A BIZOTTSÁG (EU) 2021/1773 VÉGREHAJTÁSI HATÁROZATA

(2021. június 28.)

az (EU) 2016/680 európai parlamenti és tanácsi irányelv szerint a személyes adatok Egyesült Királyság által biztosított megfelelő szintű védelméről

(az értesítés a C(2021) 4801. számú dokumentummal történt)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az említett adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló, 2016. április 27-i (EU) 2016/680 európai parlamenti és tanácsi irányelvre ([1]) és különösen annak 36. cikke (3) bekezdésére,

mivel:

1. BEVEZETÉS

(1) Az (EU) 2016/680 európai parlamenti és tanácsi rányelv meghatározza a személyes adatoknak az Unió illetékes hatóságaitól harmadik országokba és nemzetközi szervezeteknek történő átadására vonatkozó szabályokat, amennyiben az említett adattovábbítások az irányelv alkalmazási körébe tartoznak. Az illetékes hatóságok által végzett nemzetközi adattovábbítás szabályait az (EU) 2016/680 irányelv V. fejezete, pontosabban a 35–40. cikk tartalmazza. Noha a személyes adatok Európai Unión kívüli országokba és az onnan az Unióba történő áramlása elengedhetetlen a hatékony bűnüldözési együttműködéshez, garantálni kell, hogy az említett adattovábbítás ne veszélyeztesse az Európai Unióban a személyes adatok védelmi szintjét ([2]).

(2) Az (EU) 2016/680 irányelv 36. cikkének (3) bekezdése értelmében a Bizottság végrehajtási jogi aktusok útján határozhat arról, hogy a harmadik ország, a harmadik ország valamely területe, illetve egy vagy több meghatározott ágazata, illetve valamely nemzetközi szervezet biztosítja a megfelelő védelmi szintet. E feltétel szerint a személyes adatok harmadik országba történő továbbítására további engedély megszerzésének szükségessége nélkül kerülhet sor (kivéve, ha annak a másik tagállamnak, ahonnan az adatokat nyerték, engedélyt kell adnia az adattovábbításra), az (EU) 2016/680 irányelv 35. cikkének (1) bekezdésében és (66) preambulumbekezdésében előírtak szerint.

(3) Az (EU) 2016/680 irányelv 36. cikkének (2) bekezdésében meghatározottak szerint a megfelelőségi határozat elfogadásának a harmadik ország jogrendjére vonatkozó átfogó elemzésen kell alapulnia. Az értékelés során meg kell határozni, hogy az érintett harmadik ország olyan szintű védelmet biztosít-e, amely „lényegében egyenértékű” az Európai Unión belül biztosított védelem szintjével (az (EU) 2016/680 irányelv (67) preambulumbekezdése). A „lényegi egyenértékűség” értékelése az uniós jogszabályok, nevezetesen az (EU) 2016/680 irányelv, valamint az Európai Unió Bíróságának ítélkezési gyakorlata által meghatározott mércéhez képest történik ([3]). Az Európai Adatvédelmi Testület megfelelőségi referenciája ebben a tekintetben is jelentős ([4]).

(4) Az Európai Unió Bíróságának pontosítása szerint ez nem feltétlenül jelent azonos szintű védelmet ([5]). Különösen a harmadik ország által igénybe vett eszközök különbözhetnek az Európai Unióban alkalmazott eszközöktől, amennyiben – a gyakorlatban – ténylegesen megfelelő szintű védelmet biztosítanak ([6]). A megfelelőségre vonatkozó előírás ezért nem követeli meg az uniós szabályok pontról pontra történő leképezését. A vizsgálat ehelyett arra irányul, hogy a magánélet tiszteletben tartásához való jog tartalmát, hatékony végrehajtását, felügyeletét és érvényesítését tekintve az érintett harmadik ország rendszere összességében véve biztosítja-e az elvárt fokú védelmet ([7]).

([1]) HL L 119., 2016.5.4., 89. o.

([2]) Lásd az (EU) 2016/680 irányelv (64) preambulumbekezdését.

([3]) Lásd legutóbb a C-311/18. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben („Schrems II. ügy”) hozott ítéletet EU:C:2020:559.

([4]) Lásd a 2021 februárjában elfogadott, a bűnüldözési irányelv szerinti megfelelőségi referenciáról szóló 01/2021 ajánlást, amely elérhető a következő linken: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_hu

([5]) A C-362/14. sz., Maximillian Schrems kontra adatvédelmi biztos ügyben („Schrems-ügy”) hozott ítélet (EU:C:2015:650), 73. pont.

([6]) Schrems-ügy, 74. pont.

([7]) Lásd „A személyes adatok cseréje és védelme a globalizált világban” című, az Európai Parlamentnek és a Tanácsnak címzett bizottsági közleményt, (COM(2017) 7), 2017.1.10., 3.1. szakasz, 6–7. o., elérhető az alábbi helyen: https:\eur-lex.europa.eu\legal-content\HU\TXT\PDF\?uri=CELEX:52017DC0007&from=HU

(5) A Bizottság gondosan elemezte az Egyesült Királyság vonatkozó jogszabályait és gyakorlatát. Az alábbiakban kifejtett megállapításai alapján a Bizottság arra a következtetésre jut, hogy az Egyesült Királyság megfelelő szintű védelmet biztosít az (EU) 2016/680 irányelv hatálya alá tartozó, az uniós illetékes hatóságoktól az Egyesült Királyság Data Protection Act 2018 elnevezésű törvény (a 2018. évi adatvédelmi törvény) ([8]) 3. részének hatálya alá tartozó hatóságainak továbbított személyes adatok vonatkozásában.

(6) Ez a határozat azzal a következménnyel jár, hogy az említett adattovábbítások négyéves időtartamon át további engedély megszerzése nélkül történhetnek, esetleges megújítás mellett, és az (EU) 2016/680 irányelv 35. cikkében megállapított feltételek sérelme nélkül.

2. A SZEMÉLYES ADATOK ILLETÉKES HATÓSÁGOK ÁLTALI, BŰNÜLDÖZÉSI CÉLÚ KEZELÉSÉRE VONATKOZÓ SZABÁLYOK

2.1. Alkotmányos keret

(7) Az Egyesült Királyság parlamentáris demokrácia. Minden más kormányzati intézmény felett álló szuverén parlamenttel, a parlamentből választott és a parlament által elszámoltatható végrehajtó hatalommal, valamint független igazságszolgáltatással rendelkezik. A végrehajtó hatalom felhatalmazását abból a képességéből nyeri, hogy képes elnyerni a megválasztott alsóház bizalmát, és elszámoltatható a parlament mindkét háza (az alsóház és a felsőház) felé, amelyek feladata a kormány ellenőrzése, valamint a törvények megvitatása és elfogadása. Az Egyesült Királyság parlamentje átruházta az egyes skóciai, walesi és észak-írországi belső ügyekben történő törvényhozás terén a felelősséget rendre a skót parlamentre, a walesi parlamentre (Senedd Cymru) és az észak-írországi parlamentre. Míg az adatvédelem az Egyesült Királyság parlamentje számára fenntartott tárgykör, azaz ugyanazon jogszabályok érvényesek az ország egész területén, az e határozat szempontjából releváns egyéb szakpolitikai területek átruházott tárgykörök. Például Skócia és Észak-Írország büntető igazságszolgáltatási rendszereit – beleértve a rendészetet (a rendőrség által végzett tevékenységeket) – a skót parlamentre és az észak-írországi parlamentre ([9]) ruházták át.

(8) Míg az Egyesült Királyságnak nincs egy rögzített konstitutív dokumentumként értelmezhető kodifikált alkotmánya, az idők során kialakultak alkotmányos elvei az ítélkezési gyakorlatból és különösen a konvenciókból eredően. Elismerik bizonyos törvények, például a Magna Carta, az 1689-es Bill of Rights és az 1998-as Human Rights Act (emberi jogi törvény) alkotmányos értékét. Az egyének alapvető jogait az alkotmány részeként, a „common law", a törvények és a nemzetközi szerződések, különösen az Egyesült Királyság részéről 1951-ben ratifikált Emberi Jogok Európai Egyezménye (EJEE) révén fejlesztették ki. Az Egyesült Királyság 1987-ben ratifikálta az Európa Tanács az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezményét (108. egyezmény) ([10]).

(9) Az 1998. évi emberi jogi törvény beépíti az EJEE-ben foglalt jogokat az Egyesült Királyság jogába. A törvény minden egyén számára biztosítja az EJEE 2–12. és 14. cikkében, valamint az első jegyzőkönyv 1–3. cikkében és a tizenharmadik jegyzőkönyv 1. cikkében – az EJEE 16–18. cikkével együttesen – biztosított alapvető jogokat és szabadságokat. Ez magában foglalja a magán- és a családi élet tiszteletben tartásához való jogot, amelynek viszont része az adatvédelemhez való jog, valamint a tisztességes eljáráshoz való jog ([11]). Különösen az EJEE 8. cikkével összhangban e jogot hatóság csak a törvényben meghatározott esetekben korlátozhatja, amikor az egy demokratikus társadalomban a nemzetbiztonság, a közbiztonság vagy az ország gazdasági jóléte érdekében, zavargás vagy bűncselekmény megelőzése, a közegészség vagy az erkölcsök védelme, avagy mások jogainak és szabadságainak védelme érdekében szükséges.

([8]) A 2018. évi adatvédelmi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésre, F. szakasz: Bűnüldözés, elérhető az alábbi linken: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) A 108. egyezmény elveit az Egyesült Királyság jogába eredetileg az 1984-es adatvédelmi törvény révén ültették át, amelyet az 1998-as adatvédelmi törvény, majd pedig az Egyesült Királyság általános adatvédelmi rendeletével együtt a 2018-as adatvédelmi törvény) váltott fel. Az Egyesült Királyság 2018-ban aláírta az egyéneknek a személyes adatok gépi feldolgozása során való védelméről szóló egyezményt módosító jegyzőkönyvet (az úgynevezett „108+ egyezmény") is, és jelenleg az egyezmény ratifikálásán dolgozik.

([11]) Az EJEE 6. és 8. cikke (lásd még az 1998. évi emberi jogi törvény 1. mellékletét).

(10) Az 1998. évi emberi jogi törvénynek megfelelően a hatóságok minden fellépésének összeegyeztethetőnek kell lennie az EJEE által garantált jogokkal ([12]). Ezenkívül az elsődleges és az alárendelt jogszabályokat olyan módon kell értelmezni és érvényre juttatni, amely e jogokkal összeegyeztethető ([13]). Amennyiben az egyén úgy ítéli meg, hogy jogait – ideértve a magánélethez és az adatvédelemhez fűződő jogokat – a hatóságok megsértették, az 1998. évi emberi jogi törvény alapján jogorvoslattal élhet az Egyesült Királyság bíróságai előtt, és végül a nemzeti jogorvoslati lehetőségek kimerítését követően az EJEE által garantált jogok megsértése esetén jogorvoslatot nyerhet az Emberi Jogok Európai Bírósága előtt.

2.2. **Az Egyesült Királyság adatvédelmi kerete**

(11) Az Egyesült Királyság 2020. január 31-én kilépett az Unióból. A Nagy-Britannia és Észak-Írország Egyesült Királyságának az Európai Unióból és az Európai Atomenergia-közösségből történő kilépéséről szóló megállapodás ([14]) alapján az uniós jogszabályok a 2020. december 31-ig tartó átmeneti időszakban alkalmazandók voltak az Egyesült Királyságban. A kilépés előtt és az átmeneti időszak alatt az Egyesült Királyságban a személyes adatok védelméről szóló jogszabályi keretet – amely szabályozza a személyes adatok illetékes hatóságok által bűncselekmények megelőzése, kivizsgálása, felderítése vagy büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából történő kezelését, a közbiztonságot fenyegető veszélyek elleni védelemre és azok megelőzésére kiterjedően – az (EU) 2016/680 irányelvet átültető 2018. évi adatvédelmi törvény releváns részei alkották.

(12) Az EU-ból való kilépés előkészítése érdekében az Egyesült Királyság kormánya elfogadta az European Union (Withdrawal) Act 2018 elnevezésű (kilépési) törvényt (kilépési törvény) ([15]), amely beépítette a közvetlenül alkalmazandó uniós jogszabályokat az Egyesült Királyság jogába, és előírta, hogy az úgynevezett „uniós jogból eredő nemzeti jogszabályok" az átmeneti időszak végét követően is érvényesek. A kilépési törvény értelmében a 2018. évi adatvédelmi törvény (EU) 2016/680 irányelvet átültető 3. része ([16]) az „uniós jogból eredő nemzeti jogszabály". A kilépési törvénnyel összhangban a módosítatlan „uniós jogból eredő nemzeti jogszabályokat" az Egyesült Királyság bíróságainak az Európai Unió Bírósága (Bíróság) vonatkozó ítélkezési gyakorlatának és az uniós jog általános elveinek megfelelően kell értelmezniük, mivel azok közvetlenül az átmeneti időszak vége előtt hatályban voltak (a továbbiakban: „megtartott uniós ítélkezési gyakorlat", illetve „az uniós jog megtartott általános elvei") ([17]).

(13) A kilépési törvény értelmében az Egyesült Királyság miniszterei hatáskörrel rendelkeznek arra, hogy jogszabályi eszközökön keresztül másodlagos jogszabályokat vezessenek be, hogy beiktassák a megtartott uniós jogszabályokba az Egyesült Királyság Unióból való kilépéséből következő módosításokat. A Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 elnevezésű jogszabály (a kilépéssel kapcsolatos adatvédelmi szabályozás) ([18]) jelentette e hatáskör gyakorlását. Módosítja az Egyesült Királyság adatvédelmi jogszabályait, beleértve a 2018. évi adatvédelmi törvényt is, a hazai környezetnek megfeleltetés céljából ([19]).

([12]) Az 1998. évi emberi jogi törvény 6. szakasza.

([13]) Az 1998. évi emberi jogi törvény 3. szakasza.

([14]) Megállapodás Nagy-Britannia és Észak-Írország Egyesült Királyságának az Európai Unióból és az Európai Atomenergia-közösségből történő kilépéséről, 2019/C 384I/01, XT/21054/2019/INIT, HL C 384I., 2019.11.12., 1. o., („kilépési megállapodás"), elérhető a következő linken: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=HU

([15]) A 2018. évi kilépési törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) A 2018. évi adatvédelmi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) A 2018. évi kilépési törvény 6. szakasza.

([18]) A Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 elnevezésű jogszabály a következő linken érhető el: https://www.legislation.gov.uk/uksi/2019/419/contents/made, a 2020. évi kilépéssel kapcsolatos adatvédelmi törvénnyel módosított változata az alábbi linken érhető el: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) A kilépéssel kapcsolatos szabályozás számos módosítást eszközöl a 2018. évi adatvédelmi törvény 3. részében. Ezek közül sok technikai változás, például a „tagállamra" vagy a „bűnüldözési irányelvre" történő hivatkozások törlése (lásd például a 2018. évi adatvédelmi törvény 48. szakaszának (8) bekezdését vagy 73. szakaszát (5) bekezdés a) pontját, amelybe a „nemzeti jog" hivatkozás került), így a 3. rész az átmeneti időszak lejárata után ténylegesen belső jogként működik. Egyes helyeken más típusú változásokra volt szükség, például azzal kapcsolatban, hogy az Egyesült Királyság adatvédelmi jogszabályi keretrendszere alkalmazásában „ki", azaz az Európai Bizottság helyett a miniszter fogad el „megfelelőségi határozatokat" (lásd a 2018. évi adatvédelmi törvény 74A. szakaszát).

(14) Következésképpen a személyes adatok illetékes hatóságok által bűncselekmények megelőzése, kivizsgálása, felderítése vagy büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából történő kezelésére vonatkozó jogi előírásokat – az Egyesült Királyságban a közbiztonságot fenyegető veszélyek elleni védelemre és azok megelőzésére kiterjedően – a kilépési megállapodás szerinti átmeneti időszak után továbbra is a 2018. évi adatvédelmi törvény vonatkozó részei fogják meghatározni, de a kilépéssel kapcsolatos adatvédelmi szabályozás, különösen az említett törvény 3. része által módosított formában. Az Egyesült Királyság általános adatvédelmi rendelete nem vonatkozik az említett típusú adatkezelésre.

(15) A 2018. évi adatvédelmi törvény 3. része a személyes adatok bűnüldözési célú kezelésének szabályait tartalmazza, ideértve az adatvédelem elveit, az adatkezelés jogalapjait (jogszerűség), az érintettek jogait, az illetékes hatóságokat adatkezelőként terhelő kötelezettségeket és az adattovábbításra vonatkozó korlátozásokat. Ugyanakkor a bűnüldözési ágazatra alkalmazandó felügyeletre, végrehajtásra és jogorvoslatra vonatkozó szabályokat a 2018. évi adatvédelmi törvény 5. és 6. része tartalmazza.

(16) Ezen túlmenően, figyelemmel a rendőrségnek a bűnüldözési ágazatban betöltött szerepére, fontolóra kell venni a rendészeti tevékenységre vonatkozó szabályokat. Mivel a rendészet decentralizált ügy, arra eltérő, de tartalmuk szerint gyakran hasonló jogszabályok vonatkoznak a) Angliában és Walesben, b) Skóciában és c) Észak-Írországban ([20]). Ezenkívül a különféle útmutató dokumentumok további pontosítást nyújtanak a rendőrség hatáskörei felhasználási módjaira vonatkozóan. A rendőrségnek szóló útmutatóknak három fő formája létezik: 1) jogszabályok, például az Etikai Kódex alapján kiadott törvényi útmutatás ([21]) és az 1996-os rendőrségi törvény ([22]) alapján kiadott, rendőrségi információkezelés gyakorlati kódexe ([23]) vagy a rendőrségről és büntetőügyekben történő bizonyításfelvételről szóló törvény ([24]) alapján kiadott, a rendőrségi törvényhez készült kódexek ([25]), 2) a rendőrségi információk kezelésének a Rendészeti Főiskola által kiadott, engedélyezett szakmai gyakorlata (APP-útmutató a rendőrségi információk kezeléséhez) ([26]), és 3) működési útmutatók (maga a rendőrség adja ki). A Rendőrfőkapitányok Országos Tanácsa (az összes brit rendőri erő koordináló testülete) operatív útmutatókat tesz közzé, amelyeket a teljes rendőrség elfogad, és ezért országosan érvényesülnek ([27]). Ennek az útmutatónak az a célja, hogy biztosítsa az információkezelés terén a rendőri egységek következetes gyakorlatát ([28]).

(17) A rendőrségi információkezelés gyakorlati kódexét a miniszter 2005-ben adta ki, az 1996. évi rendőrségi törvény 39A. szakaszában előírt hatáskörök felhasználásával ([29]). A rendőrségi törvény alapján kiadott bármely gyakorlati kódexhez a miniszter jóváhagyása szükséges, és a Parlament elé terjesztése előtt konzultálni kell a Nemzeti Bűnügyi Ügynökséggel. A rendőrségi törvény 39A. szakaszának (7) bekezdése előírja, hogy a rendőrség vegye kellően

([20]) Az Egyesült Királyság rendőri erőivel és hatásköreikkel kapcsolatos részletesebb magyarázatot lásd: Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésre, F. szakasz: A bűnüldözés (lásd a 9. lábjegyzetet).

([21]) A rendészeti szakma angliai és walesi szakmai magatartási elveire és szabványaira vonatkozó gyakorlati kódex, amely a következő linken érhető el: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Észak-Írország rendőrségének etikai kódexe, amely a következő linken érhető el: https://www.nipolicingboard.org.uk/psni-code-ethics; a skóciai rendészeti etikai kódex a következő linken érhető el: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) A 1996. évi rendőrségi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/1996/16/contents

([23]) A rendőrségi információk kezelésének gyakorlati kódexe, amely a következő linken érhető el: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([24]) Police and Criminal Evidence Act 1984, elérhető az alábbi linken: https://www.legislation.gov.uk/ukpga/1984/60/contents

([25]) A Police and Criminal Evidence Act 1984 (rendőrségi törvény) gyakorlati kódexei a következő linken érhetők el: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([26]) A rendőrségi információk kezelésének engedélyezett szakmai gyakorlata, amely a következő linken érhető el: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Adatvédelmi kézikönyv rendőrségi adatvédelmi szakemberek számára, elérhető az alábbi linken: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) Például a rendőrségi információkezelés gyakorlati kódexe (lásd a 22. lábjegyzetet) vonatkozik a rendőri operatív információk megőrzésére (lásd e határozat (47) preambulumbekezdését).

([29]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint a megfelelőségi tárgyalások időtartama alatt a Rendészeti Főiskolán folyamatban volt a rendőrségi információkezelés gyakorlati kódexe helyébe lépő információs és iratkezelési gyakorlati kódex kidolgozása. A kódex tervezetét 2021. január 25-én tették közzé nyilvános konzultációra, és a következő linken érhető el: https://www.college.police.uk/article/information-records-management-consultation

figyelembe a törvény alapján kiadott kódexeket, ezért a rendőrség várhatóan betartja azokat ([30]). Sőt, a nem jogszabályi útmutatóknak (mint amilyen az APP-útmutató a rendőrségi információk kezeléséhez) mindig összhangban kell lenniük a rendőrségi információkezelés gyakorlati kódexével, amely azok felett áll ([31]). Mindenesetre, bár vannak olyan operatív helyzetek, amikor a rendőröknek el kell térniük ettől az útmutatótól, továbbra is meg kell felelniük a 2018. évi adatvédelmi törvény 3. része követelményeinek ([32]).

(18) Az Egyesült Királyság adatvédelmi jogszabályairól a bűnüldözési ágazatban történő adatkezeléssel kapcsolatban további információkat az információügyi biztos (Information Commissioner – ICO, a továbbiakban: biztos) nyújt ([33]) (a biztossal kapcsolatos további részletekért lásd a (93)–(109) preambulumbekezdést). Noha jogilag nem kötelező érvényű, bírósági eljárásban a bíróságok kötelesek lesznek figyelembe venni az útmutató megsértését, mivel értelmezési súlya van, és bemutatja, hogy a biztos az adatvédelmi jogszabályokat a gyakorlatban miként értelmezi és hajtja végre ([34]).

(19) Végül, amint az a (8)–(10) preambulumbekezdésben szerepel, az Egyesült Királyság bűnüldöző szerveinek biztosítaniuk kell az (EJEE) és a 108. egyezmény betartását.

(20) Felépítésében és fő alkotóelemeiben az Egyesült Királyság bűnüldöző hatóságai által végzett adatkezelésre vonatkozó jogi keret tehát nagyon hasonló az EU-ban alkalmazotthoz. Ennek része az a tény, hogy az említett keretrendszer nem csak a nemzeti jogban meghatározott, az uniós jog által kialakított kötelezettségekre támaszkodik, hanem a nemzetközi jogban rögzített kötelezettségekre is, különösen az EJEE és a 108. egyezmény Egyesült Királyság általi betartása, valamint az Emberi Jogok Európai Bírósága joghatóságának való alávetése révén. Ezek a jogilag kötelező érvényű nemzetközi okmányokból eredő, nevezetesen a személyes adatok védelme tekintetében fennálló kötelezettségek ezért az e határozatban értékelt jogi keret kiemelt jelentőségű elemét képezik.

2.3. **Tárgyi és területi hatály**

(21) A 2018. évi adatvédelmi törvény 3. részének tárgyi hatálya egybeesik az (EU) 2016/680 irányelv 2. cikkének (2) bekezdésében meghatározott hatállyal. A 3. rész vonatkozik a személyes adatok illetékes hatóságok általi, részben vagy egészben automatizált módon történő kezelésére, valamint az illetékes hatóságok által a ténylegesen a nyilvántartási rendszer részét képező vagy abba szánt személyes adatok nem automatizált kezelésére.

(22) Ezenkívül ahhoz, hogy az adatkezelő az említett 3. rész hatálya alá kerüljön, „illetékes hatóságnak" kell lennie, és az adatkezelést „bűnüldözési célból" kell végeznie. Ezért az e határozatban értékelt adatvédelmi rendszer ezen illetékes hatóságok valamennyi bűnüldözési tevékenységére irányadó.

(23) „Illetékes hatóság" az adatvédelmi törvény 30. szakaszának fogalommeghatározása szerint a 2018. évi adatvédelmi törvény 7. mellékletében felsorolt személy, valamint bármely más személy, amennyiben bármely bűnüldözési célból jogszabályi feladatai vannak. A 7. mellékletben felsorolt illetékes hatóságok nemcsak a rendőrséget, hanem az egész Egyesült Királyság minisztériumi kormányzati szerveit, valamint egyéb nyomozati feladatokkal rendelkező hatóságokat (pl. Commissioner for Her Majesty's Revenue and Customs – Őfelsége Adó- és Vámügyi Biztosa, a Welsh Revenue Authority – a walesi adóhatóság, a Competition and Markets Authority – Verseny- és Piacfelügyelet,

([30]) Az R kontra Commission of Police of the Metropolis (2014 EWCA Civ 585) ügyben megerősítették a rendőrségi információkezelés gyakorlati kódexének jogállását, és a Lord Justice Laws kijelentette, hogy a Metropolitan Police Commissioner (Fővárosi Rendőrbiztos) köteles figyelembe venni a rendőrségi információkezelés gyakorlati kódexét és a rendőrségi információk kezeléséhez az 1996-os rendőrségi törvény 39A. szakasza szerinti APP-útmutatót.

([31]) A rendőrséget a Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (Őfelsége Fővárosi Szabályozási, Tűzoltó és Mentőszolgálati Felügyelősége – HMICFRS) ellenőrzi, hogy megfelel-e a rendőrségi információkezelés gyakorlati kódexének.

([32]) Lásd ebben a tekintetben a Rendészeti Főiskola álláspontját az APP rendészet összes elemére vonatkozó útmutatójának betartásáról, amely elmagyarázza, hogy „az APP-nek a rendőrség szakmai testülete (a Rendészeti Főiskola) – mint a rendészeti tevékenység szakmai hivatalos forrása – adott felhatalmazást. A rendőröktől és az alkalmazottaktól elvárás az APP figyelembevétele feladataik ellátása során. Előfordulhatnak azonban olyan körülmények, amikor a testületnek jogszerű működési indoka van az APP-től való eltérésre, feltéve, hogy erre egyértelmű magyarázata van. A testületnek kell felelősséget vállalnia az abból eredő helyi és nemzeti kockázatokért, ha a nemzeti szinten elfogadott irányelvek be nem tartásával működik, és ha ennek következményeként eseményre vagy vizsgálatra kerül sor (például a Rendőrség Független Irodáján keresztül), a testület tartozik helytállási kötelezettséggel minden esetleges kockázatért", elérhető a következő linken https://www.app.college.police.uk/faq-page/

([33]) Útmutató a bűnüldözési ágazatban történő adatkezeléshez, elérhető a következő linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) Lásd a Bridges kontra Chief Constable of South Wales Police (2019 EWHC 2341 (Admin)) ügyet, amennyiben a Legfelsőbb Bíróság a biztos útmutatója nem jogszabályi jellegének megállapítása mellett kijelentette, hogy „annak mérlegelésekor, hogy az adatkezelő eleget tett-e a 64. szakaszban foglalt kötelezettségnek [adatvédelmi hatásvizsgálat a magas kockázatú adatkezeléssel kapcsolatban] a Számvevőszék figyelembe veszi az információügyi biztos által az adatvédelmi hatásvizsgálatokkal kapcsolatban kiadott útmutatót".

Her Majesty's Land Register – Őfelsége Ingatlannyilvántartása, vagy a Nemzeti Bűnügyi Ügynökség (National Crime Agency – NCA)), ügyészségi szerveket, más büntető igazságszolgáltatási szerveket és egyéb bűnüldözési tevékenységet folytató személyeket vagy szervezeteket is magukban foglalják ([35]). A 2018. évi adatvédelmi törvény 3. része a bíróságokra is vonatkozik, amikor bírói funkcióikat gyakorolják, kivéve az érintett jogaival és a biztos általi felügyelettel kapcsolatos részeket ([36]). A 7. mellékletben szereplő illetékes hatóságok listája nem tételes, és a miniszter rendeletekkel frissítheti azt, figyelembe véve a közhivatalok szervezetében bekövetkezett változásokat ([37]).

