiteitä tai muutoin osoittaneet tyydyttävästi, että tämän päätöksen perustana on edelleen riittävä suojan taso, komissio aloittaa direktiivin (EU) 2016/680 58 artiklan 2 kohdassa tarkoitetun menettelyn tämän päätöksen soveltamisen keskeyttämiseksi tai sen kumoamiseksi osittain tai kokonaan.

(170) Vaihtoehtoisesti komissio aloittaa kyseisen menettelyn tämän päätöksen muuttamiseksi erityisesti soveltamalla tiedonsiirtoihin lisäehtoja tai rajoittamalla tietosuojan riittävyyttä koskevan päätelmän soveltamisalan vain sellaisiin tiedonsiirtoihin, joiden osalta riittävän tietosuojan jatkuvuus on varmistettu.

(171) Asianmukaisesti perustelluissa kiireellisissä tapauksissa komissio käyttää mahdollisuutta hyväksyä direktiivin (EU) 2016/680 58 artiklan 3 kohdassa tarkoitettua menettelyä noudattaen välittömästi sovellettavia täytäntöönpanosäädöksiä tämän päätöksen soveltamisen keskeyttämiseksi tai päätöksen kumoamiseksi tai sen muuttamiseksi.

6. TÄMÄN PÄÄTÖKSEN VOIMASSAOLO JA UUSIMINEN

(172) Olisi otettava huomioon, että erosopimuksessa määrätyn siirtymäkauden päättyessä ja heti kun EU:n ja Yhdistyneen kuningaskunnan välillä tehdyn kauppa- ja yhteistyösopimuksen 782 artiklan väliaikaisen määräyksen soveltaminen lakkaa, Yhdistynyt kuningaskunta hallinnoi, soveltaa ja panee täytäntöön tietosuojajärjestelmää, joka on uusi verrattuna siihen järjestelmään, joka oli käytössä silloin, kun Euroopan unionin lainsäädäntö sitoi sitä. Tämä voi tarkoittaa erityisesti tässä päätöksessä arvioidun tietosuojakehyksen tarkistamista tai muuttamista sekä muita muutoksia.

(173) Sen vuoksi on aiheellista säätää, että tätä päätöstä sovelletaan neljän vuoden ajan sen voimaantulosta alkaen.

(174) Jos erityisesti tämän päätöksen seurannasta saadut tiedot osoittavat, että Yhdistyneen kuningaskunnan takaaman tietosuojan tason riittävyyttä koskevat havainnot ovat edelleen asiallisesti ja oikeudellisesti perusteltuja, komission olisi viimeistään kuusi kuukautta ennen tämän päätöksen soveltamisen päättymistä aloitettava menettely tämän päätöksen muuttamiseksi pidentämällä sen soveltamisaikaa periaatteessa vielä neljällä vuodella. Tällaiset tämän päätöksen muuttamista koskevat täytäntöönpanosäädökset on hyväksyttävä direktiivin (EU) 2016/680 58 artiklan 2 kohdassa tarkoitetun menettelyn mukaisesti.

7. **LOPPUPÄÄTELMÄT**

(175) Euroopan tietosuojaneuvosto on julkaissut lausuntonsa ([271]), joka on otettu huomioon tätä päätöstä valmisteltaessa.

(176) Tässä päätöksessä säädetyt toimenpiteet ovat direktiivin (EU) 2016/680 58 artiklalla perustetun komitean lausunnon mukaiset.