(24) A szóban forgó adatkezelésnek „bűnüldözési célt" kell szolgálnia, amely meghatározása szerint a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása, beleértve a közbiztonságot fenyegető veszélyekkel szembeni védelmet és e veszélyek megelőzését is ([38]). Az illetékes hatóság általi, nem bűnüldözési célból történő adatkezelésre a 2018. évi adatvédelmi törvény 3. része nem vonatkozik. Ez érvényesül például akkor, amikor a Verseny- és Piacfelügyelet kivizsgálja a bűncselekménynek nem minősülő ügyeket (pl. vállalatok egyesülése). Ebben az esetben az Egyesült Királyság általános adatvédelmi rendelete a 2018. évi adatvédelmi törvény 2. részével együtt alkalmazandó, mivel a személyes adatok illetékes hatóságok általi feldolgozása nem bűnüldözési célokból történik. Annak megállapításához, hogy melyik adatvédelmi rendszer irányadó (a 2018. évi adatvédelmi törvény 3. vagy 2. része) a szóban forgó személyes adatok kezelésére, az illetékes hatóságnak, azaz az adatkezelőnek mérlegelnie kell, hogy az említett adatkezelés „elsődleges célja" a 2018. évi adatvédelmi törvény szerinti bűnüldözési célok egyike-e.

(25) Ami a 2018. évi adatvédelmi törvény 3. részének területi hatályát illeti, a 207. cikk (2) bekezdése előírja, hogy az adatvédelmi törvény a személyes adatok olyan személy tevékenységével összefüggésben történő kezelésére vonatkozik, akinek székhelye az Egyesült Királyság teljes területén belül van. Ide tartoznak Anglia, Wales, Skócia és Észak-Írország azon területeinek hatóságai, amelyek a 2018. évi adatvédelmi törvény 3. részének tárgyi hatálya alá tartoznak ([39]).

2.3.1. *A személyes adat és az adatkezelés meghatározása*

(26) A személyes adat és az adatkezelés kulcsfogalmait a 2018. évi adatvédelmi törvény 3. szakasza határozza meg, és azok az adatvédelmi törvény egészére érvényesek. A meghatározások szorosan követik az (EU) 2016/680 irányelv 3. cikkében szereplő megfelelő meghatározásokat. A 2018. évi adatvédelmi törvény értelmében személyes adat az azonosított vagy azonosítható természetes személyre vonatkozó minden adat ([40]). A 2018. évi adatvédelmi törvény 3. szakaszának (3) bekezdése szerint az a személy azonosítható, aki közvetlenül vagy közvetve beazonosítható az információk alapján, többek között névre vagy azonosítóra, vagy a személyre jellemző egy vagy több fizikai, fiziológiai, genetikai, mentális, gazdasági, kulturális vagy társadalmi identitási tényezőre hivatkozással. Az „adatkezelés" a fogalommeghatározás szerint olyan művelet vagy műveletsorozat, amelyet információkkal vagy információkészletekkel hajtanak végre, például a) gyűjtés, rögzítés, rendszerezés, strukturálás vagy tárolás; b) kiigazítás vagy átalakítás; c) visszakeresés, betekintés vagy felhasználás; d) továbbítással, terjesztéssel vagy más módon való hozzáférhetővé tétel; e) összehangolás vagy kombináció; vagy f) korlátozás, törlés vagy megsemmisítés. Ezenkívül a törvény meghatározása szerint „különleges adat kezelése" „a) a faji vagy etnikai származást, politikai véleményeket, vallási vagy filozófiai meggyőződéseket vagy szakszervezeti tagságot feltáró személyes adatok kezelése; b) genetikai adatok vagy biometrikus adatok az egyén egyedi azonosítása céljából történő kezelése; c) egészségügyi adatok kezelése; d) az egyén nemi életére vagy szexuális irányultságára vonatkozó adatok kezelése" ([41]). E tekintetben a 2018. évi adatvédelmi törvény 205. szakasza meghatározza a „biometrikus adatok" ([42]), az „egészségügyi adatok" ([43]) és „genetikai adatok" ([44]) fogalmát.

([35]) Ezek között a 2018. évi adatvédelmi törvény 7. melléklete felsorolja az ügyészségi igazgatókat, az észak-írországi ügyészség igazgatóját vagy az Információügyi Bizottságot.

([36]) A 2018. évi adatvédelmi törvény 43. szakaszának (3) bekezdése.

([37]) A 2018. évi adatvédelmi törvény 30. szakaszának (3) bekezdése. A hírszerző ügynökségek (Secret Intelligence Service – titkosszolgálat, Security Service – biztonsági szolgálat és a Government Communications Headquarters – kormányzati kommunikációs központ) nem illetékes hatóságok (lásd a 2018. évi adatvédelmi törvény 30. szakaszának (2) bekezdését) és a 2018. évi adatvédelmi törvény 3. része egyetlen tevékenységükre sem vonatkozik. Tevékenységeik a 2018. évi adatvédelmi törvény 4. részének hatálya alá tartoznak.

([38]) A 2018. évi adatvédelmi törvény 31. szakasza.

([39]) Ez annyit jelent, hogy a 2018. évi adatvédelmi törvény és ezért ez a határozat nem vonatkozik az Egyesült Királyság koronagyarmataira és az Egyesült Királyság más tengerentúli területeire, például a Falkland-szigetekre és Gibraltár területére.

([40]) Az elhunyt személyre vonatkozó személyes adatok nem tartoznak a 2018. évi adatvédelmi törvény hatálya alá.

([41]) A 2018. évi adatvédelmi törvény 35. szakaszának (8) bekezdése.

([42]) „Biometrikus adat": egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a magánszemély egyedi azonosítását, ilyen például az arckép vagy a daktiloszkópiai adat.

([43]) „Egészségügyi adat": egy természetes személy testi vagy pszichikai egészségi állapotára vonatkozó személyes adat, ideértve a magánszemély számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információkat hordoz a magánszemély egészségi állapotáról.

([44]) „Genetikai adat": egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely elsősorban az említett természetes személyből vett biológiai minta elemzéséből ered.

(27) A 2018. évi adatvédelmi törvény 32. szakasza pontosítja az „adatkezelő” és az „adatfeldolgozó” fogalmát a személyes adatok bűnüldözési célú feldolgozása összefüggésében, szorosan követve a 2016/680 irányelvben szereplő megfelelő meghatározásokat. Adatkezelő az az illetékes hatóság, amely meghatározza a személyes adatok kezelésének céljait és eszközeit. Amennyiben az adatkezelést jogszabály írja elő, az adatkezelő az az illetékes hatóság, amelyre az említett jogszabály ilyen kötelezettséget ró. Adatfeldolgozónak minősül minden olyan személy, aki az adatkezelő nevében személyes adatokat dolgoz fel (az adatkezelő munkavállalója kivételével).

2.4. **Biztosítékok, jogok és kötelezettségek**

2.4.1. *Az adatkezelés jogszerűsége és tisztességessége*

(28) A 2018. évi adatvédelmi törvény 35. szakasza szerint a személyes adatok kezelésének jogszerűnek és tisztességesnek kell lennie, az (EU) 2016/680 irányelv 4. cikke (1) bekezdésének a) pontjához hasonló módon. A 2018. évi adatvédelmi törvény 35. szakaszának (2) bekezdése szerint a személyes adatok bármely bűnüldözési célból történő kezelése csak akkor jogszerű, ha az törvényen alapul, és vagy az érintett hozzájárult az e célból történő adatkezeléshez, vagy az adatkezelés az illetékes hatóság által e célból ellátott feladat ellátásához szükséges.

2.4.1.1. Adatkezelés jogszabály alapján

(29) Az (EU) 2016/680 irányelv 8. cikkéhez hasonlóan, a 2018. évi adatvédelmi törvény 3. részének hatálya alá tartozó adatkezelés jogszerűségének biztosítása érdekében az említett adatkezelésnek „törvényen kell alapulnia”. A „jogszerű” adatkezelés a törvény, a „common law” vagy a királyi előjogok által engedélyezett ([45]) adatkezelés.

(30) Az illetékes hatóságok hatásköreit általában törvények szabályozzák, vagyis feladataikat és hatásköreiket egyértelműen meghatározzák a Parlament által elfogadott jogszabályok ([46]). Bizonyos esetekben a rendőrség, valamint a 2018. évi adatvédelmi törvény 7. függelékében felsorolt egyéb illetékes hatóságok a „common law”-ra támaszkodhatnak az adatkezeléshez ([47]). A „common law” a bíróságok határozataival létrehozott precedensek révén épült fel. A „common law” a rendőrség rendelkezésére álló hatáskörök összefüggésében releváns, amelynek e jogforrásból fakad a bűncselekmények felderítésével és megelőzésével a lakosság védelmére vonatkozó alapvető kötelessége ([48]). A

([45]) A 2018. évi adatvédelmi törvény indokolásának 181. pontja, amely a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf

([46]) A Nemzeti Bűnügyi Ügynökség például hatásköre a Crime and Courts Act 2013 elnevezésű (a bűncselekményekről és bíróságokról szóló 2013. évi) törvényből származik, amely az alábbi linken érhető el https://www.legislation.gov.uk/ukpga/2013/22/contents Hasonlóképpen, a Food Standards Agency (az Élelmezési Szabványügyi Ügynökség) hatásköreit a Food Standards Act 1999 elnevezésű (az élelmezési szabványokról szóló 1999. évi törvény írja elő, amely a következő linken érhető el https://www.legislation.gov.uk/ukpga/1999/28/contents. Egyéb példák: a Prosecution of Offenders Act 1985 elnevezésű (az elkövetők üldözéséről szóló 1985. évi) törvény, amely létrehozta a Crown Prosecution Service (királyi ügyészség) intézményét (lásd https://www.legislation.gov.uk/ukpga/1985/23/contents); a Commissioners for Revenue and Customs Act 2005 elnevezésű (a Bevételi és vámbiztosokról szóló 2005. évi) törvény hozta létre Őfelsége Adó és Vámhatóságát (lásd: https://www.legislation.gov.uk/ukpga/2005/11/contents); a Criminal Procedure (Scotland) Act 1995 elnevezésű (a büntetőeljárásokról (Skócia) szóló 1995. évi) törvény, amely létrehozta a Scottish Criminal Cases Review Commission (skót büntetőügyek felülvizsgálati bizottsága) intézményét (lásd: https://www.legislation.gov.uk/ukpga/1995/46/contents); a the Justice (Northern Ireland) Act 2002 elnevezésű (igazságszolgáltatás (Észak-Írország) 2002. évi) törvény, amely Észak-Írországban létrehozta az ügyészséget (lásd: https://www.legislation.gov.uk/ukpga/2002/26/contents) és a Súlyos Csalásokkal foglalkozó Hivatalt, amely a Criminal Justice Act 1987 elnevezésű (a büntető igazságszolgáltatásról szóló 1987. évi) törvény alapján kapta hatásköreit (lásd: https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Például az Egyesült Királyság hatóságai által szolgáltatott információk szerint a skóciai ügyekben eljáró Crown Office és Procurator Fiscal Service keretein belül a Lord Advocate (a skóciai büntetőeljárási rendszer vezetője) halálesetek kivizsgálására és bűnüldözésre vonatkozó hatáskörét a „common law”-ból származtatja, noha feladatai egy részét törvény állapítja meg. Ezenkívül a királyi, és tágabb értelemben a különféle kormányzati, minisztériumi és miniszteri hatáskörök a jogszabályok, a „common law” és a királyi előjogok kombinációjából származnak (ezek a koronát megillető „common law” hatáskörök, de azokat miniszterek gyakorolják).

([48]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésre, F. szakasz: Bűnüldözés, 8. oldal (lásd a 9. lábjegyzetet).

rendőrségnek mind „common law", mind jogalkotói hatáskörei is vannak ([49]) az említett kötelezettség végrehajtására. Amennyiben a rendőrség törvényi hatáskörrel rendelkezik, ez minden „common law" hatáskört hatálytalanít ([50]).

(31) A bíróság elismerte, hogy a rendőr „common law" hatáskörei és kötelezettségei kiterjednek „minden olyan lépésre, amely szükségesnek tűnik a béke fenntartásához, a bűncselekmények megelőzéséhez vagy a tulajdon bűncselekményektől való védelméhez" ([51]). A „common law" hatáskörök nem korlátlan hatáskörök. Számos korlátozás vonatkozik azokra, beleértve a bíróságok ([52]), valamint a jogszabályok – különösen a Human Rights Act 1998 elnevezésű (az emberi jogokról szóló 1998. évi) törvény és az Equality Act 2010 elnevezésű (egyenlőségről szóló 2010. évi) törvény ([53]) – által megállapított korlátozásokat is. Ezenkívül a 2018. évi adatvédelmi törvény 3. része alapján adatokat kezelő illetékes hatóságok esetében ez magában foglalja a „common law" hatáskörök 2018. évi adatvédelmi törvényben meghatározott követelményekkel összhangban történő gyakorlását ([54]). Ezenkívül a bármilyen típusú adatkezelés végrehajtása tekintetében hozott döntésnek figyelembe kell vennie az alkalmazandó útmutatók követelményeit, például a rendőrségi információkezelés gyakorlati kódexét, valamint az Egyesült Királyság valamely országára vonatkozó útmutatót ([55]). A kormány és az operatív rendőrség számos útmutatót ad ki annak biztosítására, hogy a rendőrök hatásköreiket a „common law" vagy a vonatkozó törvény által meghatározott keretek között gyakorolják ([56]).

(32) A királyi előjogok a „jog" egy másik elemét képviselik, és a Koronának biztosított és a végrehajtó hatalmi ág által gyakorolható bizonyos olyan hatáskörökre vonatkoznak, amelyek nem törvényen alapulnak, hanem az uralkodó szuverenitásából fakadnak ([57]). Nagyon kevés példa van arra, hogy az előjogon alapuló hatáskörök relevánsak lennének a bűnüldözéssel összefüggésben. Idetartozik például a kölcsönös jogi segítségnyújtási keretrendszer, amely

([49]) A fő rendőrségi hatáskörök (letartóztatás, házkutatás, őrizet fenntartásának engedélyezése, ujjlenyomat vétele, intim mintavétel, parancsra elfogás, kommunikációs adatokhoz való hozzáférés) rendszerét előíró legfontosabb jogszabályok a következők: i. Anglia és Wales esetében a Police and Criminal Evidence Act 1984 (a rendőrségi törvény), elérhető az alábbi linken https://www.legislation.gov.uk/ukpga/1984/60/contents (a Protection of Freedoms Act 2012 elnevezésű (a szabadságjogok védelméről szóló 2012. évi) törvénnyel (a szabadságjogok védelméről szóló törvény) módosított formában, elérhető az alábbi linken: https://www.legislation.gov.uk/ukpga/2012/9/contents) és az Investigatory Powers Act 2016 elnevezésű (a vizsgálati határkörökről szóló 2016. évi) törvény (a vizsgálati hatáskörökről szóló törvény), amely a következő linken érhető el https://www.legislation.gov.uk/ukpga/2016/25/contents), ii. Skócia esetében a Criminal Justice (Scotland) Act 2016 elnevezésű (a büntető igazságszolgáltatásról (Skócia) szóló 2016. évi) törvény, amely az alábbi linken érhető el https://www.legislation.gov.uk/asp/2016/1/contents, és a Criminal Procedure (Scotland) Act 1995 elnevezésű (a büntetőeljárásokról (Skócia) szóló 1995. évi) törvény, amely a következő linken érhető el https://www.legislation.gov.uk/ukpga/1995/46/contents) iii. Észak-Írország esetében a Police and Criminal Evidence (Northern Ireland) Order 1989 elnevezésű (Rendőrségi és bűnügyi bizonyításfelvételről (Észak-Írország) szóló 1989. évi rendelet, elérhető az alábbi linken https://www.legislation.gov.uk/nisi/1989/1341/contents

([50]) Az Egyesült Királyság hatóságai kifejtették, hogy az írott törvények elsőbbsége az Egyesült Királyságban már régóta fennáll, már egészen az Entick kontra Carrington ügy (1765 EWHC KB J98) óta, amely elismerte, hogy a végrehajtó hatalom gyakorlásának korlátai vannak, és megállapította azt az elvet, hogy az uralkodó és a kormány „common law" hatáskörei és előjogai alá vannak rendelve az ország jogának.

([51]) Lásd a Rice kontra Connolly ügyet (1966 2 QB 414).

([52]) Lásd az R(Catt) v Association of Chief police Officers ügyet (2015 AC 1065), amelyben a rendőrség egy bűncselekményt elkövető egyén információinak megszerzésére és tárolására vonatkozó hatásköreivel kapcsolatban Lord Sumption úgy ítélte meg, hogy a „common law" szerint a rendőrségnek joga van információkat rendészeti célokra, azaz tág értelemben a közrend fenntartása, valamint a bűncselekmények megelőzése és felderítése érdekében megszerezni és tárolni. Ezek a hatáskörök nem adnak felhatalmazást az információszerzés tolakodó módszereire, például a magántulajdonba történő belépésre vagy erőszakos cselekményekre (kivéve a „common law" hatáskörök alapján történő letartóztatást). A bíró úgy ítélte meg, hogy ebben az esetben a „common law" hatáskörök elegendőek ahhoz, hogy felhatalmazást adjanak a fellebbezéssel kapcsolatos nyilvános információk megszerzésére és tárolására.

([53]) Az egyenlőségről szóló 2010. évi törvény a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) A rendőrség „common law" hatásköreinek az 1998. évi adatvédelmi törvény keretében történő értékelésére példaként lásd a Bridges v the Chief Constable of South Wales Police ügyben hozott határozatot (lásd a 33. lábjegyzetet). Lásd még az eseteket Vidal-Hall kontra Google Inc. (2015 EWCA Civ 311) és a Richard kontra BBC (2018 EWHC 1837 (Ch)) ügyet.

([55]) Lásd például az észak-ír rendőrség útmutatóját az iratkezelési szolgálati utasításról, amely a következő linken érhető el: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Az Alsóház közzétett egy tájékoztató dokumentumot, amely meghatározza az angliai és walesi rendőrség legfontosabb „common law" és törvényi hatásköreit (lásd: https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). E dokumentum szerint például, míg a „korona békéjének" fenntartása, valamint az „erőszak igénybevétele a „common law"-ból származtatott hatáskör, a „feltartóztatási és motozási hatáskörök" mindig törvényből erednek. Ezenkívül a skót kormány a honlapján tájékoztatást nyújt a letartóztatáskor és a feltartóztatáskor végzett motozásra vonatkozó rendőri hatáskörről (lásd: https://www.gov.scot/policies/police/police-powers/).

([57]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint a kormány által gyakorolt előjogok közé tartozik például a szerződések megkötése és megerősítése, a diplomácia vitele, az Egyesült Királyságon belüli fegyveres erők alkalmazása a rendőrség béke fenntartásában történő támogatására.

lehetővé teszi a miniszter számára az adatok bűnüldözési célú megosztását harmadik országokkal, és az adatok ilyen módon történő megosztásának hatásköre nem mindig törvényben rögzített ([58]). A királyi előjogokat a „common law" elvei kötik ([59]) és a törvényeknek vannak alárendelve, ezért az 1998. évi emberi jogi törvény és a 2018. évi adatvédelmi törvény által előírt korlátok vonatkoznak azokra ([60]).

(33) Az (EU) 2016/680 irányelv 8. cikkéhez hasonlóan az Egyesült Királyság rendszere előírja, hogy a jogszerűség elvének való megfelelés érdekében az illetékes hatóságoknak biztosítaniuk kell, hogy amikor az adatkezelés törvényen alapul, annak akkor is „szükségesnek" kell lennie a rendvédelmi célból elvégzett feladat ellátásához. A biztos útmutatót ad e tekintetben, pontosítva, hogy „célzottan és arányosan kell megvalósítani a cél elérését. A jogszerű alap nem érvényes, ha a cél más, kevésbé beavatkozó jellegű eszközzel észszerűen megvalósítható. Nem elég azt állítani, hogy az adatkezelésre azért van szükség, mert valaki úgy döntött, hogy üzleti vállalkozását egy adott módon működteti. A kérdés az, hogy az adatkezelés szükséges-e a megjelölt cél érdekében" ([61]).

2.4.1.2. Adatkezelés az érintett „hozzájárulása" alapján

(34) Amint a (28) preambulumbekezdés említi, a 2018. évi adatvédelmi törvény 35. szakaszának (2) bekezdése lehetőséget biztosít a személyes adatok egyén „hozzájárulása" alapján történő kezelésére.

(35) A hozzájárulás azonban nem tűnik releváns jogalapnak az e határozat hatálya alá tartozó adatkezelési műveletek szempontjából. Valójában az e határozat hatálya alá tartozó adatkezelési műveletek mindig azokra az adatokra vonatkoznak, amelyeket az (EU) 2016/680 irányelv alapján egy tagállam illetékes hatósága az Egyesült Királyság illetékes hatóságának továbbított. Ezért jellemzően nem fogják magukban foglalni a hatóság és az érintettek közötti közvetlen interakción (adatgyűjtésen) alapuló típust, amely a 2018. évi adatvédelmi törvény 35. cikke (2) bekezdésének a) pontja alapján hozzájáruláson alapulhat.

(36) Noha a hozzájárulásra hagyatkozás nem tekinthető relevánsnak az e határozat alapján végzett értékelés szempontjából, a teljesség kedvéért érdemes megjegyezni, hogy a bűnüldözési környezetben az adatkezelés soha nem kizárólag hozzájáruláson alapul, mivel az illetékes hatóságnak mindig rendelkeznie kell mögöttes hatáskörrel, amely lehetővé teszi számára az adatok kezelését ([62]). Pontosabban – és hasonlatosan az (EU) 2016/680 irányelvben ([63]) megengedettekhez – ez azt jelenti, hogy a hozzájárulás további feltételként szolgál bizonyos korlátozott és specifikus adatkezelési műveletek lehetővé tételére, amelyeket egyébként nem lehetne végrehajtani, például egy gyanúsítottnak nem minősülő személy DNS-mintájának levételét és kezelését. Ebben az esetben az adatkezelésre nem kerül sor, ha a hozzájárulást nem adják meg vagy visszavonják ([64]).

([58]) E tekintetben lásd az Egyesült Királyság adattovábbítási rendszerének értékelését a (74)–(87) preambulumbekezdésben.

([59]) Lásd a Bancoult kontra Secretary of State for Foreign and Commonwealth Affairs ügyet (2008 UKHL 61), amelyben a bíróságok úgy ítélték meg, hogy az Orders in Council (a Privy Councilban a királynő által személyesen elfogadott döntések) meghozatalának előjogon alapuló hatásköre rendes bírósági felülvizsgálatnak is alávethető.

([60]) Lásd az Attorney-General kontra De Keyser's Royal Hotel Ltd. ügyet ([1920] [1920] AC 508), amelyben a bíróság úgy ítélte meg, hogy az előjogon alapuló hatáskörök nem alkalmazhatók, ha azok helyébe törvényi hatáskörök lépnek; a Laker Airways Ltd kontra Department of Trade ügy (1977 QB 643), amelyben a bíróság megállapította, hogy az előjogon alapuló hatásköröket nem lehet felhasználni az írott jog kiiktatására; az R kontra Secretary of State for the Home Department, ex p. Fire Brigades Union ügy (1995 UKHL 3), amelyben a bíróság úgy ítélte meg, hogy az előjogon alapuló hatáskörök nem alkalmazhatók abban az esetben, ha azok ellentétesek az elfogadott jogszabályokkal, még akkor sem, ha az adott elfogadott jogszabályok még nincsenek hatályban; az R (Miller) kontra Secretary of State for Exiting the European Union ügy (2017 UKSC 5), amelyben a bíróság megerősítette, hogy az írott jog képes módosítani és megszüntetni az előjogokat. A királyi előjogokon alapuló, a törvényi vagy a „common law" hatáskörök közötti kapcsolat általános áttekintését lásd az Alsóház tájékoztató dokumentumában, amely a következő linken érhető el: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) Útmutató a bűnüldözési ágazatban történő adatkezeléshez: „Mi az első elv lényege?", elérhető az alábbi linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Ez a 2018. évi adatvédelmi törvény vonatkozó rendelkezésének megfogalmazásából következik, amely szerint a személyes adatok bármely bűnüldözési célú feldolgozása csak akkor és annyiban megengedett, ha „törvényen alapul" és a) az érintett hozzájárult az e célból történő adatkezeléshez, vagy b) az adatkezelés az illetékes hatóság által e célból elvégzett feladat teljesítéséhez szükséges".

([63]) Lásd az (EU) 2016/680 rendelet (35) és (37) preambulumbekezdését.

([64]) Az Egyesült Királyság hatóságai kifejtették, hogy a hozzájárulás megfelelő alapja lehet az adatkezelésnek, ha a rendőrség DNS-mintát vesz le annak megállapításával kapcsolatban, hogy egy eltűnt személy azonos-e egy talált holttesttel. Ilyen körülmények között nem lenne helyénvaló, ha a rendőrség mintavételre kényszeríti az érintettet; ehelyett a rendőrség az egyén hozzájárulását kéri, amely szabadon megadható és bármikor visszavonható. Ha visszavonják a hozzájárulást, az adatokat már nem lehet kezelni, amennyiben új jogalapot nem állapítanak meg a minta további kezelésére (pl. az érintett gyanúsítottá vált). További példa lehet, amikor a rendőrség olyan bűncselekményt vizsgál, amelyben az áldozat (rablás, szexuális bűncselekmény, családon belüli erőszak, gyilkosság vagy más bűncselekmény áldozatának rokonai) igénybe veheti az áldozattámogató szolgálatot (ez egy független jótékonysági szervezet, amely a bűncselekmények és nyomasztó emlékű események által sújtott emberek támogatásával foglalkozik). Ilyen körülmények között a rendőrség csak akkor osztja meg a személyes adatokat, például a nevet és az elérhetőségeket az áldozattámogató szolgálattal, ha rendelkezik az áldozat hozzájárulásával.

(37) Azokban az esetekben, amikor az egyén hozzájárulása szükséges, ennek a hozzájárulásnak egyértelműnek kell lennie és annak egyértelmű megerősítő cselekményt kell tükröznie ([65]). A rendőrség köteles adatvédelmi tájékoztatót rendszeresíteni, amely tartalmazza többek között a hozzájárulás érvényes felhasználásával kapcsolatos szükséges információkat. Ezen kívül egyes rendőri szervek további anyagokat tesz közzé arról, hogy miként tartják be az adatvédelmi jogszabályokat, többek között arról, hogy miként és mikor használják fel jogalapként a hozzájárulást ([66]).

2.4.1.3. Különleges adatok kezelése

(38) „Különleges adatok kategóriáinak" kezelése esetén külön biztosítékokat kell rendszeresíteni. Ebben a tekintetben – hasonlóan az (EU) 2016/680 irányelv 10. cikkében előírtakhoz – a 2018. évi adatvédelmi törvény 3. része erősebb biztosítékokat nyújt az úgynevezett „különleges adatok kezelése" tekintetében ([67]).

(39) Az 1998. évi adatvédelmi törvény 35. szakaszának (3) bekezdése szerint az illetékes hatóságok bűnüldözési célból csak két esetben dolgozhatnak fel különleges adatokat: (1) az érintett hozzájárult a bűnüldözési célból történő adatkezeléshez, és az adatkezelő megfelelő adatvédelmi szabályzattal ([68]) rendelkezik; vagy (2) az adatkezelés szigorúan bűnüldözési célból szükséges, az adatkezelés megfelel a 2018. évi adatvédelmi törvény 8. mellékletében szereplő feltételek legalább egyikének, és az adatkezelés időpontjában az adatkezelő megfelelő adatvédelmi szabályzattal rendelkezik ([69]).

(40) Az első esetet illetően és a (38) preambulumbekezdésben kifejtettek szerint a hozzájárulásra való hivatkozás nem tekinthető relevánsnak az e határozat hatálya alá tartozó jellegű adattovábbítási helyzetben ([70]).

(41) Ha a különleges adatok kezelése nem hozzájáruláson alapul, az a 2018. évi adatvédelmi törvény 8. mellékletében felsorolt feltételek valamelyikének felhasználásával végezhető el. Ezek a feltételek a jogszabályi célból szükséges adatkezelésre vonatkoznak; az igazságszolgáltatás igazgatása; az érintett vagy más személy létfontosságú érdekeinek védelme; a gyermekek és a veszélyeztetett személyek védelme; jogi igények; bírósági cselekmények; csalás megelőzése; archiválás; amennyiben a személyes adatokat nyilvánvalóan az érintett közli. A nyilvánvaló adatközlés esetein kívül a 8. mellékletben előírt összes feltételre szigorú szükségességi vizsgálat vonatkozik. Amint azt az információügyi biztos pontosította, „ebben az összefüggésben a feltétlenül szükséges azt jelenti, hogy az adatkezelésnek egy fontos társadalmi szükséglethez kell kapcsolódnia, amelyet kevésbé beavatkozó jellegű

([65]) A 2018. évi adatvédelmi törvény 3. része alapján a személyes adatok feldolgozása alkalmazásában a „hozzájárulás" nincs külön meghatározva. A biztos útmutatót adott a „hozzájárulás" 2018. évi adatvédelmi törvény 3. része szerinti fogalmához, pontosítva, hogy annak jelentése megegyezik a GDPR-ban adott fogalommeghatározással és ahhoz igazodnia, nevezetesen, hogy „a hozzájárulást szabadon kell megadni, konkrét és tájékozott, valódi döntést kell hozni arról, hogy valaki beleegyezik-e az adatok kezelésébe" (Útmutató a bűnüldözési ágazatban történő adatkezeléshez: „Mi az első elv lényege?" (lásd a 64. lábjegyzetet) és a hozzájárulásról szóló adatvédelmi útmutató, amely a következő linken érhető el: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Lásd például a lincolnshire-i rendőrség weboldalán (lásd: https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) vagy a West Yorkshire-i rendőrség weboldalán (lásd: https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf) található tájékoztatást.

([67]) A 2018. évi adatvédelmi törvény 35. szakaszának (8) bekezdése.

([68]) A 2018. évi adatvédelmi törvény 35. szakaszának (4) bekezdése.

([69]) A 2018. évi adatvédelmi törvény 35. szakaszának (5) bekezdése.

([70]) A teljesség kedvéért érdemes megjegyezni, hogy ha az adatkezelés hozzájáruláson alapul, akkor azt szabadon kell megadni, annak konkrétnak és tájékozottnak kell lennie, és külön döntést kell hozni az adatkezelés elfogadásáról. Ezenkívül az adatkezelőnek az érintett hozzájárulása alapján történő adatkezeléskor rendelkeznie kell egy „megfelelő adatvédelmi szabályzattal" (adatkezelési szabályzat). A 2018. évi adatvédelmi törvény 42. szakasza felvázolja azokat a követelményeket, amelyeknek az adatkezelési szabályzatnak teljesítenie kell. Egyértelművé teszi, hogy a dokumentumnak legalább el kell magyaráznia az adatkezelő adatvédelmi elvek betartásának biztosítását szolgáló eljárásait, és meg kell magyaráznia az adatkezelő személyes adatok megőrzésével és törlésével kapcsolatos irányelveit. A 2018. évi adatvédelmi törvény 42. szakasza szerint ez azt jelenti, hogy az adatkezelőnek be kell mutatnia egy olyan dokumentumot, amely a) elmagyarázza az adatkezelő adatvédelmi elvek betartásának biztosítását szolgáló eljárásait; és b) ismerteti az adatkezelő érintett hozzájárulására hagyatkozva kezelt személyes adatok megőrzésével és törlésével kapcsolatos irányelveit vagy jeleznie kell az említett személyes adatok megőrzésének valószínű idejét. Különösen az adatvédelmi szabályzat előírja, hogy az adatkezelőnek az adatkezelési tevékenységek nyilvántartására vonatkozó kötelességének tiszteletben tartásakor mindig rögzítenie kell az a) és b) pontban említett elemeket. A biztos közzétett egy sablondokumentumot (Útmutató a bűnüldözési ágazatban történő adatkezeléshez: „Különleges adatok kezelésének feltételei", elérhető a következő link alatt: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) és végrehajtási intézkedéseket hozhat, ha az adatkezelők nem teljesítik ezeket a követelményeket. Az adatkezelési szabályzatot a bíróságok is vizsgálják a 2018. évi adatvédelmi törvény esetleges sérelmének vizsgálatakor. Például a legutóbbi R (Bridges) kontra Chief Constable of South Wales Police ügyben a bíróságok felülvizsgálták az adatkezelő adatkezelési szabályzatát, és megállapították, hogy az megfelelő, de további részletezés hasznos lett volna. Ennek eredményeként a dél-walesi rendőrség felülvizsgálta az adatkezelési szabályzatot és frissítette azt az információügyi biztos új iránymutatásainak megfelelően (lásd a 33 lábjegyzetet). Ezenkívül a 2018. évi adatvédelmi törvény 42. cikkének (3) bekezdése alapján az adatkezelőnek rendszeresen felül kell vizsgálnia az adatkezelési szabályzatot. Végül, további biztosítékként az adatkezelőnek a 2018. évi adatvédelmi törvény 61. szakaszában meghatározott feldolgozási tevékenységek vonatkozásában a 2018. évi adatvédelmi törvény 42. szakaszának (4) bekezdése alapján az adatkezelőre vonatkozó általános nyilvántartási kötelezettséghez képest kibővített nyilvántartást kell vezetnie az adatkezelési tevékenységekről, beleértve a kiegészítő elemeket is.

eszközökkel nem lehet észszerűen elérni” ([71]). Sőt, néhány feltételre további korlátozások vonatkoznak. Például a „jogszerű célok” és a „garanciális feltételre” (8. melléklet, 1. és 4. pont) hivatkozáskor meg kell felelni a jelentős közérdek további vizsgálatán. Ezenkívül a gyermek védelmével kapcsolatos feltételekkel (8. melléklet, 4. pont) kapcsolatban az érintettnek meghatározott életkorúnak kell lennie és veszélyeztetettnek kell minősülnie. Ezenkívül az adatkezelő csak kivételes körülmények esetén alkalmazhatja a 8. melléklet 4. pontjában előírt feltételt ([72]). Hasonlóképpen vannak korlátozások a „bírósági cselekmények” és a „csalás megelőzése” feltétel tekintetében (8. melléklet, 7., illetve 8. pont). Mindkettő csak meghatározott adatkezelőkre vonatkozik. Bírósági cselekmények esetén csak bíróság vagy más igazságügyi hatóság alkalmazhatja ezt a feltételt, csalásmegelőzés esetén pedig csak azok az adatkezelők támaszkodhatnak erre a feltételre, amelyek csalásellenes szervezetek.

(42) Végül amikor az adatkezelés a 8. mellékletben felsorolt feltételek valamelyike alapján, illetve a 2018. évi adatvédelmi törvény 42. szakaszának megfelelően történik, egy „megfelelő adatvédelmi szabályzatnak” kell léteznie – amely elmagyarázza az adatkezelő adatvédelmi elvek betartásának biztosítását szolgáló eljárásait, valamint az adatkezelő személyes adatok megőrzésére és törlésére vonatkozó irányelveit –, és kiterjesztett nyilvántartási kötelezettségek alkalmazandók.

2.4.2. *Célhoz kötöttség*

(43) A személyes adatok kezelésének konkrét célra kell történnie, és később csak olyan mértékben használhatók fel, amely az adatkezelés céljával nem összeegyeztethetetlen. Ezt az adatvédelmi elvet a 2018. évi adatvédelmi törvény 36. szakasza garantálja. Ez a rendelkezés az (EU) 2016/680 irányelv 4. cikke (1) bekezdésének b) pontjához hasonlóan előírja, hogy a) meg kell határozni a bűnüldözési célt, amelyre személyes adatokat bármely alkalommal gyűjtenek, annak egyértelműnek és jogosnak kell lennie, és b) az így összegyűjtött személyes adatokat tilos olyan módon kezelni, amely összeegyeztethetetlen azzal a céllal, amelyre azokat gyűjtötték.

(44) Ha az illetékes hatóságok bűnüldözési célból kezelnek adatokat, ez magában foglalhat archiválási, tudományos vagy történelmi kutatási és statisztikai célokat is ([73]). Ezekben az esetekben a 2018. évi adatvédelmi törvény azt is pontosítja, hogy az archiválás (vagy tudományos vagy történelmi kutatási és statisztikai célokra történő kezelés) nem megengedett, ha azt az adott érintettre vonatkozóan hozott döntések tekintetében végzik, vagy ha ez valószínűleg jelentős kárt vagy sérelmet okoz számára ([74]).

2.4.3. *Pontosság és adattakarékosság*

(45) Az adatoknak pontosnak, és adott esetben naprakésznek kell lenniük; az adatoknak az adatkezelési célokhoz képest megfelelőnek és jelentősnek kell lenniük, valamint azokkal arányban kell állniuk. Az (EU) 2016/680 irányelv 4. cikke (1) bekezdésének c), d) és e) pontjához hasonlóan, ezek az elvek biztosítottak a 2018. évi adatvédelmi törvény 37. és 38. szakaszában. Minden észszerű lépést meg kell tenni annak érdekében, hogy a pontatlan személyes adatokat ([75]) késedelem nélkül töröljék vagy

([71]) Útmutató a bűnüldözési ágazatban történő adatkezeléshez: „A különleges adatok kezelésének feltételei” (lásd a 70. lábjegyzetet).

([72]) Az adatkezelés az érintett hozzájárulása nélkül történik az alábbi esetekben: a) az érintett nem adhat hozzájárulást az adatkezeléshez; b) az adatkezelőtől észszerűen nem várható el, hogy beszerezze az érintett hozzájárulását az adatkezeléshez: c) az adatkezelést az érintett hozzájárulása nélkül kell végrehajtani, mivel az érintett hozzájárulásának megszerzése sértheti az (1) bekezdés a) pontjában említett védelem biztosítását.

([73]) Lásd a 2018. évi adatvédelmi törvény 41. szakaszának (1) bekezdését.

([74]) Lásd a 2018. évi adatvédelmi törvény 41. szakaszának (2) bekezdését.

([75]) A 2018. évi adatvédelmi törvény 205. szakasza a „pontatlan” kifejezést „helytelen vagy félrevezető” személyes adatként határozza meg. Az Egyesült Királyság hatóságai kifejtették, hogy jellemző, hogy a nyomozásokkal kapcsolatos adatok gyakran hiányosak, de ettől függetlenül lehetnek pontosak.

kijavítsák ([76]), figyelemmel arra a bűnüldözési célra, amelyre az adatkezelés folyik ([77]), valamint annak biztosítása érdekében, hogy a pontatlan, hiányos vagy már nem naprakész személyes adatokat ne továbbítsák vagy tegyék elérhetővé bűnüldözési célra ([78]).

(46) Ezenkívül, az (EU) 2016/680 irányelv 7. cikkéhez hasonlóan az Egyesült Királyság adatvédelmi rendszere előírja, hogy a tényeken alapuló személyes adatokat lehetőség szerint meg kell különböztetni a személyes értékelésen alapuló személyes adatoktól ([79]). Adott esetben és lehetőség szerint egyértelmű különbséget kell tenni az érintettek különböző kategóriáira, például gyanúsítottakra, bűncselekmény miatt elítélt személyekre, bűncselekmény áldozataira és tanúkra vonatkozó személyes adatok között ([80]).

2.4.4. *A tárolás korlátozása*

(47) Az (EU) 2016/680 irányelv 5. cikke értelmében az adatokat elvben csak addig szabad tárolni, ameddig az a személyes adatok kezelésének céljaihoz szükséges. A 2018. évi adatvédelmi törvény 39. szakasza szerint és az említett irányelv 5. cikkéhez hasonlóan tilos a bűnüldözési célokból kezelt személyes adatokat hosszabb ideig megőrizni, mint ami az adatkezelés céljához szükséges. Az Egyesült Királyság jogrendszere megköveteli, hogy megfelelő határidőket kell meghatározni a személyes adatok bármely bűnüldözési célú folyamatos tárolása szükségességének időszakos felülvizsgálatára. A személyes adatok megőrzésével kapcsolatos gyakorlatokra és az alkalmazandó határidőkre vonatkozó további szabályokat a rendőrség hatáskörét és működését szabályozó, vonatkozó jogszabályok és útmutatók határozzák meg. Például Angliában és Walesben a Rendészeti Főiskola rendőrségi információkezelés gyakorlati kódexe, valamint az APP-útmutató a rendőrségi információk kezeléséhez biztosít keretet az operatív rendészeti információk kezelésének következetes, kockázatalapú megőrzési, felülvizsgálati és megsemmisítési folyamata biztosításához ([81]). Ez a keret egyértelmű elvárásokat támaszt az egész testületben azzal kapcsolatban, hogy az információkat miként kell létrehozni, megosztani, felhasználni és kezelni az egyes rendőrségi szerveken és más ügynökségeken belül és azok között ([82]). A rendőrségtől elvárt a gyakorlati kódex betartása, és azt a Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ellenőrzi ([83]).

(48) Az észak-írországi rendőrséget (PSNI) a törvény nem kötelezi a rendőrségi információkezelés gyakorlati kódexének betartására. A 2011-ben elfogadott a rendőrségi információkezelés gyakorlati kódexének keretrendszerét azonban kiegészíti egy PSNI kézikönyv ([84]), amely irányelveket és eljárásokat határoz meg a rendőrségi információkezelés gyakorlati kódexének Észak-Írországban történő alkalmazása módjáról.

([76]) A 2018. évi adatvédelmi törvény 38. szakasza (1) bekezdésének b) pontja.

([77]) Az Egyesült Királyság megfelelőségi megbeszélésre készített magyarázata szerint „ez biztosítja az érintettek jogainak és a bűnüldöző szervek operatív igényeinek elismerését. A fenti pontot alaposan megfontolták az adatvédelmi törvényjavaslat kidolgozási szakaszaiban, mivel lehetnek olyan konkrét és korlátozott operatív okok, amelyek miatt az adatok nem javíthatók ki. Valószínűleg ez áll fenn, ha a szóban forgó pontatlan személyes adatokat eredeti formájukban kell megőrizni bizonyítási célokra" (lásd: Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésre, F. szakasz: Bűnüldözés, 21. oldal, lásd a 9. lábjegyzetet).

([78]) A 2018. évi adatvédelmi törvény 38. szakaszának (4) bekezdése. Ezenkívül a 2018. évi adatvédelmi törvény 38. szakaszának (5) bekezdése értelmében a személyes adatok továbbítását vagy hozzáférhetővé tételét megelőzően a személyes adatok minden továbbítása során meg kell adni azokat az információkat, amelyek lehetővé teszik a címzett számára az adatok pontosságának, teljességének és megbízhatóságának felmérését, és azok aktualitásának mértékét, és ha a személyes adatok továbbítását követően derül ki, hogy az adatok helytelenek voltak, vagy az adattovábbítás jogellenes volt, akkor erről haladéktalanul értesíteni kell a címzettet.

([79]) A 2018. évi adatvédelmi törvény 38. szakaszának (2) bekezdése.

([80]) A 2018. évi adatvédelmi törvény 38. szakaszának (3) bekezdése.

([81]) Ez a keret biztosítja a kapott személyes adatok tárolásának következetességét. A felülvizsgálati időszak a bűncselekményektől függ, amelyek 4 csoportra oszthatók: 1) egyes államvédelmi kérdések; 2) egyéb szexuális erőszakos és súlyos bűncselekmények; 3) minden más bűncselekmény; 4) egyéb. További részletek az APP-útmutató a rendőrségi információk kezeléséhez című dokumentumban találhatók (lásd a 26. lábjegyzetet).

([82]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint más szervezetek szabadon követhetik a rendőrségi információkezelés gyakorlati kódexének alapelveit, ha kívánják, például a Her Majesty's Revenue and Customs and the National Crime Agency önként elfogadja a rendőrségi információkezelés gyakorlati kódexének számos alapelvét a bűnüldözés következetességének biztosítása céljából. Általánosságban elmondható, hogy a legtöbb szervezet munkatársainak konkrét irányelveket és az alkalmazottak számára útmutatókat nyújt a személyes adatok szerepkörükben történő kezelésével kapcsolatban, és az adott szervezetre szabva. Ez általában magában foglalja a kötelező képzést is.

([83]) A rendőrségi információkezelés gyakorlati kódexét az 1996-os rendőrségi törvény által biztosított hatáskörök felhasználásával adták ki, amely lehetővé teszi a Rendészeti Főiskola számára a rendészet hatékony működésével kapcsolatos gyakorlati kódexek kiadását. A törvény alapján kiadott bármely gyakorlati kódexhez a miniszter jóváhagyása szükséges, és a Parlament elé terjesztése előtt konzultálni kell a Nemzeti Bűnügyi Ügynökséggel. Az 1996. évi rendőrségi törvény 39A. cikkének (7) bekezdése előírja, hogy a rendőrség kellően vegye figyelembe az 1996. évi rendőrségi törvény alapján kiadott kódexeket.

([84]) PSNI kézikönyv a rendőrségi információkezelés gyakorlati kódexéhez, 1–6. fejezet.

(49) Skóciában a rendőrség a szabványos iratmegőrzési operatív eljárásra (szabványos operatív eljárás) ([85]) támaszkodik, amely a skóciai rendőrség iratkezelési szabályzatát ([86]) támogatja. A szabványos operatív eljárás konkrét megőrzési szabályokat határoz meg a Skóciai Rendőrség irataira vonatkozóan.

(50) A nyilvántartások felülvizsgálatára vonatkozó átfogó követelményen túlmenően – amely az Egyesült Királyság egész területén érvényesül – további részleteket a helyi szabályok tartalmaznak. Néhány példa: Anglia és Wales tekintetében a Protection of Freedom Act 2012 elnevezésű (a szabadságjogok védelméről szóló) 2012. évi törvény által módosított rendőrségről és büntetőügyekben történő bizonyításfelvételről szóló törvény rendelkezik az ujjlenyomatok és a DNS-profilok megőrzéséről, valamint külön rendszert ír elő nem elítélt személyekre ([87]). A szabadságjogok védelméről szóló törvény létrehozta a biometrikus anyagok megőrzéséért és felhasználásáért felelős biztos („a biometriáért felelős biztos") hivatalát is ([88]). Az őrizetbe vettek képeire vonatkozó konkrét szabályokat a 2017 Custody Image Review elnevezésű (az őrizetbe vettek képeinek felülvizsgálatáról szóló) 2017. évi törvény tartalmazza ([89]). Skóciát illetően a büntetőeljárásról (Skócia) szóló 1995. évi törvény tartalmazza az ujjlenyomat és biológiai minták levételének és megőrzésének szabályait ([90]). Akárcsak Anglia és Wales esetében, a jogszabályok különböző esetekre szabályozzák a biometrikus adatok megőrzését ([91]).

2.4.5. *Adatbiztonság*

(51) A személyes adatokat olyan módon kell kezelni, amely biztosítja a biztonságukat, többek között a jogosulatlan vagy jogellenes kezelés elleni védelmüket, illetve az adatok véletlen elvesztésével, megsemmisülésével vagy sérülésével szembeni védelmét. A hatóságoknak ebből a célból megfelelő technikai vagy szervezeti intézkedéseket kell hozniuk, hogy megvédjék a személyes adatokat a lehetséges veszélyektől. Ezeket az intézkedéseket a csúcstechnológia és a kapcsolódó költségek figyelembevételével kell értékelni.

(52) Ezek az elvek tükröződnek a 2018. évi adatvédelmi törvény 40. szakaszában, amely szerint – az (EU) 2016/680 irányelv 4. cikke (1) bekezdésének f) pontjához hasonlóan – a bűnüldözési célokból kezelt személyes adatokat a megfelelő biztonságot biztosító módon kell kezelni, megfelelő technikai vagy szervezési intézkedések alkalmazásával. Idetartozik az adatok védelme az illetéktelen vagy jogellenes kezeléssel, valamint a véletlen

([85]) A szabványos iratmegőrzési operatív eljárás (szabványos operatív eljárás) elérhető a következő linken: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) Az iratkezeléssel kapcsolatos további részletekért lásd a skót Nemzeti Levéltárral kapcsolatos információkat, amelyek a következő linken érhetők el: https://www.nrscotland.gov.uk/record-keeping/records-management

([87]) A megőrzési időszak attól függően változik, hogy valamely személyt elítéltek-e vagy sem (az 1984. évi rendőrségi törvény 63I–63KI. szakasza). Például egy nyilvántartandó bűncselekmény miatt elítélt felnőtt esetében az ujjlenyomatát és a DNS-profilját korlátlan ideig meg lehet őrizni (az 1984. évi rendőrségi törvény 63I. cikkének (2) bekezdése), míg a megőrzés időben korlátozott, ha az elítélt 18 év alatti, a bűncselekmény „kisebb súlyú" nyilvántartandó bűncselekmény, és az illetőt korábban nem ítélték el (az 1984. évi rendőrségi törvény 63K. szakasza). A megőrzés időtartama három év olyan személy esetében, akit letartóztattak vagy ellene vádat emeltek, de nem ítélték el (az 1984. évi rendőrségi törvény 63F. szakasza). A megőrzési idő meghosszabbítását az igazságügyi hatóságnak jóvá kell hagynia (az 1984. évi rendőrségi törvény 63F. szakaszának (7) bekezdése). Olyan személy esetében, akit letartóztattak vagy ellene vádat emeltek, de kisebb súlyú bűncselekmény miatt nem ítélték el, a megőrzés nem lehetséges (az 1984. évi rendőrségi törvény 63D. és 63H. szakasza).

([88]) A szabadságjogok védelméről 2012. évi törvény 20. szakasza létrehozza a biometriáért felelős biztos hivatalát. Egyéb feladatai mellett a biometriáért felelős biztos dönt, hogy a rendőrség megőrizheti-e a letartóztatott, de nem a megőrzésre feljogosító bűncselekménnyel vádolt személyektől nyert DNS-profil iratokat és ujjlenyomatokat (az 1984. évi rendőrségi törvény 63G. szakasza). Ezenkívül a biometriáért felelős biztos általános felelőssége a DNS és az ujjlenyomatok megőrzésének és felhasználásának, valamint nemzetbiztonsági okokból történő megőrzésének folyamatos felülvizsgálata (a szabadságjogok védelméről szóló 2012. évi törvény 20. szakaszának (2) bekezdése). A biometriáért felelős biztost a Code for Public Appointments elnevezésű (az állami kinevezések kódexéről szóló) törvény szerint nevezik ki (a kódex a következő linken érhető el: Governance Code for Public Appointments – GOV.UK (www.gov.uk)) és kinevezési feltételei egyértelművé teszik, hogy a belügyminiszter csak szűkkörűen meghatározott körülmények esetén mozdíthatja el hivatalából; idetartozik, ha kötelességei három hónapon át nem teljesíti, bűncselekmény miatt elítélik vagy kinevezésének feltételeit nem tartja be.

([89]) Az őrizetbe vettek képei felhasználásának és megőrzésének felülvizsgálata, amely a következő linken érhető el: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) A büntetőeljárásról (Skócia) szóló 1995. évi törvény 18. és rákövetkező szakaszai.

([91]) A megőrzési időszakok attól függően változnak, hogy az illetőt elítélték-e (a büntetőeljárásról (Skócia) szóló 1995. évi törvény 18. cikkének (3) bekezdése), vagy kiskorú-e. Ez utóbbi esetben a megőrzési idő a gyermekek meghallgatásán történő elítéléstől számítva 3 év (a büntetőeljárásról (Skócia) szóló 1995. évi törvény 18E. szakaszának (8) bekezdése). A letartóztatott, de el nem ítélt személyek adatait nem lehet megőrizni (az 1995. évi büntetőeljárási törvény (Skócia) 18. szakaszának (3) bekezdése), bizonyos esetek kivételével és a bűncselekmény súlyosságától függően (a büntetőeljárásról (Skócia) szóló 1995. évi törvény 18A. szakasza)). A Scottish Biometrics Commissioner Act 2020 elnevezésű (a skót biometriai biztosról szóló 2020. évi) törvény (lásd: https://www.legislation.gov.uk/asp/2020/8/contents) létrehozza a skót biometriáért felelős biztos hivatalát, akinek el kell készítenie és felül kell vizsgálnia a biometrikus adatok büntető igazságszolgáltatási és rendőrségi célú levételével, megőrzésével, felhasználásával és megsemmisítésével kapcsolatos (a skót parlament által jóváhagyott) gyakorlati kódexeket (a biometriáért felelős skót biztosról szóló 2020. évi törvény 7. szakasza).

elvesztéssel, megsemmisüléssel vagy sérüléssel szemben ([92]). A 2018. évi adatvédelmi törvény 66. szakasza meghatározza továbbá, hogy minden adatkezelőnek és minden adatfeldolgozónak megfelelő technikai és szervezési intézkedéseket kell végrehajtania a személyes adatok kezeléséből eredő kockázatoknak megfelelő biztonsági szint biztosítása érdekében. Az indokolás szerint az adatkezelőnek értékelnie kell a kockázatokat, és ezen értékelés alapján megfelelő biztonsági intézkedéseket kell végrehajtania, például titkosítást vagy az adatok kezelését végző személyzet hozzáférési engedélyének bizonyos szintjét ([93]). Az értékelésnek figyelembe kell vennie például a feldolgozott adatok jellegét és minden egyéb olyan releváns tényezőt vagy körülményt, amely befolyásolhatja az adatkezelés biztonságát.

(53) Az adatbiztonsági elvek betartását szabályozó rendszer nagyon hasonló az (EU) 2016/680 irányelv 29–31. cikkében megállapított rendszerhez. Különösen a biztonsági intézkedések személyes adatokkal kapcsolatos olyan megsértése esetén, amelyért az adatkezelő felelős, a 2018. évi adatvédelmi törvény 67. szakaszának (1) bekezdése szerint az adatkezelőnek indokolatlan késedelem nélkül, és lehetőség szerint a jogsértésről való tudomásszerzést követő 72 órán belül köteles bejelenteni a személyes adatok megsértését az információügyi biztosnak ([94]). A bejelentési kötelezettség nem alkalmazandó, ha a személyes adatok megsértése valószínűleg nem veszélyezteti az egyének jogait és szabadságait ([95]). Az adatkezelőnek dokumentálnia kell a személyes adatok megsértésével, annak következményeivel és a megtett korrekciós intézkedésekkel kapcsolatos tényeket, amelyek lehetővé teszik az információügyi biztos számára, hogy ellenőrizze az adatvédelmi törvény betartását ([96]). Ha egy adatfeldolgozó tudomást szerez a biztonsági szabályok megsértéséről, indokolatlan késedelem nélkül értesítenie kell az adatkezelőt ([97]).

(54) A 2018. évi adatvédelmi törvény 68. szakaszának (1) bekezdése szerint, ha a személyes adatok megsértése valószínűleg nagy kockázatot jelent az egyének jogaira és szabadságaira, az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet a jogsértésről ([98]). Az értesítésnek ugyanazokat az információkat kell tartalmaznia, mint az információügyi biztos (53) preambulumbekezdésben leírt értesítésének. Ez a kötelezettség nem érvényesül, ha az adatkezelő megfelelő technikai és szervezeti védelmi intézkedéseket hajtott végre, amelyeket a jogsértés által érintett személyes adatokra alkalmaztak. Nem vonatkozik arra az esetre sem, ha az adatkezelő utólagos intézkedéseket tett, amelyek biztosítják, hogy az érintettek jogait és szabadságait érintő magas kockázat valószínűleg már nem realizálódik. Végül az adatkezelőnek nem kell értesítenie az érintettet, ha ez aránytalan erőfeszítéssel járna ([99]). Ebben az esetben az információt más ugyanolyan hatékony módon, például nyilvános közlemény útján kell az érintett számára elérhetővé tenni ([100]). Ha az adatkezelő nem tájékoztatta az érintettet a jogsértésről, az információügyi biztos az adatvédelmi törvény 67. szakasza szerint értesítést kézhezvétele után, és amennyiben megítélése szerint a jogsértés valószínűleg magas kockázatú, megkövetelheti az adatkezelőtől, hogy értesítse az érintettet a jogsértésről ([101]).

([92]) A 2018. évi adatvédelmi törvény indokolásával összhangban (lásd az 45. lábjegyzetet) az adatkezelőnek különösen az alábbiakat kell megtennie: biztonságának olyan kialakítása és megszervezése, hogy illeszkedjen a nála lévő személyes adatok jellegéhez és a biztonsági szabályok megsértéséből eredő kárhoz; annak egyértelmű meghatározása, hogy a szervezetén belül kik felelősek az információbiztonság biztosításáért; annak biztosítása, hogy megfelelő fizikai és technikai biztonsággal rendelkezzen, megbízható szabályzatokkal és eljárásokkal, valamint megbízható, jól képzett személyzettel alátámasztva; és felkészültség arra, hogy gyorsan és hatékonyan reagáljon a biztonsági szabályok bármely megsértésére.

([93]) A 2018-as adatvédelmi törvény indokolásának 221. pontja (lásd az 45. lábjegyzetet).

([94]) A 2018. évi adatvédelmi törvény 67. szakaszának (4) bekezdése előírja, hogy az értesítésnek tartalmaznia kell a személyes adatok megsértésének jellegét (lehetőség szerint az érintettek kategóriáit és hozzávetőleges számát, valamint az érintett személyesadat-rekordok kategóriáit és hozzávetőleges számát), a kapcsolattartó nevét és elérhetőségeit, a személyes adatok megsértése valószínű következményeinek leírását, valamint az adatkezelő által a személyes adatok megsértésének orvoslása érdekében tett vagy javasolt intézkedések ismertetését (ideértve a hátrányos következményeinek mérséklésére irányuló intézkedéseket).