(177) Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitetyn, Yhdistyneen kuningaskunnan ja Irlannin asemasta vapauden, turvallisuuden ja oikeuden alueen osalta tehdyssä pöytäkirjassa N:o 21 olevan 6 a artiklan mukaisesti Irlantia eivät sido direktiivissä (EU) 2016/680 ja siten tässä täytäntöönpanopäätöksessä vahvistetut säännöt, jotka koskevat jäsenvaltioiden suorittamaa henkilötietojen käsittelyä näiden toteuttaessa Euroopan unionin toiminnasta tehdyn sopimuksen kolmannen osan V osaston 4 tai 5 luvun soveltamisalaan kuuluvaa toimintaa, siltä osin kuin Irlantia eivät sido rikosasioissa tehtävän oikeudellisen yhteistyön tai poliisiyhteistyön muotoa koskevat säännöt, jotka edellyttävät Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklan perusteella vahvistettujen säännösten noudattamista. Lisäksi neuvoston täytäntöönpanopäätöksen (EU) 2020/1745 ([272]) nojalla direktiivi (EU) 2016/680 on saatettava voimaan ja sitä on sovellettava väliaikaisesti Irlannissa 1 päivästä tammikuuta 2021 lähtien. Sen vuoksi tämä täytäntöönpanopäätös sitoo Irlantia samoin edellytyksin, kuin direktiiviä (EU) 2016/680 sovelletaan Irlannissa, kuten täytäntöönpanopäätöksessä (EU) 2020/1745 säädetään, siltä osin kuin on kyse Schengenin säännöstöstä, johon Irlanti osallistuu.

(178) Euroopan unionista tehtyyn sopimukseen ja Euroopan unionin toiminnasta tehtyyn sopimukseen liitetyssä, Tanskan asemasta tehdyssä pöytäkirjassa N:o 22 olevien 2 ja 2 a artiklan mukaisesti direktiivissä (EU) 2016/680 ja siten myös tässä täytäntöönpanopäätöksessä vahvistetut säännöt eivät sido Tanskaa eikä niitä sovelleta Tanskaan, jos soveltaminen liittyy jäsenvaltioiden suorittamaan henkilötietojen käsittelyyn näiden toteuttaessa Euroopan unionin toiminnasta tehdyn sopimuksen kolmannen osan V osaston 4 tai 5 luvun soveltamisalaan kuuluvaa toimintaa. Koska direktiivi (EU) 2016/680 kuitenkin perustuu Schengenin säännöstöön, Tanska ilmoitti mainitun pöytäkirjan 4 artiklan mukaisesti 26 päivänä lokakuuta 2016 päätöksestään panna direktiivi (EU) 2016/680 täytäntöön. Sen vuoksi Tanskan on kansainväliseen oikeuteen perustuvien velvoitteiden nojalla pantava tämä täytäntöönpanopäätös täytäntöön.

(179) Islannin ja Norjan osalta tällä täytäntöönpanopäätöksellä kehitetään niitä Schengenin säännöstön määräyksiä, joita tarkoitetaan Euroopan unionin neuvoston sekä Islannin tasavallan ja Norjan kuningaskunnan välillä viimeksi mainittujen osallistumisesta Schengenin säännöstön täytäntöönpanoon, soveltamiseen ja kehittämiseen tehdyssä sopimuksessa ([273]).

(180) Sveitsin osalta tällä täytäntöönpanopäätöksellä kehitetään niitä Schengenin säännöstön määräyksiä, joita tarkoitetaan Euroopan unionin, Euroopan yhteisön ja Sveitsin valaliiton välisessä sopimuksessa Sveitsin valaliiton osallistumisesta Schengenin säännöstön täytäntöönpanoon, soveltamiseen ja kehittämiseen ([274]).

(181) Liechtensteinin osalta tällä täytäntöönpanopäätöksellä kehitetään niitä Schengenin säännöstön määräyksiä, joita tarkoitetaan Euroopan unionin, Euroopan yhteisön, Sveitsin valaliiton ja Liechtensteinin ruhtinaskunnan välisessä pöytäkirjassa, joka koskee Liechtensteinin ruhtinaskunnan liittymistä Euroopan unionin, Euroopan yhteisön ja Sveitsin valaliiton väliseen Sveitsin valaliiton osallistumisesta Schengenin säännöstön täytäntöönpanoon, soveltamiseen ja kehittämiseen tehtyyn sopimukseen ([275]),

---

([271]) Lausunto 15/2021 Euroopan komission ehdotuksesta direktiivin (EU) 2016/680 mukaiseksi täytäntöönpanopäätökseksi Yhdistyneen kuningaskunnan henkilötietojen suojan riittävyydestä, saatavilla seuraavassa osoitteessa: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en

([272]) Neuvoston täytäntöönpanopäätös (EU) 2020/1745, annettu 18 päivänä marraskuuta 2020, tietosuojaa koskevien Schengenin säännöstön määräysten voimaansaattamisesta ja tiettyjen Schengenin säännöstön määräysten väliaikaisesta voimaansaattamisesta Irlannissa (EUVL L 393, 23.11.2020, s. 3).