([95]) A 2018. évi adatvédelmi törvény 67. szakaszának (2) bekezdése.

([96]) A 2018. évi adatvédelmi törvény 67. szakaszának (6) bekezdése.

([97]) A 2018. évi adatvédelmi törvény 67. szakaszának (9) bekezdése.

([98]) A 2018. évi adatvédelmi törvény 68. szakaszának (7) bekezdése szerint az adatkezelő részben vagy egészben korlátozhatja az érintettek tájékoztatását annyiban és olyan időtartamra, ameddig a korlátozás az érintettek alapvető jogaira és jogos érdekeire figyelemmel szükséges és arányos intézkedés a) hivatalos vagy jogi vizsgálat, nyomozás vagy eljárás akadályozásának elkerülése érdekében; b) a bűncselekmények megelőzése, felderítése, nyomozása vagy a vádeljárás lefolytatása, illetve a büntetőjogi szankciók végrehajtása sérelmének megelőzéséhez; c) a közbiztonság védelméhez; d) a nemzetbiztonság védelméhez; e) mások jogainak és szabadságainak védelméhez.

([99]) A 2018. évi adatvédelmi törvény 68. szakaszának (3) bekezdése.

([100]) A 2018. évi adatvédelmi törvény 68. szakaszának (5) bekezdése.

([101]) A 2018. évi adatvédelmi törvény 68. szakaszának (6) bekezdése, a 2018. évi adatvédelmi törvény 68. szakaszának (8) bekezdésében előírt korlátozásra figyelemmel.

2.4.6. *Átláthatóság*

(55) Az érintetteket tájékoztatni kell személyes adataik kezelésének főbb jellemzőiről. Ezt az adatvédelmi elvet tükrözi a 2018. évi adatvédelmi törvény 44. szakasza, amely az (EU) 2016/680 irányelv 13. cikkéhez hasonlóan előírja, hogy az adatkezelőnek általános kötelessége, hogy az érintettek számára hozzáférhetővé tegye a személyes adatok kezelésével kapcsolatos információkat (akár az információk nyilvánosság számára általánosan elérhetővé tételével, akár bármilyen más módon) ([102]). A rendelkezésre bocsátandó információk a következőket tartalmazzák: a) az adatkezelő személyazonossága és elérhetőségei; b) adott esetben az adatvédelmi tisztviselő elérhetőségei; c) azok a célok, amelyekre az adatkezelő a személyes adatokat kezeli; d) az érintettek azon jogainak megléte, hogy az adatkezelőtől kérjék a személyes adatokhoz való hozzáférést, a személyes adatok helyesbítését és a személyes adatok törlését vagy azok kezelésének korlátozását; és e) az információügyi biztoshoz panasz benyújtásának joga és a biztos elérhetőségei ([103]).

(56) Az adatkezelőnek bizonyos esetekben az érintett 2018. évi adatvédelmi törvény szerinti jogainak gyakorlása lehetővé tétele céljából (például amikor a kezelt személyes adatokat az érintett tudomása nélkül gyűjtötték) tájékoztatást kell adnia az érintettnek a következőkről: a) az adatkezelés jogalapja; b) a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai; c) adott esetben információk a személyes adatok címzettjeinek kategóriáiról (ideértve a harmadik országbeli címzetteket vagy a nemzetközi szervezeteket is); d) az érintettek 2018. évi adatvédelmi törvény 3. része szerinti jogainak gyakorlásához szükséges további információk ([104]).

2.4.7. *Az egyének jogai*

(57) Az érintetteknek számos érvényesíthető jogot kell biztosítani. A 2018. évi adatvédelmi törvény 3. részének 3. fejezete hozzáférési, helyesbítési, törlési és korlátozási jogot biztosít az egyének számára ([105]), amelyek összehasonlíthatók az (EU) 2016/680 irányelv 3. fejezetének rendelkezéseivel.

(58) A hozzáférési jog fogalmát a 2018. évi adatvédelmi törvény 45. szakasza határozza meg. Először is, az egyén jogosult annak megerősítést kérni az adatkezelőtől, hogy személyes adatait feldolgozzák-e ([106]). Másodszor, amennyiben a személyes adatokat feldolgozzák, az érintettnek joga van hozzáférni ezekhez az adatokhoz, és az adatkezelésről a következő információk kikéréséhez: a) az adatkezelés céljai és jogalapja; b) az érintett adatok kategóriái; c) a címzett, akivel az adatokat közölték; d) a személyes adatok tárolásának időtartama; e) az érintett joga személyes adatainak kijavításához és töröltetéséhez; f) panasz benyújtásának joga; és g) az érintett személyes adatok eredetére vonatkozó minden információ ([107]).

(59) A 2018. évi adatvédelmi törvény 46. szakasza értelmében az érintettnek joga van arra, hogy az adatkezelőtől megkövetelje a rá vonatkozó pontatlan személyes adatok helyesbítését. Az adatkezelőnek az adatokat indokolatlan késedelem nélkül ki kell javítania (vagy ha az adatok azért pontatlanok, mert hiányosak, ki kell egészítenie). Ha a személyes adatokat bizonyítás céljából meg kell őrizni, az adatkezelőnek (a személyes adatok helyesbítése helyett) korlátoznia kell azok kezelését ([108]).

([102]) Az Útmutató a bűnüldözési ágazatban történő adatkezeléshez című dokumentum a következő példát adja: „Webhelyükön van egy általános adatvédelmi közlemény, amely a szervezetre vonatkozó alapvető információkat, a személyes adatok kezelésének célját, az érintett jogait és az információügyi biztoshoz való panasztétel jogát tartalmazza. Értesítést kapott arról, hogy egy magánszemély bűncselekmény elkövetésekor jelen volt. A személy első meghallgatásakor meg kell adnia az általános információkat, valamint a további alátámasztó információkat, hogy lehetővé tegye jogaik gyakorlását. Csak akkor korlátozhatja az Ön által megadott adatok tisztességes kezelését, ha az hátrányosan befolyásolja az Ön által indított nyomozást." (Útmutató a bűnüldözési ágazatban történő adatkezeléshez: „Milyen tájékoztatást kell adnunk magánszemélyeknek?", elérhető az alábbi linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Az Útmutató a bűnüldözési ágazatban történő adatkezeléshez című dokumentum kimondja, hogy a személyes adatok kezeléséről adott tájékoztatásnak tömörnek, érthetőnek és könnyen hozzáférhetőnek kell lennie; világos és érthető nyelvezettel megírva, a kiszolgáltatott személyek, például a gyermekek igényeihez igazítva; és ingyenesnek kell lennie (Útmutató a bűnüldözési ágazatban történő adatkezeléshez: „Hogyan adjuk meg ezt a tájékoztatást?", elérhető az alábbi linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Lásd a 2018. évi adatvédelmi törvény 44. szakaszának (2) bekezdését.

([105]) Az érintettek jogainak részletes elemzését lásd: Útmutató a bűnüldözési ágazatban történő adatkezeléshez, az egyének jogairól, elérhető az alábbi linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) A 2018. évi adatvédelmi törvény 45. szakaszának (1) bekezdése.

([107]) A 2018. évi adatvédelmi törvény 45. szakaszának (2) bekezdése.

([108]) A 2018. évi adatvédelmi törvény 46. szakaszának (4) bekezdése.

(60) A 2018. évi adatvédelmi törvény 47. szakasza jogot biztosít az egyéneknek a törléshez és az adatfeldolgozás korlátozásához. Az adatkezelőnek indokolatlan késedelem nélkül törölnie kell ([109]) a személyes adatokat, ha a személyes adatok kezelése az adatvédelmi elvekbe, az adatkezelés jogalapjába, vagy az archiválással és a különleges adatok kezelésével kapcsolatos biztosítékokba ütközne. Az adatkezelőnek törölnie kell az adatokat is, ha erre törvényi kötelezettsége van. Ha a személyes adatokat bizonyítás céljából kell megtartani, az adatkezelőnek (a személyes adatok törlése helyett) korlátoznia kell azok kezelését ([110]). Az adatkezelőnek korlátoznia kell a személyes adatok kezelését, ha az érintett vitatja a személyes adatok pontosságát, de nem lehet megállapítani, hogy azok pontosak-e vagy sem ([111]).

(61) Amennyiben az érintett kéri a személyes adatok helyesbítését vagy törlését vagy feldolgozásuk korlátozását, az adatkezelőnek írásban tájékoztatnia kell az érintettet arról, hogy a megkeresést teljesítették-e, és ha elutasították, tájékoztatnia kell az érintettet az elutasítás okairól és a rendelkezésre álló jogorvoslati lehetőségekről (az érintett arra vonatkozó jogáról, hogy az információügyi biztoshoz forduljon a korlátozás jogszerű alkalmazásának kivizsgálásához, panaszt nyújtson be az információügyi biztoshoz, és a megfelelés elrendelése érdekében a bírósághoz fordulás jogáról) ([112]).

(62) Ha az adatkezelő egy másik illetékes hatóságtól kapott személyes adatokat helyesbít, erről értesítenie kell a másik hatóságot ([113]). Amennyiben az adatkezelő helyesbíti, törli az adatkezelő által feltárt személyes adatokat vagy korlátozza azok kezelését, az adatkezelőnek értesítenie kell a címzetteket, és a címzetteknek hasonló módon helyesbíteniük, törölniük kell a személyes adatokat vagy korlátozniuk kell azok kezelését (amennyiben a felelősség azért őket terheli) ([114]).

(63) Ezenkívül az érintettnek joga van ahhoz, hogy az adatkezelőtől indokolatlan késedelem nélkül tájékoztatást kapjon a személyes adatok megsértéséről, ha ez valószínűleg nagy kockázatot jelent az egyének jogai és szabadságai szempontjából ([115]).

(64) Az érintett valamennyi jogával kapcsolatban és az (EU) 2016/680 irányelv 12. cikkében előírtakhoz hasonlóan az adatkezelő köteles gondoskodni arról, hogy az érintettel minden információt tömören, érthetően és könnyen hozzáférhető formában ([116]) közöljön, és azt lehetőség szerint a kérelemmel megegyező formában adja meg ([117]). Az adatkezelőnek indokolatlan késedelem nélkül vagy minden esetben elvileg a kéréstől számított egy hónapos időszak vége előtt eleget kell tennie az érintett kérésének ([118]). Ha az adatkezelőnek észszerű kétségei vannak az egyén személyazonosságával kapcsolatban, további információkat kérhet, és a személyazonosság megállapításáig késleltetheti a kérés elintézését. Az adatkezelő észszerű díjat követelhet, vagy megtagadhatja az intézkedést, ha a kérést nyilvánvalóan megalapozatlannak tartja ([119]). Az információügyi biztos útmutatást adott arról, hogy a kérelem mikor minősül nyilvánvalóan megalapozatlannak vagy eltúlzottnak, és mikor lehet díjat kérni ([120]).

(65) Ezenkívül a 2018. évi adatvédelmi törvény 53. szakaszának (4) bekezdése alapján a miniszter rendelettel meghatározhatja a díj maximális összegét.

([109]) Az érintett kérheti az adatkezelőtől a személyes adatok törlését vagy azok feldolgozásának korlátozását (de az adatkezelőnek az adatok törlésére vagy feldolgozásának korlátozására vonatkozó kötelezettségei érvényesek függetlenül attól, hogy ilyen kérelmet benyújtottak-e).

([110]) A 2018. évi adatvédelmi törvény 46. szakaszának (4) bekezdése és 47. szakaszának (2) bekezdése.

([111]) A 2018. évi adatvédelmi törvény 47. szakaszának (3) bekezdése.

([112]) A 2018. évi adatvédelmi törvény 48. szakaszának (1) bekezdése.

([113]) A 2018. évi adatvédelmi törvény 48. szakaszának (7) bekezdése.

([114]) A 2018. évi adatvédelmi törvény 48. szakaszának (9) bekezdése.

([115]) A 2018. évi adatvédelmi törvény 68. szakasza.

([116]) A 2018. évi adatvédelmi törvény 52. szakaszának (1) bekezdése.

([117]) A 2018. évi adatvédelmi törvény 52. szakaszának (3) bekezdése.

([118]) A 2018. évi adatvédelmi törvény 54. szakasza meghatározza a „vonatkozó időtartam” jelentését, amely egy hónapos vagy a rendelkezésben meghatározott hosszabb időszakot jelent, a vonatkozó időponttól (amikor az adatkezelő megkapja a szóban forgó kérelmet) kezdődően; amikor az adatkezelő megkapja az adatvédelmi törvény 52. szakaszának (4) bekezdése alapján egy kéréssel kapcsolatban bekért információkat (ha van ilyen); vagy amikor az adatvédelmi törvény 53. szakasza alapján a kéréssel kapcsolatban felszámított díjat (ha van ilyen) megfizetik.

([119]) A 2018. évi adatvédelmi törvény 53. szakaszának (1) bekezdése.

([120]) Az információügyi biztos útmutatója szerint az adatkezelő dönthet úgy, hogy díjat számít fel az érintettnek, ha a kérelme nyilvánvalóan megalapozatlan vagy eltúlzott, de mégis úgy dönt, hogy választ ad arra. A díjnak észszerűnek kell lennie, és indokoltnak kell lenniük a költségekhez viszonyítva. Útmutató a bűnüldözési ágazatban történő adatkezeléshez című dokumentumban a „Nyilvánvalóan megalapozatlan és eltúlzott kérések” részt, elérhető az alábbi linken: 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. Az érintett jogainak korlátozása és az átláthatósági kötelezettségek

(66) Az illetékes hatóság bizonyos körülmények között korlátozhatja az érintett bizonyos jogait: a hozzáféréshez ([121]), a tájékoztatáshoz ([122]), a személyes adatok megsértéséről való tudomásszerzéshez ([123]), valamint arról való tájékoztatáshoz való jog, hogy a helyesbítés vagy törlés iránti kérelem elutasításának mi volt az oka ([124]). Az (EU) 2016/680 irányelv III. fejezetében foglalt rendszerhez hasonlóan az illetékes hatóság csak akkor alkalmazhatja a korlátozást, ha az az érintett alapvető jogaira és jogos érdekeire tekintettel szükséges és az alábbiak érdekében arányos: a) hivatalos vagy jogi vizsgálat, nyomozás vagy eljárás akadályozásának elkerüléséhez; b) a bűncselekmények megelőzése, felderítése, nyomozása vagy a vádeljárás lefolytatása, illetve a büntetőjogi szankciók végrehajtása sérelmének megelőzéséhez; c) a közbiztonság védelméhez; d) a nemzetbiztonság védelméhez; e) mások jogainak és szabadságainak védelméhez.

(67) Az információügyi biztos útmutatást adott e korlátozások alkalmazásáról. Ezen útmutató szerint az adatkezelőknek eseti alapon elemzést kell végezniük, hogy egyensúlyba hozzák az egyén jogait és azt a hátrányt, amelyet a közlés okozhat. Különösen indokolniuk kell az alkalmazott korlátozások szükségességét és arányosságát, és csak akkor korlátozhatják a rendelkezéseket, ha az sérti a fent említett célokat ([125]).

(68) Számos egyéb, az illetékes hatóságok által kiadott útmutató is létezik, amelyek részletes tájékoztatást nyújtanak az adatvédelmi jogszabályok minden vonatkozásáról, ideértve az érintettek jogaira ([126]) korlátozás alkalmazását is. Például a 45. szakasz (4) bekezdésével kapcsolatban az országos rendőrfőkapitány jogtanácsosának adatvédelmi kézikönyve kimondja: „Fontos megjegyezni, hogy a korlátozások csak a szükséges mértékben, és csak a szükséges ideig alkalmazhatók. Következésképpen a kérelmező összes személyes adatára vonatkozó korlátozás vagy állandó korlátozás alkalmazása nem megengedett. Ez utóbbi vonatkozásban gyakran előfordul, hogy egy nyomozás gyanúsítottjának minősülő érintett tudomása nélkül gyűjtött személyes adatokat először védeni kell közlés ellen a nyomozás folyamán a nyomozás sérelmének megelőzése érdekében, de egy későbbi időpontban nem okozna hátrányt a közlés, ha a személyes adatokat a kihallgatás során közölnék az egyénnel. A rendőrségnek olyan eljárásokat kell elfogadnia, amelyek biztosítják, hogy e korlátozások csak a szükséges mértékben és csak a szükséges időtartamig érvényesüljenek” ([127]). Ez az útmutató példákat is tartalmaz arra vonatkozóan, hogy az egyes korlátozásokra mikor kerülhet sor ([128]).

(69) Ezenkívül a fent említett jogok bármelyikének a „nemzetbiztonság” védelme érdekében történő korlátozásának lehetősége kapcsán az adatkezelő kérhet a miniszter vagy a legfőbb ügyész (vagy a skóciai főügyész) által aláírt tanúsítványt), amely tanúsítja, hogy az említett jogok korlátozása szükséges és arányos intézkedés a nemzetbiztonság védelme érdekében ([129]). Az Egyesült Királyság kormánya útmutatót adott ki a nemzetbiztonsági tanúsítványokról a 2018. évi adatvédelmi törvény alapján, amely különösen kiemeli, hogy az érintettek jogainak korlátozásának arányosnak és szükségesnek kell lennie a nemzetbiztonság védelme érdekében ([130]) (a nemzetbiztonsági tanúsítványokról bővebben lásd a (131)–(134) preambulumbekezdést).

([121]) A 2018. évi adatvédelmi törvény 45. szakaszának (4) bekezdése.
([122]) A 2018. évi adatvédelmi törvény 44. szakaszának (4) bekezdése.
([123]) A 2018. évi adatvédelmi törvény 68. szakaszának (7) bekezdése.
([124]) A 2018. évi adatvédelmi törvény 48. szakaszának (3) bekezdése.
([125]) Lásd például az Útmutató a bűnüldözési ágazatban történő adatkezeléshez című dokumentum a hozzáférési jogról, amely a következő linken érhető el: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) Lásd például az Országos Rendőr-főkapitányság által kiadott, Adatvédelmi kézikönyv a rendőrség adatvédelmi szakembereinek számára című dokumentumot (lásd a 27. lábjegyzetet) vagy a Súlyos Csalásokkal foglalkozó Hivatal által készített útmutatót, amely a következő linken érhető el: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) Az országos rendőrség vezető jogtanácsosának adatvédelmi kézikönyve, 140. oldal (lásd a 27. lábjegyzetet).
([128]) Az Országos Rendőr-főkapitányság vezető jogtanácsosának adatvédelmi kézikönyve előírja, hogy „a hivatalos vagy jogi vizsgálat, nyomozás vagy eljárás akadályozásának megelőzése” valószínűleg releváns a vizsgálatok, a családjogi bíróság eljárásai, a nem büntetőjogi belső fegyelmi vizsgálatok során kezelt személyes adatok, és olyan vizsgálatok vonatkozásában, mint a gyermekek szexuális zaklatásával kapcsolatos független vizsgálat; míg a „mások jogainak és szabadságainak védelme” olyan személyes adatok vonatkozásában releváns, amelyek más személyekre és a kérelmezőre is vonatkozhatnak”(az Országos Rendőr-főkapitányság adatvédelmi kézikönyve, 140. oldal, lásd a 27. lábjegyzetet).
([129]) A 2018. évi adatvédelmi törvény 79. szakasza.
([130]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, amely a következő linken érhető el: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

(70) Ezenkívül, ha az érintett jogainak korlátozása érvényesül, az illetékes hatóságnak indokolatlan késedelem nélkül tájékoztatnia kell az érintettet jogainak korlátozásáról, a korlátozás okairól és a rendelkezésre álló jogorvoslati lehetőségekről, kivéve, ha az információ rendelkezésre bocsátása aláásná a korlátozás alkalmazásának okát ([131]). A korlátozásokkal való visszaélések elleni további biztosítékként az adatkezelőnek rögzítenie kell a tájékoztatás korlátozásának okait, és kérésre a nyilvántartást az információügyi biztos rendelkezésére kell bocsátania ([132]).

(71) Ha az adatkezelő megtagadja az átláthatóságra vonatkozó további tájékoztatás nyújtását vagy a hozzáférést, vagy elutasítja az adatkezelés helyesbítésére, törlésére vagy korlátozására vonatkozó kérést, az egyén kérheti az információügyi biztostól annak vizsgálatát, hogy az adatkezelő jogszerűen alkalmazta-e a korlátozást ([133]). Az érintett személy panasszal fordulhat az információügyi biztoshoz, vagy bírósághoz fordulhat, hogy az kötelezze az adatkezelőt a kérelem teljesítésére ([134]).

2.4.7.2. Automatizált döntéshozatal

(72) A 2018. évi adatvédelmi törvény 49. az automatizált döntéshozatalhoz kapcsolódó jogokat, az 50. szakasza az alkalmazandó biztosítékokat rendezi ([135]). Az (EU) 2016/680 irányelv 11. cikkéhez hasonlóan az adatkezelő csak akkor hozhat kizárólag a személyes adatok automatizált feldolgozásán alapuló jelentős döntést, ha ezt törvény előírja vagy engedélyezi ([136]). A döntés akkor jelentős, ha az érintettre nézve hátrányos joghatással járna, vagy jelentősen érintené az érintettet ([137]).

(73) Ha az adatkezelő számára törvény írja elő vagy engedélyezi jelentős döntés meghozatalát, a 2018. évi adatvédelmi törvény 50. szakasza meghatározza azokat a biztosítékokat, amelyek egy ilyen döntés esetében alkalmazandók (amelyet „minősített jelentős döntésként" határoznak meg). Az adatkezelőnek a lehető leghamarabb értesítenie kell az érintettet arról, hogy ilyen döntés született. Az érintett ezután egy hónapon belül kérheti az adatkezelőt, hogy vizsgálja felül a döntést, vagy hozzon olyan új döntést, amely nem kizárólag automatizált feldolgozáson alapul. Az adatkezelőnek mérlegelnie kell a kérést, és tájékoztatnia kell az érintettet a mérlegelés eredményéről. A 2018. évi adatvédelmi törvény felhatalmazza a minisztert a további biztosítékokról szóló szabályozás elfogadására ([138]). Még nem fogadtak el ilyen szabályozást.

2.4.8. *Adattovábbítás harmadik fél részére*

(74) A valamely tagállam bűnüldöző hatóságától az egyesült királyságbeli bűnüldöző hatóságnak továbbított személyes adatok védelmének szintjét nem veszélyeztetheti az említett adatok Egyesült Királyságon kívüli harmadik országokban található adatátvevők részére történő továbbítása. Az említett „újbóli adattovábbítás", amely az egyesült királyságbeli adatkezelők vagy adatfeldolgozók szemszögéből Egyesült Királyságból történő nemzetközi adattovábbításnak minősül, csak abban az esetben engedélyezett, ha az Egyesült Királyságon kívüli újabb adatátvevőre olyan szabályok vonatkoznak, amelyek biztosítják az Egyesült Királyság jogrendje szerint biztosított védelem szintjéhez hasonló szintű védelmet.

([131]) A 44. szakasz (5) és (6) bekezdése: a 45. szakasz (5) és (6) bekezdése; A 2018. évi adatvédelmi törvény 48. szakaszának (4) bekezdése.
([132]) 44. szakasz (7) bekezdése; a 45. szakasz (7) bekezdése; a 2018. évi adatvédelmi törvény 48. szakaszának (6) bekezdése.
([133]) A 2018. évi adatvédelmi törvény 51. szakasza.
([134]) A 2018. évi adatvédelmi törvény 167. szakasza.
([135]) Az automatizált feldolgozás körét illetően a 2018. évi adatvédelmi törvény indokolása kimondja: „Ezek a rendelkezések a teljesen automatizált döntéshozatalhoz kapcsolódnak, és nem az automatizált adatfeldolgozáshoz. Automatizált adatfeldolgozás (ideértve a profilalkotást is) az, amikor az adatokon emberi beavatkozás nélkül végeznek valamely műveletet. Rendszeresen használják a bűnüldözésben a nagy adathalmazok emberi operátor által használható, kezelhető mennyiségre történő szűrésére. Az automatizált döntéshozatal az automatizált feldolgozás egyik formája, és ahhoz a végső döntést emberi beavatkozás nélkül kell meghozni". (Az adatvédelmi törvény magyarázata, 204. bekezdés, lásd az 45. lábjegyzetet).
([136]) Az adatvédelmi törvényben nyújtott védelem mellett az Egyesült Királyság jogi keretében vannak más olyan jogszabályi korlátozások is, amelyek a bűnüldöző szervekre vonatkoznak és céljuk az illegális hátrányos megkülönböztetést eredményező automatizált feldolgozás (ideértve a profilalkotást is) megelőzése. Az 1998. évi emberi jogi törvény beépíti az emberi jogok európai egyezményében foglalt jogokat – beleértve az egyezmény 14. cikkében foglalt jogot, azaz a hátrányos megkülönböztetés tilalmát – az Egyesült Királyság jogába. Hasonlóképpen, az egyenlőségről szóló 2010. évi törvény tiltja a védett tulajdonságokkal (idetartozik a nem, faj, fogyatékosság stb.) rendelkező személyekkel szembeni hátrányos megkülönböztetést.
([137]) A 2018. évi adatvédelmi törvény 49. szakaszának (2) bekezdése.
([138]) A 2018. évi adatvédelmi törvény 50. szakaszának (4) bekezdése.

(75) A nemzetközi adattovábbításokra vonatkozó egyesült királyságbeli rendszert a 2018. évi adatvédelmi törvény 3. részének 5. fejezete szabályozza ([139]) és az (EU) 2016/680 irányelv V. fejezetében alkalmazott megközelítést tükrözi. A személyes adatok harmadik országba történő továbbításához az illetékes hatóságnak különösen három feltételnek kell megfelelnie: a) az adattovábbításnak bűnüldözési célból szükségesnek kell lennie; b) az adattovábbításnak a következőkön kell alapulnia: i. megfelelőségi rendeleten a harmadik ország vonatkozásában, ii. ha nem megfelelőségi rendeleten alapul, a megfelelő biztosítékok meglétén, vagy iii. ha nem megfelelőségi rendeleten vagy megfelelő biztosítékokon alapul, akkor a kivételes körülményeken kell alapulnia; és c) az adattovábbítás címzettjének az alábbinak kell lennie: i. a harmadik ország megfelelő hatósága (azaz az illetékes hatóság megfelelője); ii. „érintett nemzetközi szervezet", például olyan nemzetközi testület, amely a bűnüldözési célok bármelyikének megfelelő feladatokat lát el; vagy iii. az illetékes hatóságtól eltérő személy, de csak akkor, ha az adattovábbítás feltétlenül szükséges a bűnüldözési célok valamelyikének teljesítéséhez; a szóban forgó érintetteknek nincsenek olyan alapvető jogai és szabadságai, amelyek elsőbbséget élveznének az adattovábbításhoz fűződő közérdekkel szemben; a személyes adatok harmadik ország illetékes hatóságához történő továbbítása hatástalan vagy nem helyénvaló lenne; és a címzettet tájékoztatják az adatok kezelésének lehetséges céljairól ([140]).

(76) Harmadik országra, egy harmadik ország területére vagy ágazatára, nemzetközi szervezetre vonatkozó megfelelőségi rendeleteket vagy ([141]) az ilyen állam, terület, ágazat vagy szervezet leírását a miniszter fogadja el. Az elérendő szintet illetően a miniszternek értékelnie kell, hogy az említett terület/ágazat/szervezet biztosítja-e a személyes adatok megfelelő szintű védelmét. A 2018. évi adatvédelmi törvény 74A. szakaszának (4) bekezdése előírja, hogy ennek érdekében a miniszternek számos olyan elemet kell figyelembe vennie, amely az (EU) 2016/680 irányelv 36. cikkében felsoroltakat tükrözi ([142]). Ebben a tekintetben az átmeneti időszak vége óta a 2018. évi adatvédelmi törvény 3. része alkotja az „uniós jogból eredő nemzeti jogszabályokat", amelyeket – a magyarázat szerint – az Egyesült Királyság bíróságai a Bíróság vonatkozó, az Egyesült Királyság Unióból való kilépése előtti időből származó ítélkezési gyakorlatának és az uniós jog közvetlenül az átmeneti időszak vége előtt hatályos általános elveinek megfelelően fognak értelmezni. Idetartozik a „lényegi egyenértékűség" mérce, amelyet ekként alkalmazni fognak az Egyesült Királyság hatóságai által végzett megfelelőségértékelések esetében is.