([273]) EYVL L 176, 10.7.1999, s. 36.

([274]) EUVL L 53, 27.2.2008, s. 52.

([275]) EUVL L 160, 18.6.2011, s. 21.

ON HYVÄKSYNYT TÄMÄN PÄÄTÖKSEN:

1 artikla

Direktiivin (EU) 2016/680 36 artiklan soveltamiseksi Yhdistyneessä kuningaskunnassa varmistetaan riittävä suoja henkilötiedoille, jotka siirretään Euroopan unionista rikosten ennalta estämisestä, tutkimisesta, paljastamisesta, rikoksiin liittyvistä syytetoimista tai rikosoikeudellisten seuraamusten täytäntöönpanosta vastaaville Yhdistyneen kuningaskunnan viranomaisille.

2 artikla

Aina kun jäsenvaltioiden toimivaltaiset valvontaviranomaiset käyttävät direktiivin (EU) 2016/680 47 artiklan mukaisia toimivaltuuksiaan suojellakseen yksilöiden henkilötietoja 1 artiklan soveltamisalaan kuuluvien Yhdistyneen kuningaskunnan viranomaisille suuntautuvien tiedonsiirtojen osalta, asianomaisen jäsenvaltion on ilmoitettava siitä komissiolle viipymättä.

3 artikla

1. Komissio seuraa jatkuvasti tämän päätöksen perustana olevan oikeudellisen kehyksen soveltamista, mukaan lukien ne edellytykset, joiden mukaisesti tietoja siirretään edelleen ja yksilön oikeuksia käytetään, sen arvioimiseksi, takaako Yhdistynyt kuningaskunta edelleen suojan riittävän tason 1 artiklassa tarkoitetussa merkityksessä.

2. Jäsenvaltiot ja komissio ilmoittavat toisilleen tapauksista, joissa tietosuojavaltuutettu tai muu Yhdistyneen kuningaskunnan toimivaltainen viranomainen laiminlyö sen varmistamisen, että tämän päätöksen perustana olevaa oikeudellista kehystä noudatetaan.

3. Jäsenvaltiot ja komissio ilmoittavat toisilleen mahdollisista havainnoista, joiden mukaan Yhdistyneen kuningaskunnan viranomaiset puuttuvat yksilöiden oikeuteen suojella henkilötietojaan suuremmassa määrin, kuin on ehdottoman välttämätöntä, tai tällaista puuttumista vastaan ei ole olemassa tehokasta oikeudellista suojaa.

4. Jos komissiolla on viitteitä siitä, että tietosuojan riittävää tasoa ei enää turvata, komissio ilmoittaa asiasta Yhdistyneen kuningaskunnan toimivaltaisille viranomaisille ja voi keskeyttää tämän päätöksen soveltamisen tai kumota sen tai muuttaa sitä.

5. Komissio voi keskeyttää tämän päätöksen soveltamisen tai kumota sen tai muuttaa sitä, jos Yhdistyneen kuningaskunnan hallituksen yhteistyöhaluttomuus estää komissiota määrittelemästä, onko asialla vaikutusta 1 artiklassa olevaan päätelmään.

4 artikla

Tämän päätöksen voimassaolo päättyy 27 päivänä kesäkuuta 2025, ellei sitä pidennetä direktiivin (EU) 2016/680 58 artiklan 2 kohdassa tarkoitetun menettelyn mukaisesti.

5 artikla

Tämä päätös on osoitettu kaikille jäsenvaltioille.

Tehty Brysselissä 28 päivänä kesäkuuta 2021.

Komission puolesta
Didier REYNDERS
Komission jäsen