(77) Ami az eljárást illeti, a szabályozásra a 2018. évi adatvédelmi törvény 182. szakaszában előírt „általános" eljárási követelmények vonatkoznak. Ennek az eljárásnak az alapján a miniszternek konzultálnia kell az információügyi

([139]) Ez az új keret az átmeneti időszak végén lépett hatályba, beleértve a miniszter megfelelőségi rendeletek meghozására vonatkozó hatáskörét. Ugyanakkor a kilépéssel kapcsolatos adatvédelmi szabályozás (különösen a 21. melléklet 10–12. pontja, amelyeket e szabályozás beiktat a 2018. évi adatvédelmi törvénybe) előírja, hogy az átmeneti időszak végén és azt követően a személyes adatok bizonyos továbbítását úgy kell kezelni, mintha azok megfelelőségi rendeleteken alapulnának. Ezek az adattovábbítások magukban foglalják azokat a harmadik országokba történő adattovábbításokat, amelyekre az átmeneti időszak végén uniós megfelelőségi határozat vonatkozik, valamint az EU tagállamaiba, az EFTA-államokba és Gibraltár területére történő adattovábbításokat, mivel ezek a bűnüldözési irányelvet alkalmazzák a bűnüldözési célú adatkezelésre (az EFTA-államok a schengeni vívmányok alapján fennálló kötelezettségeik eredményeként alkalmazzák az (EU) 2016/680 irányelvet). Ez azt jelenti, hogy az átmeneti időszak végén az adattovábbítások ezekbe az országokba az Unióból való kilépés előttivel megegyezően folytatódhatnak. Az átmeneti időszak lejárta után a miniszternek 4 éven belül felül kell vizsgálnia a megfelelőségi megállapításokat.

([140]) A 2018. évi adatvédelmi törvény 73. és 77. szakasza.

([141]) Az Egyesült Királyság hatóságai kifejtették, hogy egy ország vagy egy nemzetközi szervezet leírása arra a helyzetre utal, amikor a megfelelőség konkrét és részleges meghatározására van szükség, konkrét területre vonatkozó korlátozásokkal (például a megfelelőségi rendelet csak bizonyos típusú adattovábbításokra vonatkozik).

([142]) Lásd a 2018. évi adatvédelmi törvény 74A. szakaszának (4) bekezdését, amely előírja, hogy a védelmi szint megfelelőségének értékelésekor „a miniszternek különösen figyelembe kell vennie a) a jogállamiságot, az emberi jogok és az alapvető szabadságok tiszteletben tartását, a vonatkozó általános és ágazati jogszabályokat, ideértve a közbiztonságra, a védelemre, a nemzetbiztonságra és a büntetőjogra, valamint a hatóságok személyes adatokhoz való hozzáférésére vonatkozó jogszabályokat, valamint az említett jogszabályok, adatvédelmi szabályok, szakmai szabályok és biztonsági intézkedések végrehajtását, beleértve a személyes adatok harmadik országba vagy nemzetközi szervezetnek történő továbbításának az adott ország vagy nemzetközi szervezet által betartott szabályait, az ítélkezési gyakorlatot, valamint a tényleges és érvényesíthető érintetti jogokat, valamint azon érintetek számára a tényleges közigazgatási és bírósági jogorvoslat meglétét, akiknek személyes adatait továbbítják, b) egy vagy több független felügyeleti hatóság meglétét és hatékony működését a harmadik országban vagy a nemzetközi szervezetre vonatkozóan, amely felelős az adatvédelmi szabályok betartásának biztosításáért és érvényre juttatásáért, ideértve a megfelelő végrehajtási hatásköröket, az érintetteknek jogaik gyakorlásában történő segítségnyújtást és tanácsadást, valamint a biztossal való együttműködést, és) az érintett harmadik ország vagy nemzetközi szervezet által vállalt nemzetközi kötelezettségvállalásokat, vagy a jogilag kötelező érvényű egyezményekből vagy okmányokból, valamint a multilaterális vagy regionális rendszerekben való részvételéből eredő egyéb kötelezettségeket, különösen a személyes adatok védelme tekintetében".

biztossal, amikor javaslatot tesz az Egyesült Királyság jövőbeli megfelelőségi rendeleteinek megalkotására ([143]). Miután a miniszter elfogadta ezeket a rendeleteket, azokat a Parlament elé terjesztik, és a „negatív állásfoglalási" eljárás érvényesül, amelynek során a Parlament mindkét háza megvizsgálhatja a rendeletet, és 40 napos határidőn belül elfogadhat a rendelet megsemmisítésére vonatkozó indítványt ([144]).

(78) A 2018. évi adatvédelmi törvény 74B. szakaszának (1) bekezdése szerint a megfelelőségi rendeletet legfeljebb négyéves időközönként felül kell vizsgálni, a miniszternek pedig folyamatosan figyelemmel kell kísérnie a harmadik országokban és nemzetközi szervezetekben azokat a fejleményeket, amelyek befolyásolhatják a megfelelőségi rendeletek megalkotására, illetve az említett rendeletek módosítására vagy visszavonására vonatkozó döntéseket. Ha a miniszter tudomására jut, hogy egy adott ország vagy szervezet már nem biztosítja a személyes adatok megfelelő szintű védelmét, a szükséges mértékben módosítania vagy hatályon kívül kell helyeznie a szabályokat, és konzultációt kell folytatnia a harmadik országgal vagy nemzetközi szervezettel a megfelelő védelem hiányának orvoslása érdekében.

(79) Az (EU) 2016/680 irányelv 37. cikkében előírtakhoz hasonlóan, megfelelőségi rendelet hiányában a személyes adatok továbbítása a bűnüldözési ágazattal összefüggésben lehetséges, ha megfelelő biztosítékokat rendszeresítettek. Ezek a biztosítékok a következők révén biztosíthatók: a) a személyes adatok védelmére megfelelő biztosítékokat tartalmazó, kötelező érvényű jogi eszköz; vagy b) az adatkezelő által elvégzett értékelés, amely az adattovábbítással kapcsolatos összes körülmény felmérése után arra a következtetésre jut, hogy megfelelő biztosítékok léteznek az adatok védelmére ([145]). Továbbá, ha az adattovábbítások megfelelő biztosítékokon alapulnak, a 2018. évi adatvédelmi törvény előírja, hogy a biztos szokásos felügyeleti szerepe mellett az illetékes hatóságoknak konkrét információkat kell szolgáltatniuk a biztosnak történő adattovábbításokról ([146]).

(80) Ha az adattovábbítás nem megfelelőségi rendeleten vagy megfelelő biztosítékokon alapul, akkor arra csak bizonyos, meghatározott körülmények között kerülhet sor, amelyeket „kivételes körülményeknek" nevezünk ([147]). Ez a helyzet áll fen, ha az adattovábbítás az alábbiak miatt szükséges: a) az érintett vagy egy másik személy létfontosságú érdekeinek védelme érdekében; b) az érintett jogos érdekeinek biztosításához; c) harmadik ország közbiztonságát közvetlenül és komolyan fenyegető veszély elhárítása érdekében; d) egyedi esetekben bármely bűnüldözési célból; vagy e) egyedi esetekben jogi célból (például jogi eljárásokkal vagy jogi tanács kikérésével kapcsolatban) ([148]). Megjegyzendő, hogy a d) és e) pont nem alkalmazandó, ha az érintett jogai és szabadságai felülírják az adattovábbítással kapcsolatos közérdeket ([149]). Ezek a körülmények megfelelnek az (EU) 2016/680 irányelv 38. cikke alapján „eltérésnek" minősülő kivételes eseteknek és feltételeknek.

(81) Ilyen körülmények között az adattovábbítás napját, idejét és indokát, a címzett nevét és minden egyéb vonatkozó információt, valamint az átadott személyes adatok leírását dokumentálni kell, és kérésre át kell adni az információügyi biztosnak ([150]).

(82) A 2018. évi adatvédelmi törvény 78. szakasza szabályozza az „utólagos továbbítás" esetét, nevezetesen amikor az Egyesült Királyságból egy harmadik országba továbbított személyes adatokat utóbb egy másik harmadik országba vagy egy nemzetközi szervezetnek továbbítják. A 78. szakasz (1) bekezdése szerint az egyesült királyságbeli átadó adatkezelőnek az adattovábbítás feltételeként kell megszabnia, hogy az adatokat nem szabad továbbítani harmadik országba az átadó adatkezelő engedélye nélkül. A 2018. évi adatvédelmi törvény továbbá – a 78. szakasz (3) bekezdése szerint, hasonlóan az (EU) 2016/680 irányelv 35. cikke (1) bekezdése e) pontjában előírtakhoz – lényegi

([143]) Lásd: a Digitális, Kulturális, Média- és Sportminisztérium minisztere (DCMS) és az információügyi biztos hivatala közötti egyetértési megállapodást, amely meghatározza a DCMS és a biztos közötti kölcsönösen elfogadott munkamódszereket az Egyesült Királyság jövőbeni megfelelőségértékelései tekintetében, elérhető a következő linken: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Ebben a 40 napos időszakban a Parlament mindkét házának lehetősége nyílik arra, hogy az említett rendeleteket leszavazzák, ha kívánják; az említett szavazás esetén a szabályozás további joghatása megszűnik.

([145]) A 2018. évi adatvédelmi törvény 75. szakasza.

([146]) A 2018. évi adatvédelmi törvény 75. szakaszának (3) bekezdése szerint, amennyiben az adattovábbítás megfelelő biztosítékok alapján történik: a) az adattovábbítást dokumentálni kell, b) a dokumentációt kérésre át kell adni a biztosnak és c) a dokumentációnak tartalmaznia kell különösen i. az adattovábbítás napját és időpontját, ii. és minden egyéb releváns információt a címzettről, iii. az adattovábbítás indokát, és iv. az átadott személyes adatok leírását.

([147]) Útmutató a bűnüldözési eljárásokhoz: „Vannak-e kivételes körülmények?", elérhető a következő linken: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) A 2018. évi adatvédelmi törvény 76. szakasza.

([149]) A 2018. évi adatvédelmi törvény 76. szakasza.

([150]) A 2018. évi adatvédelmi törvény 76. szakaszának (3) bekezdése.

követelményeket ír elő abban az esetben, ha ilyen engedélyre van szükség. Pontosabban az illetékes hatóságnak az adattovábbítás engedélyezésének vagy elutasításának eldöntésekor meg kell győződnie arról, hogy a további adattovábbítás bűnüldözési célból szükséges-e, és figyelembe kell vennie többek között a következőket: az engedély iránti kérelemhez vezető körülmények súlyossága, b) a személyes adatok eredeti továbbításának célja és c) a személyes adatok védelmére vonatkozó azon normák, amelyek azon harmadik országban vagy nemzetközi szervezetben érvényesek, amelynek a személyes adatokat továbbították.

(83) Ezenkívül amikor az Egyesült Királyságból a további adattovábbítással érintett adatokat eredetileg az Európai Unióból továbbították, további biztosítékok érvényesülnek.

(84) Először is, a 2018. évi adatvédelmi törvény 73. szakasza (1) bekezdésének b) pontja – az (EU) 2016/680 irányelv 35. cikke (1) bekezdésének c) pontjához hasonlóan – előírja, hogy abban az esetben, ha a személyes adatokat eredetileg az adatkezelő vagy más tagállami illetékes hatóság részére továbbították vagy más módon rendelkezésére bocsátották, az a tagállam, vagy az adott tagállamban letelepedett és az (EU) 2016/680 irányelv alkalmazásában illetékes hatóságnak minősülő más személy a tagállam jogával összhangban engedélyezte az adattovábbítást.

(85) Ugyanakkor az (EU) 2016/680 irányelv 35. cikkének (2) bekezdéséhez hasonlóan ilyen engedélyre nincs szükség, ha a) az adattovábbításra a tagállam vagy harmadik ország közbiztonságát vagy valamely tagállam alapvető érdekeit fenyegető közvetlen vagy súlyos veszély megelőzése érdekében van szükség, és b) az engedély nem szerezhető be időben. Ebben az esetben haladéktalanul tájékoztatni kell a tagállam azon hatóságát, amely felelős lett volna az adattovábbítás engedélyezéséről való döntésért ([151]).

(86) Másodszor, ugyanez a megközelítés vonatkozik azokra az adatokra, amelyeket eredetileg az Európai Unióból továbbítottak az Egyesült Királyságba, majd az Egyesült Királyság továbbított egy harmadik országba, amely ezt követően azokat egy másik harmadik országba továbbította. Ebben az esetben a 78. szakasz (4) bekezdése szerint az egyesült királyságbeli illetékes hatóság ez utóbbi további adattovábbításhoz nem adhatja hozzájárulását a 78. szakasz (1) bekezdése szerint, kivéve, ha „a (szóban forgó adatokat eredetileg továbbító) tagállam vagy a bűnüldözési irányelv alkalmazásában illetékes hatóságnak minősülő, az adott tagállamban letelepedett más személy a tagállam jogával összhangban engedélyezte az adattovábbítást". Ezek a biztosítékok fontosak, mivel lehetővé teszik a tagállami hatóságoknak, hogy az EU adatvédelmi jogszabályainak megfelelően biztosítsák a védelem folytonosságát a teljes „továbbítási láncban".

(87) A nemzetközi adattovábbítások új keretrendszere az átmeneti időszak végén vált alkalmazhatóvá ([152]). Azonban a 21. melléklet 10–12. pontja (amelyet a kilépéssel kapcsolatos adatvédelmi szabályozás vezetett be) előírja, hogy az átmeneti időszak végétől kezdve a személyes adatok bizonyos továbbítását úgy kezelik, mintha azok megfelelőségi rendeleteken alapulnának. Ezen adattovábbítások körébe tartoznak a valamely tagállamba, EFTA-állambа, Gibraltár területére, valamint olyan harmadik országokba történő adattovábbítások, amelyekre az átmeneti időszak végén uniós megfelelőségi határozat vonatkozik. Következésképpen az ezekbe az országokba irányuló adattovábbítások ugyanúgy folytatódhatnak, mint az Egyesült Királyság Unióból való kilépése előtt. Az átmeneti időszak lejárta után a miniszternek négy éven belül, azaz 2024. december végéig felül kell vizsgálnia ezeket a megfelelőségi megállapításokat. Az Egyesült Királyság hatóságainak magyarázata szerint, bár a miniszternek 2024 december végéig el kell végeznie egy ilyen felülvizsgálatot, az átmeneti rendelkezések nem tartalmaznak „megszüntetési" rendelkezést, és a vonatkozó átmeneti rendelkezések hatálya nem szűnik meg automatikusan, ha a felülvizsgálat 2024. december végéig nem fejeződik be.

2.4.9. *Elszámoltathatóság*

(88) Az elszámoltathatóság elve értelmében az adatkezelőknek megfelelő technikai és szervezeti intézkedéseket kell hozniuk, hogy ténylegesen megfeleljenek adatvédelmi kötelezettségeiknek, és bizonyítani tudják ezt a megfelelést, különösen az illetékes felügyeleti hatóság felé.

(89) Ezt az elvet tükrözi a 2018. évi adatvédelmi törvény 56. szakasza, amely általános elszámoltathatósági kötelezettséget vezet be az adatkezelő számára, azaz megfelelő technikai és szervezési intézkedések végrehajtásának kötelezettségét annak biztosítására és bizonyítására, hogy a személyes adatok kezelése megfelel a 2018. évi adatvédelmi törvény 3. része követelményeinek. A végrehajtott intézkedéseket szükség esetén felül kell vizsgálni és frissíteni kell, és amennyiben az arányos az adatkezeléssel, megfelelő adatvédelmi irányelveket kell tartalmazniuk.

([151]) A 2018. évi adatvédelmi törvény 73. szakaszának (5) bekezdése.

([152]) Ezen új keret alkalmazhatóságát az egyrészről az Európai Unió és az Európai Atomenergia-közösség, és másrészről Nagy-Britannia és Észak-Írország Egyesült Királysága közötti kereskedelmi és együttműködési megállapodás (HL L 444., 2020.12.31., 14. o.) 782. cikkére figyelemmel kell értelmezni, amely az alábbi linken érhető el: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:22020A1231(01)

(90) Az (EU) 2016/680 irányelv IV. fejezetével összhangban a 2018. évi adatvédelmi törvény 55–71. szakasza különböző mechanizmusokat ír elő az elszámoltathatóság biztosítása érdekében, és lehetővé teszi az adatkezelőknek és az adatfeldolgozóknak a megfelelőség bizonyítását. Az adatkezelőknek különösen beépített adatvédelmi intézkedéseket kell végrehajtaniuk alapértelmezésben, vagyis biztosítaniuk kell az adatvédelmi elvek eredményes végrehajtását, és nyilvántartást kell vezetniük az adatkezelő felelősségi körébe tartozó összes adatkezelési tevékenységről (ideértve a következőket is: az adatkezelő azonosító adatai, az adatvédelmi tisztviselő elérhetőségei, az adatkezelés céljai, a közlés címzettjeinek kategóriái, valamint az érintettek és a személyes adatok kategóriáinak leírása), és ezeket az adatokat kérésre az információügyi biztos számára hozzáférhetővé kell tenni. Az adatkezelőnek és az adatfeldolgozónak naplót is vezetnie kell bizonyos adatkezelési műveletekről, és azt az információügyi biztos rendelkezésére kell bocsátania ([153]). Az adatkezelőknek kifejezetten együtt kell működniük az információügyi biztossal a biztos feladatainak ellátása során.

(91) A 2018. évi adatvédelmi törvény további követelményeket is megállapít az adatkezelésre, ha az valószínűsíthetően magas kockázattal jár az egyének jogaira és szabadságaira nézve. Ezek magukban foglalják az adatvédelmi hatásvizsgálatok elvégzésének és az adatkezeléssel foglalkozó biztossal való konzultáció kötelezettségét, ha az említett értékelés azt jelzi, hogy az adatkezelés (a kockázat csökkentésére irányuló intézkedések hiányában) magas kockázatot jelentene az egyének jogaira és szabadságaira.

(92) Az adatkezelőknek továbbá ki kell jelölniük egy adatvédelmi tisztviselőt, kivéve, ha az adatkezelő bíróság vagy más, igazságszolgáltatási minőségben eljáró igazságügyi hatóság ([154]). Az adatkezelőnek biztosítania kell, hogy az adatvédelmi tisztviselőt bevonják a személyes adatok védelmével kapcsolatos minden kérdésbe, rendelkezzen a szükséges erőforrásokkal és hozzáféréssel a személyes adatokhoz, valamint az adatkezelési műveletekhez, és önállóan el tudja látni feladatait. Az adatvédelmi tisztviselő feladatait a 2018. évi adatvédelmi törvény 71. szakasza határozza meg, ideértve a tájékoztatás és tanácsadás nyújtását, a megfelelés nyomon követését, valamint az információügyi biztossal való együttműködést és vele kapcsolattartóként történő eljárást. Feladatainak ellátása során az adatvédelmi tisztviselőnek figyelembe kell vennie az adatkezelési műveletekhez kapcsolódó kockázatokat, figyelembe véve az adatkezelés jellegét, terjedelmét, összefüggéseit és céljait.

2.5. **Felügyelet és végrehajtás**

2.5.1. *Független felügyelet*

(93) Az adatvédelem megfelelő szintjének gyakorlati biztosítása érdekében létre kell hozni egy független felügyeleti hatóságot, amely hatáskörrel rendelkezik az adatvédelmi szabályoknak való megfelelés nyomon követésére és a megfelelés kikényszerítésére. Ennek a hatóságnak teljes egészében függetlenül és pártatlanul kell eljárnia feladatainak ellátása és hatáskörének gyakorlása során.

(94) Az Egyesült Királyság általános adatvédelmi rendeletének és a 2018. évi adatvédelmi törvénynek való megfelelés felügyeletét és kikényszerítését az Egyesült Királyságban az információügyi biztos ([155]) végzi. Az információügyi biztos felügyeli továbbá a személyes adatok illetékes hatóságok általi, a 2018. évi adatvédelmi törvény 3. részének hatálya alá tartozó kezelését ([156]). Az információügyi biztos „Corporation Sole": egyetlen személyben megtestesülő önálló jogi személy. Az információügyi biztos munkáját egy hivatal támogatja. Az Információs Biztos Hivatalának 2020. március 31-én 768 állandó munkavállalója volt ([157]). Az információügyi biztos támogató minisztériuma a Digitális, Kulturális, Média- és Sportminisztérium ([158]).

([153]) A 2018. évi adatvédelmi törvény 62. szakasza.

([154]) A 2018. évi adatvédelmi törvény 69. szakasza.

([155]) Az (EU) 2016/680 irányelv 36. cikke (2) bekezdésének b) pontja.

([156]) A 2018. évi adatvédelmi törvény 116. szakasza.

([157]) Az információügyi biztos 2019–2020-es éves beszámolója és pénzügyi kimutatásai az alábbi linken érhetők el: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([158]) Egy ügyviteli megállapodás szabályozza a kettő kapcsolatát. Különösen a DCMS, mint támogató minisztérium fő feladatai közé tartoznak a következők: a biztos megfelelő finanszírozásának és erőforrásainak biztosítása; a biztos érdekeinek képviselete a Parlament és más kormányzati szervek előtt; szilárd nemzeti adatvédelmi keret biztosítása; valamint útmutatás és támogatás nyújtása a biztosnak olyan szervezeti kérdésekben, mint az ingatlanügyletek, a bérleti szerződések és a beszerzések (a 2018–2021-es ügyviteli megállapodás a következő linken érhető el: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) A biztos függetlenségét az Egyesült Királyság általános adatvédelmi rendeletének 52. cikke kifejezetten rögzíti, amely tükrözi az (EU) 2016/679 európai parlamenti és tanácsi rendelet ([159]) 52. cikkének (1)–(3) bekezdésében megállapított követelményeket. A biztosnak teljesen függetlenül kell eljárnia feladatainak ellátása és hatásköreinek az Egyesült Királyság általános adatvédelmi rendeletével összhangban történő gyakorlása során, mentesnek kell maradnia bármiféle közvetlen vagy közvetett külső befolyástól e feladatok és hatáskörök tekintetében, és senkitől nem kérhet és nem fogadhat el utasításokat. A biztosnak tartózkodnia kell minden olyan feladattól is, amely összeegyeztethetetlen a feladataival, és hivatali idejében nem folytathat összeegyeztethetetlen foglalkozást, legyen az fizetett vagy önkéntes munka.

(96) Az információügyi biztos kinevezésének és visszahívásának feltételeit a 2018. évi adatvédelmi törvény 12. melléklete tartalmazza. Az információügyi biztost a királynő nevezi ki a kormány ajánlása alapján, tisztességes és nyílt verseny alapján. A jelöltnek rendelkeznie kell a megfelelő képesítéssel, készségekkel és kompetenciákkal. A Governance Code on Public Appointments (állami kinevezések irányítása kódexe) elnevezésű dokumentummal összhangban ([160]) a kinevezhető jelöltek listáját egy tanácsadó értékelő testület állítja össze. Mielőtt a Digitális, Kulturális, Média- és Sportminisztérium minisztere véglegesíti döntését, az illetékes parlamenti válogató bizottságnak kinevezés előtti ellenőrzést kell lefolytatnia. A bizottság álláspontját nyilvánosságra hozzák ([161]).

(97) Az információügyi biztos hivatali ideje legfeljebb hét év. Őfelsége a Parlament mindkét házának beszédét követően felmentheti hivatalából ([162]). Az információügyi biztos felmentésére vonatkozó kérelem nem terjeszthető be a Parlament egyik házához sem, ha egy miniszter nem terjesztett elő jelentést az adott háznak, amelyben kijelenti, hogy meg van győződve arról, hogy az információügyi biztos súlyos kötelességszegésben vétkes és/vagy a biztos már nem felel meg a biztos feladatainak ellátásához szükséges feltételeknek ([163]).

(98) Az információügyi biztos finanszírozása három forrásból származik: i. az adatkezelők által fizetett adatvédelmi díjak, amelyeket a miniszter rendelete határoz meg ([164]) és ezek a Hivatal éves költségvetésének 85–90 %-át teszik ki ([165]); ii. támogatás, amelyet a kormány fizethet az információügyi biztos részére, és amelyet elsősorban az információügyi biztos adatvédelemhez nem kapcsolódó feladatai tekintetében felmerülő működési költségeinek finanszírozására fordítanak ([166]); iii. a szolgáltatásokért felszámított díjak ([167]). Jelenleg ilyen díjakat nem számítanak fel.

(99) Az információügyi biztos általános feladatait a 2018. évi adatvédelmi törvény 3. részének hatálya alá tartozó személyes adatok kezelésével kapcsolatban a 2018. évi adatvédelmi törvény 13. melléklete határozza meg. A feladatok magukban foglalják a 2018. évi adatvédelmi törvény 3. részének nyomon követését és végrehajtását, a közvélemény tudatosságának elősegítését, tanácsadást a Parlamentnek, a kormánynak és más intézményeknek a jogalkotási és adminisztratív intézkedések terén, az adatkezelők és az adatfeldolgozók tudatosságának fokozását

([159]) Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (HL L 119., 2016.5.4., 1. o.).

([160]) Governance Code on Public Appointments, elérhető a következő linken: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Az alsóház kulturális, média- és sportbizottsága 2015–2016-os ülésszakának második jelentése, az alábbi linken érhető el: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) A „beszéd” a Parlament elé terjesztett indítvány, amelynek célja, hogy az uralkodót megismertesse a Parlament véleményével egy adott kérdésben.

([163]) A 2018. évi adatvédelmi törvény 12. mellékletének 3. pontja.

([164]) A 2018. évi adatvédelmi törvény 137. szakasza.

([165]) A 2018. évi adatvédelmi törvény 137. és 138. szakasza számos biztosítékot tartalmaz annak biztosítására, hogy a díjakat megfelelő szinten állapítsák meg. Különösen, a 2018. évi adatvédelmi törvény 137. szakaszának (4) bekezdése felsorolja azokat az ügyeket, amelyekre a miniszternek tekintettel kell lennie, amikor a különböző szervezetek által fizetendő összeget meghatározza rendeleteket elfogadja. A 2018. évi adatvédelmi törvény 138. szakaszának (1) bekezdése és 182. cikke szintén előírja, hogy a miniszternek konzultálnia kell az információügyi biztossal és a rendeletek által valószínűleg érintett személyek más képviselőivel, a rendeletek elfogadása előtt, hogy véleményüket figyelembe lehessen venni. Ezenkívül a 2018. évi adatvédelmi törvény 138. szakaszának (2) bekezdése értelmében az információügyi biztos köteles felülvizsgálni a díjakról szóló rendeletek működését, és javaslatokat nyújthat be a miniszterhez a rendeletek módosítására. Végül a rendeletekre „pozitív állásfoglalási” eljárás vonatkozik – kivéve azokat az eseteket, amikor a rendelet pusztán a kiskereskedelmi árindex növekedésének figyelembevétele érdekében készül (ebben az esetben a „negatív állásfoglalási” eljárás irányadó) –, és csak akkor fogadhatók el, ha a Parlament mindegyik háza azokat határozattal jóváhagyta.

([166]) Az ügyviteli megállapodás egyértelművé teszi, hogy „a miniszter az információügyi biztosnak teljesíthet kifizetéseket a Parlament által a 2018. évi adatvédelmi törvény 12. mellékletének 9. pontja alapján biztosított forrásokból. Az információügyi biztossal folytatott konzultációt követően a DCMS kifizeti (támogatásként átadja) a megfelelő összegeket az információügyi biztosnak a biztos igazgatási költségeire és a biztos számos konkrét feladatkörével kapcsolatos funkcióinak gyakorlásáért, ideértve az információszabadságot is (a 2018–2021-es ügyviteli megállapodás, 1.12. pont, lásd a 158. lábjegyzetet).

([167]) A 2018. évi adatvédelmi törvény 134. szakasza.

kötelezettségeikről, az érintettek tájékoztatását az érintett jogainak gyakorlásáról és vizsgálatok lefolytatását. Az igazságszolgáltatás függetlenségének fenntartása érdekében az információügyi biztos nem jogosult feladatait a személyes adatok bírói minőségben eljáró egyén, vagy bírósági minőségében eljáró bíróság vagy törvényszék általi kezelésével kapcsolatban ellátni. Az igazságszolgáltatás felügyeletét azonban az alábbiakban tárgyalt szakosított testületek biztosítják.

2.5.1.1. Jogérvényesítés, ezen belül a szankciók

(100) A biztos általános nyomozati, korrekciós, engedélyezési és tanácsadói hatáskörrel rendelkezik azon személyes adatok kezelésével kapcsolatban, amelyekre a 2018. évi adatvédelmi törvény 3. része vonatkozik. A biztos hatáskörrel rendelkezik arra, hogy értesítse az adatkezelőt vagy az adatfeldolgozót a 3. rész állított megsértéséről, figyelmeztetést adjon ki az adatkezelőnek vagy az adatfeldolgozónak, hogy a tervezett adatkezelési műveletek valószínűleg a 3. rész rendelkezéseibe ütköznek, és megrovást adhat az adatkezelőnek vagy az adatfeldolgozónak, ha az adatkezelési műveletek a 3. rész rendelkezéseibe ütköznek. Ezenkívül saját kezdeményezésére vagy kérelemre a biztos véleményt nyilváníthat az Egyesült Királyság Parlamentjének, a kormánynak vagy más intézményeknek és szerveknek, valamint a nyilvánosságnak a személyes adatok védelmével kapcsolatos bármely kérdésben ([168]).

(101) Ezenkívül a biztos hatáskörrel rendelkezik az alábbiakra:

– az adatkezelő és az adatfeldolgozó (és bizonyos körülmények között bármely más személy) számára a szükséges információk megadásának elrendelése tájékoztatás kérésével („adatkérési felhívás") ([169]);

– vizsgálat és ellenőrzés végzése vizsgálati felhívás útján, amelyben elrendelheti az adatkezelő vagy az adatfeldolgozó számára, hogy engedélyezze a biztos számára a belépést meghatározott helyiségekbe, dokumentumok vagy berendezések megtekintését vagy vizsgálatát, a személyes adatokat az adatkezelő nevében feldolgozó emberek kihallgatását („vizsgálati felhívás") ([170]);

– egyébként hozzáférés az adatkezelők és az adatfeldolgozók dokumentumaihoz, valamint belépés helyiségeikbe a 2018. évi adatvédelmi törvény 154. szakaszának („belépési és ellenőrzési jogkör") megfelelően;

– korrekciós hatáskör gyakorlása, többek között jogérvényesítési felhívás útján figyelmeztetések és megrovások, vagy utasítás adása révén, amelyben megköveteli az adatkezelőktől/adatfeldolgozóktól konkrét lépések megtételét vagy azoktól tartózkodást („jogérvényesítési felhívás") ([171]); valamint

– bírságértesítő formájában közigazgatási bírságot szab ki („bírságértesítő") ([172]).

(102) A biztos szabályozási cselekvési politikája meghatározza azokat a körülményeket, amelyek mellett a biztos adatkérési, vizsgálati, jogérvényesítési felhívást és bírságértesítőt fog kiadni ([173]). A jogérvényesítési felhívás olyan követelményeket támaszthat, amelyeket a biztos a mulasztás orvoslása érdekében megfelelőnek tart. A bírságértesítő előírja a személynek, hogy az értesítésben meghatározott összeget fizesse meg az információügyi biztosnak. Bírságértesítőt akkor lehet kiadni, ha a 2018. évi adatvédelmi törvény bizonyos rendelkezéseit nem tartották be ([174]) vagy olyan adatkezelőnek/adatfeldolgozónak adható, amely nem tett eleget adatkérési, vizsgálati vagy jogérvényesítési felhívásnak.

(103) Pontosabban, annak eldöntésekor, hogy valamely adatkezelőnek/adatfeldolgozónak bírságértesítőt küldenek-e, valamint a büntetés összegének meghatározásakor, az információügyi biztosnak figyelembe kell vennie a 2018. évi adatvédelmi törvény 155. szakaszának (3) bekezdésében felsorolt kérdéseket, ideértve a mulasztás jellegét és súlyosságát, a mulasztás szándékos vagy gondatlan jellegét, az adatkezelő vagy az adatfeldolgozó által az érintettek

([168]) A 2018. évi adatvédelmi törvény 13. mellékletének 2. pontja.
([169]) A 2018. évi adatvédelmi törvény 142. szakasza (a 2018. évi adatvédelmi törvény 143. szakaszában foglalt korlátozásokra figyelemmel).
([170]) A 2018. évi adatvédelmi törvény 146. szakasza (a 2018. évi adatvédelmi törvény 147. szakaszában foglalt korlátozásokra figyelemmel).
([171]) A 2018. évi adatvédelmi törvény 149–151. szakasza (a 2018. évi adatvédelmi törvény 152. szakaszában foglalt korlátozásokra figyelemmel).
([172]) A 2018. évi adatvédelmi törvény 155. szakasza (a 2018. évi adatvédelmi törvény 156. szakaszában foglalt korlátozásokra figyelemmel).
([173]) Szabályozási cselekvési politika, elérhető a következő linken: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) A biztos különösen a 2018. évi adatvédelmi törvény 149. szakaszának (2), (3), (4) vagy (5) bekezdésében meghatározottak be nem tartása miatt adhat ki bírságértesítőt.

által elszenvedett kár enyhítése érdekében tett bármely intézkedést, az adatkezelő vagy az adatfeldolgozó felelősségének mértékét (figyelembe véve az adatkezelő vagy az adatfeldolgozó által végrehajtott technikai és szervezési intézkedéseket), az adatkezelő vagy az adatfeldolgozó esetleges korábbi mulasztásait; a mulasztás által érintett személyes adatok kategóriáit, valamint hogy a büntetés hatékony, arányos és visszatartó erejű legyen.

(104) A bírságértesítővel kiszabható büntetés maximális összege a) 17 500 000 GBP az adatvédelmi elvek (a 2018. évi adatvédelmi törvény 35., 36., 37. szakasza, 38. szakaszának (1) bekezdése, 39. szakaszának (1) bekezdése és 40. szakasza) az átláthatósági kötelezettségek és az egyének jogai (a 2018. évi adatvédelmi törvény 44., 45., 46., 47., 48., 49., 52. és 53. szakasz), valamint a személyes adatok nemzetközi továbbításának elvei (a 2018. évi adatvédelmi törvény 73., 75., 76., 77. vagy 78. szakasza) be nem tartása kapcsán; és b) 8 700 000 GBP egyéb esetekben ([175]). Az adatkérési, vizsgálati vagy jogérvényesítési felhívás be nem tartásával kapcsolatban a bírságértesítővel kiszabható büntetés maximális összege 17 500 000 GBP.

(105) Legfrissebb éves jelentései szerint (2018–2019 ([176]), 2019–2020 ([177])) az információügyi biztos számos vizsgálatot folytatott a személyes adatok bűnüldöző szervek általi kezelése kapcsán. Például a biztos vizsgálatot folytatott, és 2019 októberében véleményt tett közzé az arcfelismerési technológia nyilvános helyeken bűnüldözési céllal történő használatáról. A vizsgálat különösen az élő arcfelismerő képességek használatára összpontosított a dél-walesi rendőrség és a Metropolitan Police Service (MPS) területén. Ezenkívül a biztos megvizsgálta az MPS „bandamátrixát" ([178]) és számos olyan adatvédelmi jogi jogsértést állapított meg, amelyek valószínűleg aláássák a lakosság mátrixba és az adatok felhasználásába vetett bizalmát.

(106) 2018 novemberében az információügyi biztos jogérvényesítési felhívást adott ki, és az MPS ezt követően megtette a szükséges lépéseket a biztonság és az elszámoltathatóság növelése, valamint az adatok arányos felhasználásának biztosítása érdekében.

(107) A legutóbbi jogérvényesítési intézkedésekre másik példa a 325 000 GBP összegű bírság, amelyet a biztos 2018 májusában bocsátott ki a Crown Prosecution Service (királyi ügyészség) ellen, a rendőrségi kihallgatásokat tartalmazó titkosítatlan DVD-k elvesztése miatt. Emellett az információügyi biztos tágabb témákban folytatott vizsgálatokat, például 2020 első felében a mobiltelefonból kinyert adatok rendészeti célokra történő felhasználásáról és az áldozatok adatainak rendőrség általi kezeléséről.

(108) Az információügyi biztos e végrehajtási hatáskörein túl az adatvédelmi jogszabályok bizonyos megsértései bűncselekménynek minősülnek, ezért büntetőjogi szankciókkal sújthatók (a 2018. évi adatvédelmi törvény 196. szakasza). Ez vonatkozik például a személyes adatok adatkezelő hozzájárulása nélküli megszerzésére vagy közlésére, valamint más személy megbízása a személyes adatok adatkezelő hozzájárulása nélküli közlésével ([179]); az anonimizált személyes adatnak minősülő információk újbóli azonosítása a személyes adatok anonimizálásáért felelős adatkezelő hozzájárulása nélkül ([180]); a biztos szándékosan akadályozása abban, hogy gyakorolja a személyes adatok nemzetközi kötelezettségekkel összhangban történő ellenőrzésével kapcsolatos hatáskörét ([181]), hamis állítások megtétele az adatkérési felhívásra adott válaszul, vagy információk megsemmisítése az adatkérési és vizsgálati felhívások kapcsán ([182]).

(109) Az információügyi biztosnak a 2018. évi adatvédelmi törvény 139. szakasza értelmében kötelessége a Parlament mindegyik házának általános jelentés benyújtása a törvény szerinti feladataik ellátásáról ([183]).

([175]) A 2018. évi adatvédelmi törvény 157. szakasza.

([176]) Az információügyi biztos 2018-2019-es éves beszámolója és pénzügyi kimutatásai az alábbi linken érhetők el: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) Az információügyi biztos 2019–2020-as éves jelentése (lásd a 157. lábjegyzetet).

([178]) Adatbázis, amely rögzítette a feltételezett bandatagokkal és a bandához kapcsolható bűncselekmények áldozataival kapcsolatban szerzett információkat.

([179]) A 2018. évi adatvédelmi törvény 170. szakasza.

([180]) A 2018. évi adatvédelmi törvény 171. szakasza.

([181]) A 2018. évi adatvédelmi törvény 119. szakasza.

([182]) A 2018. évi adatvédelmi törvény 144. és 148. szakasza.

([183]) Az ügyviteli megállapodásban foglaltak szerint az éves jelentésnek: i. ki kell terjednie a biztos ellenőrzése alatt álló minden vállalatra, leányvállalatra vagy közös vállalkozásra; ii. meg kell felelnie a Kincstár Pénzügyi Beszámolási Kézikönyvének (Financial Reporting Manual – FReM); iii. tartalmaznia kell egy irányítási nyilatkozatot, amely meghatározza, hogy a számvitelért felelős tisztviselő hogyan kezelte és ellenőrizte az év során a szervezetben felhasznált erőforrásokat, bemutatva, hogy a szervezet mennyire képes megfelelően kezelni a céljainak és célkitűzéseinek elérésével kapcsolatos kockázatokat; és iv. ismertetnie kell az előző pénzügyi év fő tevékenységeit és teljesítményét, és összefoglaló formában meg kell határoznia az előretekintő terveket (2018–2021-es ügyviteli megállapodás, 3.26. pont, lásd a 158. lábjegyzetet).

2.5.2. *Az igazságszolgáltatás felügyelete*

(110) A személyes adatok bíróságok és igazságszolgáltatás általi kezelésének felügyelete kettős. Ha egy igazságügyi tisztségviselő vagy bíróság nem bírói minőségben jár el, a felügyeletet az információügyi biztos látja el. Amennyiben az adatkezelő bírói minőségben jár el, a biztos nem gyakorolhatja felügyeleti funkcióit ([184]) és a felügyeletet speciális szervek végzik. Ez az (EU) 2016/680 irányelv 32. cikkében megjelenő felfogást tükrözi.

(111) A második esetkörben az angliai és walesi bíróságok, valamint az angliai és walesi első és felsőbb bíróságok esetében az említett felügyeletet konkrétan a bírói adatvédelmi testület biztosítja ([185]). Ezenkívül a Lord Chief Justice és a Senior President of Tribunals adatkezelési tájékoztatót adott ki ([186]) amely meghatározza, hogy az angliai és walesi bíróságok miként kezelik a személyes adatokat bírósági funkciók ellátása céljából. Hasonló nyilatkozatot adott ki az északír ([187]) és a skót bírói kar is ([188]).

(112) Sőt, Észak-Írországban az északír Lord Chief Justice kinevezett egy legfelsőbb bírósági bírót adatvédelmi felügyelő bírónak (Data Supervisory Judge – DSJ) ([189]). Ugyancsak útmutatót adtak ki az északír bírói karnak arról, hogy mit kell tenniük adatok elvesztése vagy potenciális elvesztése esetén, valamint az ebből adódó kérdések kezelésének folyamatáról ([190]).

(113) Skóciában a Lord President nevezett ki egy adatvédelmi felügyelő bírót az adatvédelmi alapon tett esetleges panaszok kivizsgálására. Ezt a bírósági panaszokra vonatkozó szabályok rögzítik, amelyek az Anglia és Wales vonatkozásában megállapított szabályokat tükrözik ([191]).

(114) Végül a Legfelsőbb Bíróságon az egyik legfelsőbb bírósági bírót nevezik ki az adatvédelem felügyeletére.

([184]) A 2018. évi adatvédelmi törvény 117. szakasza.

([185]) A testület feladata a bírói kar számára útmutatás és képzés nyújtása. Foglalkozik továbbá az érintettektől a személyes adatok bíróságok, törvényszékek és bírósági minőségben eljáró egyének általi feldolgozása kapcsán érkező panaszokkal. A testület célja, hogy eszközt biztosítson az esetleges panaszok megoldására. Ha egy panaszos nem elégedett a testület döntésével, és további bizonyítékokat szolgáltat, a testület felülvizsgálhatja határozatát. Noha a testület maga nem szab ki pénzügyi szankciókat, ha a testület úgy ítéli meg, hogy a 2018. évi adatvédelmi törvény kellően súlyos sérelme történt, a panaszt a Bírói Magatartást Vizsgáló Hivatalhoz (JCIO) utalhatja, amely azt kivizsgálja. Ha a panaszt helybenhagyják, a Lord Chancellor és a Lord Chief Justice (vagy a nevében eljáró vezető bíró) feladata annak eldöntése, hogy milyen intézkedést hozzanak a tisztségviselővel szemben. Ez súlyosság szerinti sorrendben az alábbi lehet: hivatalos tanácsadás, hivatalos figyelmeztetés és megrovás, végső soron hivatalból való felmentés. Ha egy személy elégedetlen azzal, ahogyan a JCIO kivizsgálta a panaszt, további panaszt tehet a bírói kinevezésekkel és magatartással foglalkozó ombudsmannál (lásd https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Az ombudsman hatáskörrel rendelkezik arra, hogy felkérje a JCIO-t a panasz újbóli kivizsgálására, és javaslatot tehet a panaszos részére kártérítés fizetésére, amennyiben úgy véli, hogy hivatali visszásság miatt kárt szenvedett.

([186]) A Lord Chief Justice és a Senior President of Tribunals adatkezelési tájékoztatója a következő linken érhető el: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([187]) Az észak-írországi Lord Chief Justice által kiadott adatkezelési tájékoztató a következő linken érhető el: https://judiciaryni.uk/data-privacy

([188]) A skót bíróságok adatkezelési tájékoztatója következő linken érhető el: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([189]) A DSJ útmutatást nyújt a bírói kar számára, és kivizsgálja a személyes adatok bíróságok vagy bírói minőségben eljáró egyének általi kezelésével kapcsolatos jogsértéseket és/vagy panaszokat.

([190]) Amennyiben a panasz vagy a jogsértés súlyosnak minősül, azt továbbítják az igazságügyi panaszügyi tisztviselőhöz további vizsgálat céljából, az észak-írországi Lord Chief Justice panaszokkal kapcsolatos gyakorlati kódexének megfelelően. Az említett panasz kimenetele lehet: további intézkedés mellőzése, tanácsadás, képzés vagy mentorálás, informális figyelmeztetés, hivatalos figyelmeztetés, utolsó figyelmeztetés, a gyakorlat korlátozása vagy a törvényszék elé utalás. Az észak-írországi Lord Chief Justice panaszokkal kapcsolatos gyakorlati kódexe a következő linken érhető el: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]) Az adatvédelmi felügyelő bíró minden megalapozott panaszt kivizsgál, és a Lord Presidenthez továbbítja, aki jogosult tanácsot, hivatalos figyelmeztetést vagy megrovást kiadni, ha szükségesnek ítéli (a bíróság tagjaira egyenértékű szabályok léteznek, amelyek a következő linken érhetőek el: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Jogorvoslat*

(115) A megfelelő védelem biztosítása és különösen a személyhez fűződő jogok érvényesítésének biztosítása érdekében az érintettet hatékony közigazgatási és bírósági jogorvoslatban kell részesíteni, beleértve a kártérítést.

(116) Először is, az érintettnek joga van panaszt benyújtani az információügyi biztoshoz, ha az érintett úgy ítéli meg, hogy a rá vonatkozó személyes adatokkal kapcsolatban a 2018. évi adatvédelmi törvény 3. részét megszegték ([192]). A (100) és (109) preambulumbekezdésben leírtak szerint az információügyi biztos hatáskörrel rendelkezik annak értékelésére, hogy az adatkezelő és az adatfeldolgozó megfelel-e a 2018. évi adatvédelmi törvénynek, megkövetelheti tőlük, hogy tegyék meg a szükséges lépéseket, vagy tartózkodjanak azoktól meg nem felelés esetén és bírságot szab ki.

(117) Másodszor, a 2018. évi adatvédelmi törvény jogot biztosít az információügyi biztos elleni jogorvoslatra. Ha a biztos nem „halad" ([193]) az érintett által benyújtott panasz ügyében, a panaszost bírósági jogorvoslat illeti meg, mivel a First Tier Tribunal ([194]) előtt kérheti a biztos arra kötelezését, hogy tegye meg a megfelelő lépéseket a panasz elintézésére, vagy tájékoztassa a panaszost a panasz állásáról ([195]). Ezenkívül bárki, aki a biztostól a fenti bármelyik felhívást (adatkérési, vizsgálati, jogérvényesítési felhívás vagy bírságértesítő) megkapja, fellebbezést nyújthat be a First Tier Tribunalhoz. Ha ez a bíróság úgy ítéli meg, hogy a biztos döntése nincs összhangban a jogszabályokkal, vagy az információügyi biztosnak másként kellett volna gyakorolnia mérlegelési jogkörét, akkor engedélyeznie kell a fellebbezést, vagy olyan másik felhívást vagy határozatot kell elfogadnia, amelyet az információügyi biztos elfogadhatott volna ([196]).

(118) Harmadszor: az egyének az adatkezelőkkel és az adatfeldolgozókkal szemben közvetlenül a bírósághoz fordulva is bírósági jogorvoslatot nyerhetnek a 2018. évi adatvédelmi törvény 167. szakasza alapján. Ha az érintett kérelmére a bíróság meggyőződik arról, hogy megsértették az érintett adatvédelmi jogszabályok szerinti jogait, a bíróság kötelezheti az adatkezelésben érintett adatkezelőt, vagy az adatkezelő nevében eljáró adatfeldolgozót a kötelezésben maghatározott intézkedések megtételére, vagy az abban meghatározott lépésektől való tartózkodásra. Ezenkívül a 2018. évi adatvédelmi törvény 169. szakasza szerint minden olyan személy kártérítésre jogosult az adatkezelőtől vagy az adatfeldolgozótól, aki – az Egyesült Királyság általános adatvédelmi rendeletétől eltérő – adatvédelmi jogszabályok (ideértve a 2018. évi adatvédelmi törvény 3. részét) valamely követelményének megsértése miatt szenved kárt, kivéve, ha az adatkezelő vagy az adatfeldolgozó bizonyítja, hogy az adatkezelő vagy adatfeldolgozó semmilyen módon nem felelős a kárt okozó eseményért. A kártérítés kiterjed mind az anyagi veszteségre, mind a nem vagyoni kárra, például a sérelemre.

(119) Negyedszer, amennyiben bárki úgy ítéli meg, hogy a hatóságok megsértették jogait, beleértve a magánélethez és az adatvédelemhez fűződő jogokat, az 1998. évi emberi jogi törvény alapján jogorvoslatot kaphat az Egyesült Királyság bíróságai előtt. A 2018. évi adatvédelmi törvény 3. része szerinti adatkezelők – vagyis az illetékes hatóságok – mindig az 1998. évi emberi jogi törvény értelmében vett hatóságok. Az a személy, aki azt állítja, hogy egy hatóság olyan módon járt el (vagy olyan eljárást javasol), amely összeegyeztethetetlen az egyezmény szerinti joggal, következésképpen az 1998. évi emberi jogi törvény 6. szakaszának (1) bekezdése alapján jogellenes, eljárást indíthat a hatóság ellen a megfelelő bíróság vagy törvényszék előtt, vagy bármely bírósági eljárásban hivatkozhat az érintett jogokra, amennyiben a jogellenes cselekmény áldozata (vagy az lenne) ([197]).

([192]) A 2018. évi adatvédelmi törvény 165. szakasza.

([193]) A 2018. évi adatvédelmi törvény 166. szakasza konkrétan az alábbi helyzetekre utal: a) a biztos nem tesz megfelelő intézkedéseket a panasz megválaszolására, b) a biztos nem ad a panaszosnak tájékoztatást a panasz állásáról vagy kimeneteléről a panasz biztos általi kézhezvételétől számított 3 hónapos időszak végéig, vagy c) ha a panasz biztos általi vizsgálata ebben az időszakban nem fejeződik be, a következő három hónapos időszak alatt nem ad tájékoztatást erről a panaszosnak.

([194]) A First Tier Tribunal a kormányzati szabályozó szervek által hozott határozatok elleni fellebbezések elintézésére illetékes bíróság. Az információügyi biztos döntése esetén az illetékes tanács az „Általános szabályozói tanács", amelynek illetékessége az Egyesült Királyság egészére kiterjed.

([195]) A 2018. évi adatvédelmi törvény 166. szakasza.

([196]) A 2018. évi adatvédelmi törvény 161. és 162. szakasza.

([197]) Lásd a Met 2016. évi Brown kontra biztos ügyét, amelyben a bíróság a rendőrség ellen indított perben adatvédelmi összefüggésben jogorvoslatot nyújtott a felperes számára. A bíróság a felperes javára döntött, helyt adva igényének az 1998. évi adatvédelmi törvényből eredő kötelezettségek megsértése, az 1998. évi emberi jogi törvény (és az EJEE 8. cikkében foglalt kapcsolódó jog) megsértése, valamint a magáninformációkkal való visszaélés miatt (az alperes végül elismerte, hogy az adatvédelmi törvénybe és az EJEE-be ütközően járt el, ezért az ítélet a megfelelő jogorvoslatra összpontosított). E jogsértések következtében a bíróság pénzbeli kártérítést ítélt meg a felperesnek.

(120) Ha a bíróság valamely hatóság valamely cselekményét jogellenesnek találja, hatáskörein belül olyan kártérítést vagy jogorvoslatot adhat, illetve határozatot hozhat, amelyet igazságosnak és megfelelőnek tart ([198]). A bíróság összeegyeztethetetlennek nyilváníthatja az elsődleges jogszabályok valamely rendelkezését az EJEE által biztosított jogokkal is.

(121) Végül, a nemzeti jogorvoslatok kimerülése után az egyén az Emberi Jogok Európai Bíróságánál kérhet jogorvoslatot az EJEE által biztosított jogok megsértése miatt.

2.6. **Adatok további megosztása**

(122) Az Egyesült Királyság joga bizonyos feltételek mellett engedélyezi a bűnüldöző hatóságok számára az adatok más hatóságokkal való megosztását, a gyűjtés eredeti céljától eltérő célra (úgynevezett „további megosztás").

(123) Az (EU) 2016/680 irányelv 4. cikkének (2) bekezdésében előírtakhoz hasonlóan a 2018. évi adatvédelmi törvény 36. szakaszának (3) bekezdése lehetővé teszi az illetékes hatóságok által bűnüldözési célból gyűjtött személyes adatokat további feldolgozását (akár az eredeti adatkezelő vagy egy másik adatkezelő által) bármely más bűnüldözési célra, feltéve, hogy az adatkezelőt törvény felhatalmazza az adatok más célú kezelésére, és az adatkezelés szükséges és arányos ([199]). Ebben az esetben a 2018. évi adatvédelmi törvény 3. részében biztosított és a fent elemzett összes biztosíték vonatkozik a fogadó hatóság által végzett adatkezelésre.

(124) Az Egyesült Királyság jogrendjében különböző törvények kifejezetten megengedik a további megosztást. Különösen: i. a Digital Economy Act 2017 elnevezésű (a digitális gazdaságról szóló 2017. évi) törvény lehetővé teszi a hatóságok közötti megosztást többféle célra, például az állami szektorral szembeni bármilyen csalás esetén, amely egy hatóság számára veszteséggel vagy veszteség kockázatával járna ([200]) vagy hatósággal vagy az állammal szemben fennálló tartozás esetén ([201]); ii. a Crime and Courts Act 2013 elnevezésű (a bűncselekményekről és bíróságokról szóló 2013. évi) törvény lehetővé teszi az információk Nemzeti Bűnügyi Ügynökséggel (NCA) ([202]) való megosztását a súlyos bűncselekmények és a szervezett bűnözés elleni küzdelem, azok nyomozása és a büntetőeljárás lefolytatása érdekében; iii. a Serious Crime Act 2007 elnevezésű (a súlyos bűncselekményekről szóló 2007. évi) törvény lehetővé teszi a hatóságok számára, hogy csalás megelőzése céljából információkat közöljenek a csalásellenes szervezetekkel ([203]).

(125) Ezek a törvények kifejezetten előírják, hogy az információmegosztásnak meg kell felelnie a 2018. évi adatvédelmi törvényben meghatározott szabályoknak. Emellett a Rendészeti Főiskola kiadta az információmegosztás engedélyezett szakmai gyakorlatát ([204]) a rendőrségnek az Egyesült Királyság általános adatvédelmi rendelete, adatvédelmi törvény és 1998. évi emberi jogi törvény szerinti adatvédelmi kötelezettségeik teljesítésében történő segítségnyújtás céljából. A megosztás irányadó adatvédelmi jogi keretnek való megfelelése tekintetében természetesen bírósági felülvizsgálatnak helye van ([205]).

(126) Ezenkívül az (EU) 2016/680 irányelv 9. cikkében foglaltakhoz hasonlóan a 2018. évi adatvédelmi törvény előírja, hogy a bűnüldözési célokból gyűjtött személyes adatokat a bűnüldözés céljától eltérő célból is fel lehet dolgozni, amennyiben az adatkezelést törvény engedélyezi ([206]). Ez a típusú megosztás két esetkört ölel fel: 1) amikor a bűnüldöző hatóság az adatokat egy hírszerző ügynökségnek nem minősülő, nem bűnüldöző végrehajtó hatósággal osztja meg (például pénzügyi vagy adóhatóság, versenyhatóság, ifjúsági jóléti hivatal); 2) amikor a bűnüldöző hatóság az adatokat hírszerző ügynökséggel osztja meg. Az első esetkör szerint a személyes adatok feldolgozása az

([198]) Az 1998. évi emberi jogi törvény 8. szakaszának (1) bekezdése.

([199]) A 2018. évi adatvédelmi törvény 36. szakaszának (3) bekezdése.

([200]) A digitális gazdaságról szóló 2017. évi törvény 56. szakasza, elérhető az alábbi linken https://www.legislation.gov.uk/ukpga/2017/30/contents

([201]) A digitális gazdaságról szóló 2017. évi törvény 48. szakasza.

([202]) A bűncselekményekről és bíróságokról szóló 2013. évi törvény 7. szakasza az alábbi linken érhető el: https://www.legislation.gov.uk/ukpga/2013/22/contents

([203]) A súlyos bűncselekményekről szóló 2007. évi törvény 68. szakasza, elérhető az alábbi linken https://www.legislation.gov.uk/ukpga/2007/27/contents

([204]) Az információmegosztás engedélyezett szakmai gyakorlata a következő linken érhető el: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

([205]) Lásd például az M kontra the Chief Constable of Sussex Police ügyet (2019 EWHC 975 (Admin)), amelyben a Legfelsőbb Bíróságot arra kérték, hogy fontolja meg az adatok megosztását a rendőrség és az üzleti bűncselekmények visszaszorítását célzó partnerség (Business Crime Reduction Partnership – BCRP) között, amely szervezet felhatalmazást kapott a kitiltási értesítés rendszer kezelésére, megtiltva személyeknek tagjaik üzleti helyiségeibe való belépést. A bíróság felülvizsgálta az adatmegosztást, amely a lakosság védelme és a bűncselekmények megelőzése céljából létrejött megállapodás alapján zajlott, és végül arra a következtetésre jutott, hogy az adatmegosztás legtöbb vonatkozása jogszerű volt, a rendőrség és a BCRP között megosztott néhány különleges adat kivételével. Egy másik példa a Cooper kontra NCA ügy (2019 EWCA Civ 16), amelyben a Court of Appeal helybenhagyta az adatok rendőrség és a Súlyos Szervezett Bűnözés Elleni Ügynökség (SOCA, amely egy bűnüldöző szerv, jelenleg az NCA része) között megosztását.

([206]) A 2018. évi adatvédelmi törvény 36. szakaszának (4) bekezdése.

Egyesült Királyság általános adatvédelmi rendeletének, valamint a 2018. évi adatvédelmi törvény 2. részének hatálya alá tartozik. Az (EU) 2016/679 rendelet alapján elfogadott határozatban előírtak szerint az Egyesült Királyság általános adatvédelmi rendelete és a 2018. évi adatvédelmi törvény 2. része által biztosított biztosítékok olyan szintű védelmet nyújtanak, amely lényegében megegyezik az Unión belül biztosított védelemmel ([207]).

(127) A második esetkörben a bűnüldöző hatóságok által nemzetbiztonsági célokból gyűjtött adatok hírszerző ügynökséggel történő megosztása tekintetében az említett megosztás jogalapja a Counter Terrorism Act 2008 elnevezésű (terrorizmus elleni 2008. évi) törvény ([208]). A terrorizmus elleni 2008. évi törvény alapján bárki információt adhat bármely hírszerző ügynökségnek az ügynökség bármely feladatának ellátása céljából, beleértve a „nemzetbiztonságot" is.

(128) Az adatok nemzetbiztonsági célú megosztását illetően a hírszerző ügynökségekről szóló törvény és a biztonsági szolgálatokról szóló törvény a törvényi funkcióik ellátásához szükséges mértékre korlátozza a hírszerző ügynökségek adatszerzési képességét. A 2018. évi adatvédelmi törvény 3. részének hatálya alá tartozó, az adatok hírszerző ügynökségekkel történő megosztására törekvő illetékes hatóságoknak az ügynökségek jogszerű feladatain túlmenően számos tényezőt/korlátozást is figyelembe kell venniük, amelyeket a hírszerző ügynökségekről szóló törvény és a biztonsági szolgálatokról szóló törvény ([209]) határoz meg. A terrorizmus elleni 2008. évi törvény 20. szakasza egyértelművé teszi, hogy a terrorizmus elleni 2008. évi törvény 19. szakasza szerinti adatmegosztásnak továbbra is meg kell felelnie az adatvédelmi jogszabályoknak; ami azt jelenti, hogy a 2018. évi adatvédelmi törvény összes korlátozása és követelménye érvényesül. Ezenkívül a bűnüldöző hatóságok és a hírszerző ügynökségek az 1998. évi emberi jogi törvény alkalmazásában hatóságok, és ezért biztosítaniuk kell, hogy az EJEE által garantált jogokkal – ideértve annak 8. cikkét is – összhangban járjanak el. Más megfogalmazásban ezek a követelmények azt jelentik, hogy a bűnüldöző szervek és a hírszerző ügynökség közötti minden adatmegosztásnak meg kell felelnie az adatvédelmi jogszabályoknak és az EJEE-nek.

(129) A bűnüldöző hatóságoktól kapott vagy megszerzett személyes adatok hírszerző ügynökségek általi, nemzetbiztonsági célokra történő kezelésére számos feltétel és biztosíték vonatkozik ([210]). A 2018. évi adatvédelmi törvény 4. része a hírszerző ügynökség által vagy nevében végzett minden adatkezelésre vonatkozik, meghatározza

([207]) A Bizottság C(2021)4800 végrehajtási határozata a személyes adatok Egyesült Királyság általi megfelelő védelméről szóló (EU) 2016/679 európai parlamenti és tanácsi rendelet szerint.

([208]) A terrorizmus elleni 2008. évi törvény 19. szakasza a következő linken érhető el: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([209]) A hírszerző ügynökségekről szóló 1994. évi törvény 2. szakaszának (2) bekezdése (lásd: https://www.legislation.gov.uk/ukpga/1994/13/contents) kimondja, hogy „A hírszerző ügynökség vezetője felelős a szolgálat hatékonyságáért, és kötelessége gondoskodni arról, hogy a) azt biztosító szabályozás legyen érvényben, hogy a hírszerző ügynökség ne gyűjtsön olyan adatokat, amelyek a feladatai megfelelő ellátásához nem szükségesek, és hogy semmiféle információt ne hozzon nyilvánosságra, kivéve, ha az szükséges i. feladatai megfelelő ellátásának céljából; ii. a nemzetbiztonság érdekében; iii. súlyos bűncselekmények megelőzése vagy felderítése céljából; vagy a) bármely büntetőeljárás céljaira; és b) a hírszerző ügynökség ne tegyen semmilyen lépést az Egyesült Királyság valamely politikai pártja érdekeinek érvényre juttatása érdekében", míg a biztonsági szolgálatokról szóló 1989. évi törvény 2. szakaszának (2) bekezdése (lásd: https://www.legislation.gov.uk/ukpga/1989/5/contents) kimondja, hogy „A főigazgató felelős a szolgálat hatékonyságáért, és kötelessége biztosítani, hogy a) azt biztosító szabályozás legyen érvényben, hogy a szolgálat ne gyűjtsön olyan adatokat, amelyek a feladatai megfelelő ellátásához nem szükségesek, és hogy semmiféle információt ne hozzon nyilvánosságra, kivéve, ha ez súlyos bűncselekmények megelőzése vagy felderítése, vagy bármely büntetőeljárás céljából szükséges; és b) a szolgálat ne tegyen semmilyen lépést az Egyesült Királyság valamely politikai pártja érdekeinek érvényre juttatása érdekében; és c) a Nemzeti Bűnügyi Ügynökség főigazgatójával egyeztetett szabályozás létezzen a szolgálat tevékenységének e törvény 1. szakasza (4) bekezdésének megfelelően a rendőrség, a Nemzeti Bűnügyi Ügynökség tevékenységével és más bűnüldöző szervek tevékenységével történő összehangolására".

([210]) A hírszerző ügynökség hatásköreire vonatkozó biztosítékokat és korlátozásokat a Investigatory Powers Act 2016 elnevezésű (a nyomozati hatáskörökről szóló 2016. évi) törvény is szabályozza, amely Anglia, Wales és Észak-Írország vonatkozásában a Regulation of Investigatory Powers Act 2000 elnevezésű (a nyomozati hatáskörök szabályozásáról szóló 2000. évi) törvénnyel, valamint Skócia vonatkozásában Regulation of Investigatory Powers (Scotland) Act 2000 (a nyomozati hatáskörök (Skócia) szabályozásáról szóló 2000. évi) törvénnyel együtt adja az említett hatáskörök igénybevételének jogalapját. Ezek a hatáskörök azonban nem relevánsak a „további megosztás" keretében, mivel a személyes adatok hírszerző ügynökségek általi közvetlen gyűjtésére vonatkoznak. A hírszerző ügynökségeknek a nyomozati hatáskörökről szóló törvény alapján biztosított hatáskörök értékeléséhez lásd a személyes adatok Egyesült Királyság általi megfelelő védelméről szóló (EU) 2016/679 európai parlamenti és tanácsi rendelet szerinti C(2021)4800 bizottsági végrehajtási határozatot.

a fő adatvédelmi elveket (jogszerűség, tisztesség és átláthatóság) ([211]); célhoz kötöttség ([212]); adattakarékosság ([213]); pontosság ([214]); tárolás korlátozása ([215]) és biztonság ([216]), feltételeket szab a különleges adatok kategóriáinak kezelésére ([217]), rendelkezik az érintettek jogairól ([218]), megköveteli a beépített adatvédelmet ([219]) és szabályozza a személyes adatok nemzetközi továbbítását ([220]).

(130) Ugyanakkor a 2018. évi adatvédelmi törvény 110. szakasza kivételt ír elő a 2018. évi adatvédelmi törvény 4. részének meghatározott rendelkezései alól, amennyiben az említett kivételre a nemzetbiztonság megőrzése érdekében van szükség. A 2018. évi adatvédelmi törvény 110. szakaszának (2) bekezdése sorolja fel azokat a rendelkezéseket, amelyek alól kivétel engedélyezhető. Ide tartoznak az adatvédelmi elvek (a jogszerűség elvének kivételével), az érintettek jogai, az információügyi biztos tájékoztatásának kötelezettsége a személyes adatok megsértéséről, az információügyi biztos nemzetközi kötelezettségeknek megfelelő ellenőrzési hatásköre, az információügyi biztos bizonyos végrehajtási hatáskörei, az egyes adatvédelmi megsértéseket bűncselekménnyé nyilvánító rendelkezések, valamint az adatkezelés speciális, például újságírói, tudományos vagy művészeti céljaira, vonatkozó rendelkezések. Ezt a kivételt eseti elemzés alapján lehet igénybe venni ([221]). Amint azt az Egyesült Királyság hatóságai kifejtették és az Egyesült Királyság bíróságainak ítélkezési gyakorlata megerősítette, „a) az adatkezelőnek mérlegelnie kell a nemzetbiztonságra vagy a védelemre gyakorolt tényleges következményeket, ha be kellene tartaniuk az adott adatvédelmi rendelkezést, és ha észszerűen eleget tudnak tenni a szokásos szabálynak a nemzetbiztonság vagy a védelem befolyásolása nélkül" ([222]). Az, hogy a kivételt megfelelően alkalmazzák-e, a biztos felügyelete alá tartozik ([223]).

([211]) A 2018. évi adatvédelmi törvény 86. szakaszának (6) bekezdése értelmében az adatkezelés tisztességességének és átláthatóságának meghatározásához figyelembe kell venni az adatok megszerzésének módját. Ebben az értelemben a méltányosság és az átláthatóság követelménye akkor teljesül, ha az adatokat olyan személytől szerzik be, aki az adatszolgáltatásra jogszerűen felhatalmazott vagy köteles.

([212]) A 2018. évi adatvédelmi törvény 87. szakasza szerint az adatkezelés céljait meg kell határozni, azoknak egyértelműnek és jogszerűnek kell lenniük. Az adatokat tilos olyan módon kezelni, amely összeegyeztethetetlen azokkal a célokkal, amelyekre azokat gyűjtik. A 87. szakasz (3) bekezdése értelmében a személyes adatok összeegyeztethető további kezelése csak akkor engedélyezhető, ha az adatkezelőt törvény hatalmazza fel az adatok e célból történő kezelésére, és az adatkezelés szükséges és arányos e másik célra. Az adatkezelést összeegyeztethetőnek kell tekinteni, ha az adatkezelés közérdekű, tudományos vagy történelmi kutatási vagy statisztikai célú archiválási célú feldolgozásból áll, és megfelelő biztosítékok vonatkoznak arra (a 2018. évi adatvédelmi törvény 87. szakaszának (4) bekezdése).

([213]) A személyes adatoknak megfelelőnek, relevánsnak és nem eltúlzott mértékűnek kell lenniük (a 2018. évi adatvédelmi törvény 88. szakasza).

([214]) A személyes adatoknak pontosnak és naprakésznek kell lenniük (a 2018. évi adatvédelmi törvény 89. szakasza).

([215]) A személyes adatokat tilos a szükségesnél tovább tárolni (a 2018. évi adatvédelmi törvény 90. szakasza).

([216]) A hatodik adatvédelmi elv az, hogy a személyes adatokat olyan módon kell kezelni, amely magában foglalja a személyes adatok kezeléséből eredő kockázatokkal kapcsolatos megfelelő biztonsági intézkedések meghozatalát. A kockázatok közé tartozik (a teljesség igénye nélkül) a személyes adatokhoz véletlenszerű vagy illetéktelenek általi hozzáférés, illetve azok megsemmisítése, elvesztése, felhasználása, módosítása vagy közlése (a 2018. évi adatvédelmi törvény 91. szakasza). A 107. szakasz előírja továbbá, hogy (1) minden adatkezelőnek be kell vezetnie a személyes adatok kezeléséből eredő kockázatoknak megfelelő biztonsági intézkedéseket, és (2) automatizált feldolgozás esetén minden adatkezelő és minden adatfeldolgozó a kockázat értékelése alapján megelőző vagy enyhítő intézkedéseket hajt végre.

([217]) A 2018. évi adatvédelmi törvény 86. szakasza (2) bekezdésének b) pontja és 10. melléklete.

([218]) A 2018. évi adatvédelmi törvény 4. részének 3. fejezete, nevezetesen az alábbiakra vonatkozó jogok: hozzáférés, helyesbítés és törlés, tiltakozás az adatkezelés ellen, és az automatizált döntéshozatal elutasítása, beavatkozás az automatizált döntéshozatalba és tájékoztatás a döntéshozatalról. Ezenkívül az adatkezelőnek tájékoztatást kell adnia az érintettnek személyes adatainak kezeléséről.

([219]) A 2018. évi adatvédelmi törvény 103. szakasza.

([220]) A 2018. évi adatvédelmi törvény 109. szakasza. Személyes adatok továbbítása nemzetközi szervezeteknek vagy az Egyesült Királyságon kívüli országoknak akkor lehetséges, ha az adattovábbítás szükséges és arányos intézkedés, amelyet az adatkezelő jogszabályi funkcióinak vagy a biztonsági szolgálatról szóló 1989. évi törvény és a hírszerző ügynökségekről szóló 1994. évi törvény egyes szakaszaiban előírt egyéb céloknak megfelelően hajtanak végre.

([221]) Lásd a Baker kontra Secretary of State for the Home Department ügyet (2001 UKIT NSA2) („Baker kontra miniszter ügy").

([222]) Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonsági adatvédelmi és vizsgálati hatásköri keret, 15–16. oldal, elérhető a következő linken https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf Lásd még Baker kontra miniszter ügyet (lásd a 220. lábjegyzetet), amelyben a Törvényszék megsemmisítette a belügyminiszter által kiállított és a nemzetbiztonsági kivétel alkalmazását megerősítő nemzetbiztonsági tanúsítványt, mivel úgy ítélte meg, hogy nincs oka általános mentesség megadására a hozzáférési kérelmek megválaszolásának kötelezettsége alól, és hogy az említett kivétel eseti elemzés nélkül minden körülmények között történő alkalmazása meghaladná a nemzetbiztonság védelméhez szükséges és arányos mértéket.

([223]) Lásd a biztos és az UKIC közötti egyetértési megállapodást, amely szerint „amikor a biztos panaszt kap egy érintettől, az információügyi biztos meg kíván győződni arról, hogy a kérdést helyesen kezelték, és adott esetben a mentesség alkalmazását megfelelően vették igénybe" (az Információügyi Bizottság Irodája és az Egyesült Királyság Hírszerző Közössége közötti egyetértési megállapodás 16. pontja, elérhető az alábbi linken: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Ezenkívül a fent említett jogok bármelyike korlátozásának lehetőségével kapcsolatban a 2018. évi adatvédelmi törvény 79. szakasza előírja, hogy a „nemzetbiztonság” érdekében az adatkezelő kérhet a kabinetminiszter vagy a legfőbb ügyész által aláírt tanúsítványt, amely tanúsítja, hogy az említett jogok korlátozása jelenleg vagy mindenkor szükséges és arányos intézkedés a nemzetbiztonság védelme érdekében ([224]). Az Egyesült Királyság kormánya útmutatót adott ki a 2018. évi adatvédelmi törvény szerint a nemzeti biztonsági tanúsítványokról, amely kiemeli, hogy az érintettek jogai korlátozásának a nemzetbiztonság védelme érdekében arányosnak és szükségesnek kell lennie ([225]). Valamennyi nemzeti biztonsági tanúsítványt közzé kell tenni a biztos honlapján ([226]).

(132) A tanúsítvány meghatározott időtartamra, legfeljebb öt évre szólhat, ezért azt a végrehajtó hatalom rendszeresen felülvizsgálja ([227]). A tanúsítványban meg kell jelölni a kivétel hatálya alá tartozó személyes adatokat vagy személyesadat-kategóriákat, valamint a 2018. évi adatvédelmi törvény azon rendelkezéseit, amelyekre a kivétel vonatkozik ([228]).

(133) Fontos megjegyezni, hogy a nemzetbiztonsági tanúsítványok nem jelentenek további alapot az adatvédelmi jogok nemzetbiztonsági okokból történő korlátozásához. Más megfogalmazásban: az adatkezelő vagy az adatfeldolgozó csak akkor veheti igénybe a tanúsítványt, ha megállapítást nyert, hogy szükség van a nemzetbiztonsági kivételre, amelyet esetenkénti alapon kell alkalmazni. Még ha nemzetbiztonsági tanúsítvány is vonatkozik a szóban forgó kérdésre, a biztos megvizsgálhatja, hogy a nemzetbiztonsági kivételre hivatkozás egy adott esetben indokolt volt-e ([229]).

(134) Bármely személy, akit a tanúsítvány kiállítása közvetlenül érint, fellebbezést nyújthat be a Felsőbb Törvényszékhez ([230]) a tanúsítvány ellen ([231]) vagy ha a tanúsítvány általános leírás alapján azonosítja az adatokat, megtámadhatja a tanúsítvány konkrét adatokra való alkalmazását ([232]).

(135) A törvényszék felülvizsgálja a tanúsítvány kiadásáról szóló határozatot, és dönt, hogy volt-e észszerű indok a tanúsítvány kiadására ([233]). Számos kérdést mérlegelhet, beleértve a szükségességet, az arányosságot és a jogszerűséget, figyelemmel az érintettek jogaira gyakorolt hatásra, és a nemzetbiztonság védelme szükségességének kiegyensúlyozására. Ennek eredményeként a bíróság megállapíthatja, hogy a tanúsítvány nem vonatkozik a fellebbezés tárgyát képező konkrét személyes adatokra ([234]).

([224]) A 2018. évi adatvédelmi törvény megszüntette a tanúsítvány az 1998. évi adatvédelmi törvény 28. cikkének (2) bekezdése alapján történő kiállításának lehetőségét. A „régi tanúsítványok” kiadásának lehetősége azonban továbbra is fennáll annyiban, amennyiben az 1998. évi törvény szerinti történelmi kihívás áll fenn (lásd a 2018. évi adatvédelmi törvény20. melléklete 5. részének 17. pontját). Ez a lehetőség azonban nagyon ritkának tűnik, és csak korlátozott esetekben fog érvényesülni, például, amikor az érintett kihívást jelent a nemzetbiztonsági mentesség olyan hatóság általi adatkezeléshez kapcsolódó alkalmazásával kapcsolatban, amely az adatkezelést az 1998. évi törvény szerint végezte. Meg kell jegyezni, hogy ezekben az esetekben az 1998. évi adatvédelmi törvény 28. szakasza teljes egészében alkalmazandó, ideértve a tanúsítvány érintett általi megtámadásának lehetőségét is. Jelenleg nincsenek az 1998. évi adatvédelmi törvény szerint kibocsátott nemzetbiztonsági tanúsítványok.

([225]) Az Egyesült Királyság kormányának útmutatója a 2018. évi adatvédelmi törvény szerinti nemzetbiztonsági tanúsítványokról, amely a következő linken érhető el: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

([226]) A 2018. évi adatvédelmi törvény 130. szakasza szerint a biztos dönthet úgy, hogy nem teszi közzé a tanúsítvány szövegét vagy annak egy részét, ha az ellentétben állna a nemzetbiztonsági érdekkel vagy a közérdekkel, vagy veszélyeztethetné bármely személy biztonságát. Ezekben az esetekben a biztos a tanúsítvány kiállításának tényét teszi közzé.

([227]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, 15. pont, lásd a 224. lábjegyzetet.

([228]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, 5. pont, 224. lábjegyzet.

([229]) A 2018. évi adatvédelmi törvény 102. szakasza előírja, hogy az adatkezelőnek képesnek kell lennie annak bizonyítására, hogy betartotta a 2018. évi adatvédelmi törvényt. Ez azt jelenti, hogy egy hírszerző ügynökségnek igazolnia kell a biztosnak, hogy a kivétel igénybevételekor figyelembe vette az eset sajátos körülményeit. A biztos egyben közzéteszi a nemzetbiztonsági tanúsítványok nyilvántartását, amely a következő linken érhető el: elérhető az alábbi linken: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) A Felső Törvényszék az alsóbb közigazgatási bíróságok által hozott határozatok elleni fellebbezések elbírálására illetékes bíróság, és különleges hatáskörrel rendelkezik bizonyos kormányzati szervek határozatai elleni közvetlen fellebbezésekre.

([231]) A 2018. évi adatvédelmi törvény 111. szakaszának (3) bekezdése.

([232]) A 2018. évi adatvédelmi törvény 111. szakaszának (5) bekezdése.

([233]) A Baker kontra miniszter ügyben (lásd a 221. lábjegyzetet) a Törvényszék megsemmisítette a belügyminiszter által kiadott nemzetbiztonsági tanúsítványt, mivel úgy ítélte meg, hogy nincs ok a hozzáférési kérelmek megválaszolásának kötelezettsége alóli általános mentesség megadására, és hogy az említett kivétel eseti elemzés nélkül minden körülmények között történő alkalmazása meghaladná a nemzetbiztonság védelméhez szükséges és arányos mértéket.

([234]) Az Egyesült Királyság kormányának útmutatója a nemzetbiztonsági tanúsítványokról, 25. pont, 224. lábjegyzet.

(136) A lehetséges korlátozások egy másik csoportja a 2018. évi adatvédelmi törvény 11. melléklete alapján a 2018. évi adatvédelmi törvény 4. részének egyes rendelkezéseire ([235]) egyéb fontos általános közérdekű vagy védett érdekek – például parlamenti kiváltságok, jogi szakmai kiváltságok (ügyvédi titoktartás), bírósági eljárások lefolytatása vagy a fegyveres erők harci hatékonysága – védelmére alkalmazott korlátozásokat érinti. Ezeknek a rendelkezéseknek az alkalmazása alóli kivétel bizonyos adatkategóriákra vonatkozik („csoportalapú"), vagy pedig a kivétel annyiban érvényesül, amennyiben e rendelkezések alkalmazása valószínűleg sérti a védett érdekeket („sérelem alapú") ([236]). A sérelmen alapuló kivételekre csak akkor lehet hivatkozni, amennyiben a felsorolt adatvédelmi rendelkezések alkalmazása valószínűleg sérti a szóban forgó konkrét érdekeket. A kivétel alkalmazását ezért mindig indokolni kell az adott esetben valószínűleg bekövetkező, releváns sérelemre való hivatkozással. Csoportalapú kivételekre csak azon konkrét, szűken meghatározott adatkategóriák esetében lehet hivatkozni, amelyekre a mentességet megadják. Ezek célja és hatása hasonló az Egyesült Királyság általános adatvédelmi rendelete alóli számos kivételhez (a 2018. évi adatvédelmi törvény 2. melléklete alapján), amelyek viszont tükrözik a GDPR 23. cikkében foglaltakat.

(137) A fentiekből következik, hogy az alkalmazandó egyesült királyságbeli jogszabályi rendelkezések tekintetében – a bíróságok és az Információügyi Bizottság által is értelmezett – korlátozások és feltételek érvényesülnek annak biztosítása érdekében, hogy ezek a kivételek és korlátozások a nemzetbiztonság védelméhez szükséges és arányos határokon belül maradjanak.

(138) A személyes adatok hírszerző ügynökségek által a 2018. évi adatvédelmi törvény 4. része alapján végzett kezelését az információügyi biztos felügyeli ([237]).

(139) Az információügyi biztos általános feladatait a személyes adatok hírszerző ügynökségek általi, a 2018. évi adatvédelmi törvény 4. része szerinti kezelésével kapcsolatban a 2018. évi adatvédelmi törvény 13. melléklete állapítja meg. A feladatok a teljesség igénye nélkül magukban foglalják a 2018. évi adatvédelmi törvény 4. részének nyomon követését és végrehajtását, a közvélemény tudatosságának növelését, a Parlamentnek, a kormánynak és más intézményeknek történő tanácsadást a jogalkotási és közigazgatási intézkedések terén, az ellenőrök és adatfeldolgozók kötelezettségei tudatosításának előmozdítását, az érintettek tájékoztatását az érintett jogainak gyakorlásáról és vizsgálatok lefolytatását.

(140) A biztos – mint a 2018. évi adatvédelmi törvény 3. része esetében is – hatáskörrel rendelkezik arra, hogy értesítse az adatkezelőket az állítólagos jogsértésekről, és figyelmeztetéseket adjon ki, hogy egy adatkezelés valószínűleg a szabályokba ütközik, és a jogsértés megállapításakor megrovást ad. Kiadhat jogérvényesítési felhívást és bírságértesítőt is a törvény bizonyos rendelkezéseinek megsértése esetén ([238]). Ugyanakkor a 2018. évi adatvédelmi törvény más részeitől eltérően a biztos nem adhat ki vizsgálati felhívást a nemzetbiztonságnak ([239]).

(141) Ezenkívül a 2018. évi adatvédelmi törvény 110. szakasza kivételt tesz a biztos bizonyos hatásköreinek használata alól, amennyiben erre a nemzetbiztonság védelme érdekében van szükség. Idetartozik a biztos arra vonatkozó hatásköre, hogy az adatvédelmi törvény alapján (bármilyen típusú) felhívást adjon ki (adatkérési, vizsgálati,

([235]) Ez az alábbiakat foglalja magában: i. a 4. rész adatvédelmi elvei, kivéve az adatkezelés jogszerűségének első elv szerinti követelményét és azt a tényt, hogy az adatkezelésnek meg kell felelnie a 9. és 10. mellékletben meghatározott vonatkozó feltételek egyikének; ii. az érintettek jogai; és iii. a jogsértések biztosnak történő bejelentésével kapcsolatos kötelezettségek.

([236]) Az Egyesült Királyság magyarázata szerint a „csoportalapú" kivételek a következők: i. információk a korona kitüntetéseinek és méltóságainak elnyeréséről; ii. ügyvédi titoktartási kötelezettség; iii. bizalmas foglalkoztatási, képzési vagy oktatási referenciák; és iv. vizsgalapok és jegyek. A „sérelmen alapuló" kivételek a következő kérdéseket érintik: i. bűncselekmények megelőzése vagy felderítése; az elkövetők visszatartása és üldözése; ii. parlamenti kiváltság; iii. bírósági eljárások; iv. az állami fegyveres erők harci hatékonysága; v. az Egyesült Királyság gazdasági jóléte; vi. az érintettel folytatott tárgyalás; vii. tudományos vagy történelmi kutatás vagy statisztikai célok; viii. közérdekű archiválás. Az Egyesült Királyság magyarázata a megfelelőségi megbeszélésekre, H. szakasz: Nemzetbiztonság, 13. oldal, lásd a 222. lábjegyzetet

([237]) A 2018. évi adatvédelmi törvény 116. szakasza.

([238]) A 2018. évi adatvédelmi törvény 149. szakaszának (2) bekezdésének és 155. szakaszának együttes olvasatában jogérvényesítési és bírságértesítőket az adatkezelőnek vagy az adatfeldolgozónak lehet kiadni a következők megsértése miatt: a 2018. évi adatvédelmi törvény 4. részének 2. fejezete (az adatkezelés alapelvei), amely a 2018. évi adatvédelmi törvény 4. részének az érintetteknek jogokat biztosító rendelkezése, a személyes adatok megsértésének a biztosnak történő bejelentésének követelménye a 2018. évi adatvédelmi törvény 108. szakasza alapján, valamint a személyes adatok harmadik országoknak, az egyezményen kívüli országoknak és a nemzetközi szervezeteknek történő továbbításának a 2018. évi adatvédelmi törvény 109. szakaszában foglalt elvei. (A jogérvényesítési felhívással és bírságértesítővel kapcsolatos további részletekért lásd a (102)–(103) preambulumbekezdést).

([239]) A 2018. évi adatvédelmi törvény 147. szakaszának (6) bekezdése szerint az információügyi biztos nem adhat ki vizsgálati felhívást a 2000. évi információszabadságról szóló törvény 23. szakaszának (3) bekezdésében meghatározott szervnek. Ezek közé tartozik a biztonsági szolgálat (MI5), a titkosszolgálat (MI6) és a Kormányzati Kommunikációs Központ.

jogérvényesítési felhívás és bírságértesítők), a nemzetközi kötelezettségeknek megfelelő ellenőrzések elvégzésének hatásköre, a belépési és ellenőrzési jogkörök, valamint a bűncselekményekre vonatkozó szabályok ([240]). Amint azt a (136) preambulumbekezdés kifejti, ezek a kivételek csak szükség esetén és arányosan, eseti alapon érvényesülnek. A kivételek alkalmazása ellen bírósági felülvizsgálatnak lehet helye ([241]).

(142) A biztos és az Egyesült Királyság hírszerző ügynökségei egyetértési megállapodást írtak alá ([242]), amely létrehozza az együttműködés kereteit számos kérdésben, ideértve az adatvédelmi bejelentéseket és az érintettek panaszainak kezelését. Különösen azt írja elő, hogy a panasz kézhezvételekor a biztos értékeli, hogy a nemzetbiztonsági kivételre megfelelően hivatkoztak-e. A biztos által az egyedi panaszok vizsgálata kapcsán feltett kérdésekre 20 munkanapon belül választ kell adnia az érintettnek az Egyesült Királyság kormányának az adatvédelmi törvény szerinti nemzetbiztonsági tanúsítványokról szóló, megfelelő útmutatója szerint, megfelelő biztonságos csatornákon keresztül, ha minősített adatokat érint. 2018 áprilisától a mai napig a biztos 21 panaszt kapott magánszemélyektől a hírszerző ügynökségekkel kapcsolatban. Minden panaszt értékeltek, és az eredményről tájékoztatták az érintettet ([243]).

(143) Ezenkívül a Hírszerzési és Biztonsági Bizottság (ISC) parlamenti felügyeletet lát el a hírszerző ügynökségek által végzett adatkezelés felett. Ennek a bizottságnak a jogszabályi alapja a Justice and Security Act 2013 elnevezésű (2013. évi igazságügyi és biztonsági) törvény ([244]). A törvény az ISC-t az Egyesült Királyság Parlamentjének bizottságaként hozza létre. Az ISC tagjai a Parlament bármely házának képviselői, akiket a miniszterelnök nevez ki az ellenzék vezetőjével folytatott konzultációt követően ([245]). Az ISC-nek éves jelentést kell készítenie a Parlamentnek feladatai ellátásáról, valamint egyéb, általa megfelelőnek tartott jelentéseket ([246]).

(144) 2013 óta az ISC nagyobb hatásköröket kapott, ideértve a biztonsági szolgálatok operatív tevékenységeinek felügyeletét is. A 2013. évi igazságügyi és biztonsági törvény 2. szakasza értelmében az ISC feladata a nemzetbiztonsági ügynökségek kiadásainak, adminisztrációjának, politikájának és működésének felügyelete. A 2013. évi igazságügyi és biztonsági törvény meghatározza, hogy az ISC operatív kérdésekben vizsgálatokat

([240]) A kivétel körébe vonható rendelkezések a következők: a 108. szakasz (személyes adatok megsértésének bejelentése a biztosnak), 119. szakasz (ellenőrzés a nemzetközi kötelezettségeknek megfelelően); a 142–154. szakasz és 15. melléklet (a biztos felhívásai, belépési és ellenőrzési jogkörök); és a 170–173. szakasz (személyes adatokkal kapcsolatos bűncselekmények). A hírszerző ügynökség által végzett adatkezelés mellett a 13. melléklet (a biztos egyéb általános feladatai) 1. pontjának a) és g) alpontjában, valamint a 2. pontjában szereplő kezeléssel kapcsolatban.

([241]) Lásd például a Baker kontra Secretary of State for the Home Department ügyet (lásd a 221. lábjegyzetet)

([242]) A biztos és az Egyesült Királyság Hírszerző Közössége közötti egyetértési megállapodás, lásd a 231. lábjegyzetet.

([243]) Ezen esetek közül hétben a biztos azt tanácsolta a panaszosnak, hogy aggályaival forduljon az adatkezelőhöz (ez az eset áll fenn, amikor egy magánszemély aggályait a biztosnál veti fel, de előbb az adatkezelőhöz kellett volna fordulnia), az egyik ilyen esetekben a biztos általános tanácsokkal látta el az adatkezelőt (ezt akkor veszik igénybe, ha az adatkezelő intézkedései nem tűnnek jogsértőnek, de a gyakorlatok javításával megelőzhető a biztosnál aggályok felvetése), és a másik 13 esetben az adatkezelőtől nem volt szükség semmilyen intézkedésre (ezt akkor veszik igénybe, ha az egyén által felvetett aggályok valóban a 2018. évi adatvédelmi törvény hatálya alá tartoznak, mert személyes adatok kezelésére vonatkoznak, de az adatkezelő az általa szolgáltatott információk alapján a jelek szerint nem sértette meg a jogszabályokat).

([244]) Amint azt az Egyesült Királyság hatóságai kifejtették, az igazságügyi és biztonsági törvény kibővítette az ISC hatáskörét, és szerepet kapott a három ügynökségen túl a hírszerzési közösség felügyeletében, és lehetővé tette az ügynökségek operatív tevékenységeinek visszamenőleges felügyeletét jelentős nemzeti érdekű kérdésekben.

([245]) Lásd a 2013. évi igazságügyi és biztonsági törvény 1. szakaszát. A miniszterek nem lehetnek tagok. A tagok az ISC-n belül azon parlamenti ciklus alatt töltik be tisztségüket, amely alatt kinevezték őket. Elmozdíthatók azon ház határozatával, amely kinevezte őket, vagy ha megszűnik képviselői tisztségük, vagy miniszterré válnak. A tag le is mondhat.

([246]) A bizottság jelentései és nyilatkozatai online elérhetők az alábbi linken: http://isc.independent.gov.uk/committee-reports. Az ISC 2015-ben jelentést adott ki „Adatvédelem és biztonság: Korszerű és átlátható jogi keret” címmel (lásd: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), amelyben megvizsgálta a hírszerző ügynökségek által alkalmazott megfigyelési technikák jogi kereteit, és egy sor ajánlást adott ki, amelyeket ezután figyelembe vettek és beépítettek a nyomozati hatáskörökről szóló, törvénnyé átalakult törvényjavaslatba, a vizsgálati hatáskörökről szóló 2016. évi törvénybe. A kormány adatvédelmi és biztonsági jelentésre adott válasza az következő linken érhető el: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

folytathat le, ha azok nem folyamatban lévő műveletekhez kapcsolódnak ([247]). A miniszterelnök és az ISC között megkötött egyetértési megállapodás ([248]) részletesen meghatározza azokat az elemeket, amelyeket figyelembe kell venni annak mérlegelésekor, hogy egy tevékenység nem része-e valamely folyamatban lévő műveletnek ([249]). Az ISC-t felkérheti a miniszterelnök is a folyamatban lévő műveletek kivizsgálására, és felülvizsgálhatja az ügynökségek által önkéntesen szolgáltatott információkat.

(145) A 2013. évi igazságügyi és biztonsági törvény 1. melléklete értelmében az ISC felkérheti a három hírszerző ügynökség bármelyikének vezetőjét, hogy adjon ki adatokat. Az ügynökségnek hozzáférhetővé kell tennie ezeket az adatokat, kivéve, ha a miniszter megvétózza ezt ([250]). Az Egyesült Királyság hatóságai kifejtették, hogy a gyakorlatban nagyon kevés információt tartanak vissza az ISC-től ([251]).

(146) A jogorvoslattal kapcsolatban: először is az érintett a 2018. évi adatvédelmi törvény 165. szakaszának (2) bekezdése alapján panaszt nyújthat be a biztoshoz, ha úgy véli, hogy a rá vonatkozó személyes adatokkal kapcsolatban a 2018. évi adatvédelmi törvény 4. részét megsértették, ideértve a nemzetbiztonsági eltérések és korlátozások visszaélésszerű használatát.

(147) Ezenkívül a 2018. évi adatvédelmi törvény 4. része értelmében az egyének jogosultak a High Courttól (vagy Skóciában a Court of Sessiontől) kérni az adatkezelő kötelezését az adatokhoz való hozzáféréshez ([252]), az adatkezelés elleni tiltakozáshoz ([253]), a helyesbítéshez vagy a törléshez való jog tiszteletben tartására.

(148) A magánszemélyek jogosultak az adatkezelőtől vagy az adatfeldolgozótól kérni a 2018. évi adatvédelmi törvény 4. részében foglalt követelmények megsértése miatt elszenvedett károk megtérítését is ([254]). A kártérítés kiterjed mind az anyagi veszteségre, mind a nem vagyoni kárra, például a sérelemre ([255]).

(149) Végül az egyén panaszt nyújthat be az Investigatory Powers Tribunalhoz az Egyesült Királyság hírszerző ügynökségei által vagy képviseletében elkövetett bármilyen magatartás miatt ([256]). A nyomozati hatáskörrel foglalkozó bíróságot (Investigatory Powers Tribunal – IPT) Anglia, Wales és Észak-Írország vonatkozásában a Regulation of Investigatory Powers Act 2000 elnevezésű (a nyomozati hatáskörök szabályozásáról szóló 2000. évi) törvénnyel, valamint Skócia vonatkozásában a Regulation of Investigatory Powers (Scotland) Act 2000 (a nyomozati hatáskörök (Skócia) szabályozásáról szóló 2000. évi) törvénnyel (a továbbiakban: a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény) hozták létre, és független a végrehajtó hatalomtól ([257]). A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának megfelelően az IPT tagjait Őfelsége nevezi ki ötéves időtartamra.

(150) A Törvényszék egy tagját Őfelsége felmentheti a Parlament mindkét házához ([258]) intézett indítvánnyal ([259]).

(151) Az IPT-nél kereset benyújtása előtt („perelhetőségi követelmény”) a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakasza szerint az egyénnek meg kell győződnie arról, hogy i. a hírszerző ügynökség eljárása vele, vagyonával, bármely általa küldött vagy neki szánt kommunikációval, vagy bármilyen postai szolgáltatás, telekommunikációs szolgáltatás vagy távközlési rendszer igénybevételével kapcsolatos ([260]) és ii. hogy a

([247]) Lásd a 2013. évi igazságügyi és biztonsági törvény 2. szakaszát.
([248]) A miniszterelnök és az ISC közötti egyetértési megállapodás, amely a következő linken érhető el: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) A miniszterelnök és az ISC közötti egyetértési megállapodás, 14. pont, lásd a 248. lábjegyzetet.
([250]) A miniszter csak két okból vétózhatja meg az információk közlését: az információ különleges adat és nemzetbiztonsági érdekből nem szabad az ISC elé tárni; vagy olyan jellegű információról van szó, hogy ha a minisztert arra kérnék fel, hogy mutassa be azt az alsóház egyik minisztériumi választott bizottsága előtt, a miniszter úgy ítélné meg (nem kizárólag a nemzetbiztonsági okokból), hogy ez nem lenne helyénvaló (a 2013. évi igazságügyi és biztonsági törvény 1. melléklete 4. pontjának (2) bekezdése).
([251]) Az Egyesült Királyság magyarázata – H. szakasz: Nemzetbiztonság, 43. o.
([252]) A 2018. évi adatvédelmi törvény 94. szakaszának (11) bekezdése.
([253]) A 2018. évi adatvédelmi törvény 99. szakaszának (4) bekezdése.
([254]) A 2018. évi adatvédelmi törvény 169. szakasza, amely lehetővé teszi „azon személy igényét, aki az adatvédelmi jogszabályok követelményeinek megsértése miatt kárt szenved”.
([255]) A 2018. évi adatvédelmi törvény 169. szakaszának (5) bekezdése.
([256]) Lásd a nyomozati hatáskörök szabályozásáról szóló törvény 65. szakasza (2) bekezdésének b) pontját.
([257]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 3. melléklete értelmében a tagoknak meghatározott igazságügyi tapasztalattal kell rendelkezniük, és újból kinevezhetők.
([258]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 3. melléklete 1. pontjának (5) bekezdése.
([259]) Az „indítvány” fogalmáról lásd a 183. lábjegyzetet.
([260]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának (4) bekezdése.

magatartás „vitatható körülmények között” történt ([261]) vagy „azt a hírszerző ügynökség vagy annak képviseletében más hajtotta végre ([262]). Mivel ezt a „meggyőződés” mércét elég tágan értelmezték ([263]), az ügynek a Törvényszék elé terjeszthetőségére viszonylag alacsony követelmények vonatkoznak.

(152) Amennyiben a Törvényszék mérlegeli a hozzá benyújtott panaszt, a Törvényszék feladata annak vizsgálata, hogy a panaszban vádolt személyek részt vettek-e a panaszossal kapcsolatos tevékenységben, valamint vizsgálni kell azt a hatóságot, amely állítólag részt vett a jogsértésekben, és hogy az állítólagos magatartás megtörtént-e ([264]). Ha a Törvényszék egy ügyet tárgyal, az eljárásban ugyanazon elveket kell alkalmaznia a határozat hozatalához, amelyeket a bíróság a bírósági felülvizsgálat iránti kérelemre alkalmazna ([265]).

(153) A Törvényszéknek értesítenie kell a panaszost arról, hogy hozott-e határozatot a javára vagy sem ([266]). A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67. szakaszának (6) és (7) bekezdése szerint a Törvényszéknek jogában áll ideiglenes intézkedést hozni, és az általa megfelelőnek tartott kártérítést megítélni vagy egyéb végzést meghozni ([267]). A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67A. szakasza szerint a Törvényszék határozata ellen fellebbezni lehet, a Törvényszék vagy az illetékes fellebbviteli bíróság engedélyével.

(154) Az egyének különösen nyújthatnak be keresetet – és kaphatnak jogorvoslatot – az IPT-hez, ha úgy ítélik meg, hogy egy hatóság az EJEE szerinti jogokkal – ideértve a magánélethez és az adatvédelemhez való jogot – összeegyeztethetetlen módon járt el (vagy ilyen eljárást javasol), következésképpen az 1998. évi emberi jogi törvény 6. szakaszának (1) bekezdése alapján jogellenes. Az IPT-nek kizárólagos illetékessége van a hírszerző ügynökségekkel kapcsolatban az emberi jogokról szóló törvény szerinti összes követelés tekintetében. Ez azt jelenti, ahogyan azt a Legfelsőbb Bíróság megjegyezte: „az, hogy egy adott ügy tényállása az emberi jogi törvénybe ütközik-e, azt elvileg egy olyan független bíróság vetheti fel és döntheti el, amely hozzáférhet az összes vonatkozó anyaghoz, a titkos anyagokat is beleértve. […] Ebben az összefüggésben azt is szem előtt tartjuk, hogy az IPT döntései ellen ma már lehetőség van fellebbezni a megfelelő fellebbviteli bíróságnál (Angliában és Walesben ez a Court of Appeal); és hogy a Legfelsőbb Bíróság nemrégiben úgy döntött, hogy az IPT döntései ellen elvileg bírósági felülvizsgálatnak van helye: lásd: az R (Privacy International) kontra Investigatory Powers Tribunal ügyet (2019, UKSC 22; 2019, 2 WLR 1219)” ([268]). Ha az IPT megállapítja valamely hatóság valamely cselekményének jogellenességét, hatáskörein belül az általa igazságosnak és megfelelőnek ítélt kártérítést vagy jogorvoslatot megítélheti ([269]).

([261]) Ezek a körülmények a hatóságok felhatalmazással történt magatartására utalnak (pl. egy parancs, a kommunikáció megszerzésére vonatkozó felhatalmazás/felhívás stb.), vagy ha a körülmények olyanok, hogy (függetlenül attól, hogy van-e ilyen hatóság) a magatartás nem lett volna helyénvaló felhatalmazás, vagy legalábbis annak megfelelő mérlegelése nélkül, hogy ilyen felhatalmazást kell-e kérni. Az igazságügyi biztos által engedélyezett magatartás vitatható körülmények között megvalósult minősül (a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakasz (7ZA) szakasz), míg a bírói tisztséget betöltő személy engedélyével folytatott egyéb magatartás nem vitatható körülmény (a nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 65. szakaszának (7) és (8) bekezdése).

([262]) Az Egyesült Királyság hatóságai által szolgáltatott információk szerint a panasz benyújtásához szükséges alacsony küszöb következtében nem szokatlan, hogy a Törvényszék vizsgálata azt állapítja meg, hogy a panaszost valójában soha nem vizsgálta a hatóság. Az IPT legfrissebb statisztikai jelentésében szerepel, hogy 2016-ban a Törvényszékhez 209 panasz érkezett, ezek 52 %-át komolytalannak vagy zaklatónak, 25 %-át pedig „határozatlan”-nak ítélték. Az Egyesült Királyság hatóságai kifejtették, hogy ez vagy azt jelenti, hogy nem használtak leplezett tevékenységet/hatásköröket a panaszossal kapcsolatban, vagy hogy alkalmaztak leplezett technikákat, és a Törvényszék megállapította a tevékenység jogszerűségét. Ezenkívül 11 % esetében nem volt hatáskör, azokat visszavonták vagy érvénytelenek voltak, 5 %-ukat elutasították elévülés miatt, 7 %-ukban a panaszos javára döntöttek. Az Investigatory Powers Tribunal 2016. évi statisztikai jelentése, amely az alábbi linken érhető el: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) Lásd a Human Rights Watch kontra Secretary of State ügyet (2016 UKIPTrib15_165-CH). Ebben az ügyben az IPT az EJEB ítélkezési gyakorlatára hivatkozva úgy ítélte meg, hogy a megfelelő teszt az arról való meggyőződéséhez, hogy a nyomozati hatáskörök (Skócia) szabályozásáról szóló 2000. évi törvény 68. szakasza (5) bekezdésének hatálya alá tartozó magatartást bármelyik hírszerző ügynökség vagy képviseletében más elkövette-e, az, hogy van-e alapja az említett meggyőződésnek, beleértve azt a tényt is, hogy az egyén akkor vallhatja magát leplezett intézkedések vagy a leplezett intézkedéseket megengedő jogszabályok puszta léte által okozott jogsértés áldozatának, ha képes azt bizonyítani, hogy személyes helyzete miatt potenciálisan fennáll annak a veszélye, hogy ilyen intézkedéseknek vetik alá (lásd a Human Rights Watch kontra Secretary of State ügy 41. pontját).

([264]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67. szakaszának (3) bekezdése.

([265]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 67. szakaszának (2) bekezdése.

([266]) A nyomozati hatáskörök szabályozásáról szóló 2000. évi törvény 68. szakaszának (4) bekezdése.

([267]) Ennek része lehet egy azt előíró végzés, hogy semmisítsék meg a hatóság által bármely személlyel kapcsolatban tárolt információkat.

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

([269]) Az 1998. évi emberi jogi törvény 8. szakaszának (1) bekezdése.

(155) A nemzeti jogorvoslati lehetőségek kimerítése után az egyén jogorvoslatot kaphat az Emberi Jogok Európai Bírósága előtt az EJEE értelmében garantált jogok – ideértve a magánélethez és az adatvédelemhez való jogot – megsértése miatt.

(156) A fentiekből következik, hogy az Egyesült Királyság bűnüldöző hatóságai által az e határozat alapján továbbított adatok más hatóságokkal, köztük hírszerző ügynökségekkel történő megosztására korlátozások és feltételek vonatkoznak, amelyek biztosítják, hogy az említett további megosztás szükséges és arányos legyen, és érvényesüljenek a 2018. évi adatvédelmi törvény szerinti adatvédelmi biztosítékok. Ezenkívül az érintett hatóságok által végzett adatkezelést független szervek felügyelik, és az érintett egyének hozzáférhetnek hatékony bírósági jogorvoslathoz.

3. KÖVETKEZTETÉS

(157) A Bizottság úgy véli, hogy a 2018. évi adatvédelmi törvény 3. része biztosítja az Unió illetékes hatóságaitól az Egyesült Királyság illetékes hatóságaihoz bűnüldözési célból továbbított személyes adatok olyan szintű védelmét, amely lényegében megegyezik az (EU) 2016/680 irányelv által garantált védelem szintjével.

(158) A Bizottság ezenfelül úgy ítéli meg, hogy az Egyesült Királyság jogában létező felügyeleti mechanizmusok és jogorvoslati megoldások összességében véve lehetővé teszik, hogy a gyakorlatban azonosítsák és szankcionálják, ha a személyes adatokat kezelő bűnüldözési hatóságok jogsértést követnek el, továbbá jogorvoslatot biztosítanak az érintetteknek, hogy betekinthessenek a rájuk vonatkozó személyes adatokba, és adott esetben helyesbíttethessék vagy töröltethessék ezeket az adatokat.

(159) Végül az Egyesült Királyság jogrendjéről rendelkezésre álló információk alapján a Bizottság úgy véli, hogy azon személyek alapvető jogaiba való beavatkozás, akiknek személyes adatait az Egyesült Királyság hatóságai közérdekből továbbítják az Európai Unióból az Egyesült Királyságba a személyes adatok bűnüldöző hatóságok és más hatóságok, például a nemzetbiztonsági szervek közötti megosztása keretében, arra korlátozódik, ami a szóban forgó jogszerű cél eléréséhez feltétlenül szükséges, és hogy hatékony jogvédelem áll rendelkezésre ilyen beavatkozás esetén.

(160) Ezért olyan határozatot kell hozni, hogy az Egyesült Királyság megfelelő szintű védelmet biztosít az (EU) 2016/680 irányelv Alapjogi Chartára figyelemmel értelmezett 36. cikkének (2) bekezdése értelmében.

(161) Ez a következtetés az Egyesült Királyság vonatkozó belföldi rendszerén és nemzetközi kötelezettségvállalásain alapul, különös tekintettel az Emberi Jogok Európai Egyezményének betartására és az Emberi Jogok Európai Bírósága joghatóságának való alávetésre. Az említett nemzetközi kötelezettségek folyamatos betartása ezért különösen fontos eleme az e határozat alapját képező értékelésnek.

4. E HATÁROZAT ÉS AZ ADATVÉDELMI HATÓSÁGOK INTÉZKEDÉSÉNEK JOGHATÁSAI

(162) A tagállamok és szerveik kötelesek megtenni az ahhoz szükséges intézkedéseket, hogy betartsák az uniós intézmények jogi aktusait, mivel az utóbbiak vélelmezhetően jogszerűek, és ennélfogva mindaddig joghatásokat váltanak ki, amíg azokat vissza nem vonják, megsemmisítés iránti kereset alapján meg nem semmisítik, illetve előzetes döntéshozatal iránti kérelem vagy jogellenességi kifogás következtében nem nyilvánítják érvénytelennek.

(163) Következésképpen a Bizottságnak az (EU) 2016/680 irányelv 36. cikkének (3) bekezdése alapján elfogadott megfelelőségi határozata kötelező a címzett tagállamok valamennyi szervére, így a független felügyeleti hatóságaikra is. E határozat alkalmazásának időtartama alatt különösen az uniós adatkezelőtől vagy adatfeldolgozótól az egyesült királyságbeli adatkezelőkhöz vagy adatfeldolgozókhoz történő továbbításra további engedély megszerzése nélkül kerülhet sor.

(164) Ugyanakkor emlékeztetni kell arra, hogy az (EU) 2016/680 irányelv 47. cikkének (5) bekezdése alapján, és amint azt a Bíróság a Schrems-ítéletben kifejtette, amennyiben egy nemzeti adatvédelmi hatóság megkérdőjelezi – ideértve a panaszra történő eljárást is – a Bizottság megfelelőségi határozatának az egyén magánélethez és adatvédelemhez fűződő alapvető jogaival való összeegyeztethetőségét, a nemzeti jognak biztosítania kell a jogorvoslati lehetőségeket, amelyek lehetővé teszik számára, hogy a nemzeti bíróságok előtt a kifogásokra hivatkozzon annak érdekében, hogy azok esetlegesen előzetes döntéshozatali eljárást kezdeményezhessenek e határozat érvényességének vizsgálata céljából ([270]).

([270]) Schrems-ügy, 65. pont.

5. E HATÁROZAT NYOMON KÖVETÉSE, FELFÜGGESZTÉSE, VISSZAVONÁSA VAGY MÓDOSÍTÁSA

(165) Az (EU) 2016/680 irányelv 36. cikkének (4) bekezdése értelmében a Bizottságnak folyamatosan figyelemmel kell kísérnie az Egyesült Királyságban az e határozat elfogadását követő fejleményeket annak értékelése érdekében, hogy az továbbra is biztosítja-e a lényegében azonos szintű védelmet. Az említett nyomon követés ebben az esetben különösen fontos, mivel az Egyesült Királyság egy olyan új, idővel esetlegesen változó adatvédelmi rendszert fog igazgatni, alkalmazni és végrehajtani, amelyre az uniós jog már nem vonatkozik. Ebben a tekintetben különös figyelmet fognak fordítani a személyes adatok harmadik országokba történő továbbítására vonatkozó egyesült királyságbeli szabályok gyakorlati alkalmazására, többek között nemzetközi megállapodások megkötése révén, valamint annak az e határozat alapján továbbított adatok esetében nyújtott védelem szintjére gyakorolt hatására; valamint az egyéni jogok gyakorlásának eredményességére az e határozat hatálya alá tartozó területeken. Többek között az ítélkezési gyakorlat alakulása és az információügyi biztos és más független testületek általi felügyelet fog adatokat szolgáltatni a Bizottság általi nyomon követéshez.

(166) A nyomon követés elősegítése céljából az Egyesült Királyság hatóságainak haladéktalanul és rendszeren tájékoztatniuk kell a Bizottságot az Egyesült Királyság jogrendjének minden olyan lényeges változásáról, amely hatást gyakorol az e határozat tárgyát képező jogi keretre, valamint személyes adatok az e határozatban értékelt kezelésével kapcsolatos gyakorlatok minden változásáról, különösen a (165) preambulumbekezdésben említett elemek vonatkozásában.

(167) Továbbá annak lehetővé tétele érdekében, hogy a Bizottság hatékonyan lássa el nyomonkövetési feladatát, a tagállamoknak tájékoztatniuk kell a Bizottságot a nemzeti adatvédelmi hatóságok minden vonatkozó lépéséről, különösen az uniós érintetteknek a személyes adatok Európai Unióból az egyesült királyságbeli bűnüldözési hatóságok felé történő továbbításával kapcsolatos kérései vagy panaszai tekintetében. A Bizottságot továbbá tájékoztatni kell minden arra utaló információról, hogy a bűncselekmények megelőzéséért, nyomozásáért, felderítéséért vagy a vádemelésért, illetve a nemzetbiztonságért felelős egyesült királyságbeli közigazgatási szervek intézkedései nem biztosítják a megfelelő szintű védelmet.

(168) Amennyiben a rendelkezésre álló információk, különösen az e határozat nyomon követéséből származó, vagy az Egyesült Királyság vagy a tagállamok hatóságai által szolgáltatott információk arra utalnak, hogy az Egyesült Királyság által biztosított védelem szintje már nem feltétlenül megfelelő, a Bizottságnak erről haladéktalanul tájékoztatnia kell az Egyesült Királyság illetékes hatóságait, és kérheti a megfelelő intézkedések meghatározott, észszerű határidőn belüli meghozatalát. Szükség esetén ez a határidő egy meghatározott időtartammal meghosszabbítható, figyelembe véve a szóban forgó kérdés jellegét és/vagy a meghozandó intézkedéseket.

(169) Ha az említett határidő lejártakor az Egyesült Királyság illetékes hatóságai nem hozzák meg ezeket az intézkedéseket, vagy más módon nem bizonyítják kielégítően, hogy e határozat továbbra is a megfelelő szintű védelmen alapul, a Bizottság megindítja az (EU) 2016/680 irányelv 58. cikkének (2) bekezdésében említett eljárást e határozat részleges vagy teljes felfüggesztése vagy hatályon kívül helyezése céljából.

(170) Ennek alternatívájaként a Bizottságnak ezt az eljárást e határozat módosítása céljából indítja meg, különösen az adattovábbításra további feltételek előírásával vagy a megfelelőség megállapítása hatályának azokra az adattovábbításokra korlátozásával, amelyek esetében biztosított a megfelelő szintű védelem folyamatossága.

(171) Megfelelően indokolt, rendkívül sürgős esetben a Bizottság élni fog azzal a lehetőséggel, hogy az (EU) 2016/680 irányelv 58. cikkének (3) bekezdésében említett eljárásnak megfelelően azonnal alkalmazandó, a határozatot felfüggesztő, hatályon kívül helyező vagy módosító végrehajtási jogi aktusokat fogadjon el.

6. A HATÁROZAT TARTAMA ÉS MEGÚJÍTÁSA

(172) Figyelembe kell venni, hogy a kilépési megállapodásban előírt átmeneti időszak lejártával és amint az EU – Egyesült Királyság kereskedelmi és együttműködési megállapodás 782. cikke szerinti ideiglenes rendelkezés hatályát veszti, egy új adatvédelmi rendszert fog igazgatni, alkalmazni és végrehajtani azzal összehasonlítva, amely akkor volt érvényben, amikor az Európai Unió joga kötötte. Ez nevezetesen az e határozatban értékelt adatvédelmi keret módosításával vagy változásával, valamint egyéb releváns fejleményekkel járhat.

(173) Ezért helyénvaló előírni, hogy ezt a határozatot a hatálybalépésétől számított négy évig kell alkalmazni.

(174) Amennyiben különösen az e határozat nyomon követéséből származó információk azt jelzik, hogy az Egyesült Királyságban biztosított védelmi szint megfelelőségére vonatkozó megállapítások még mindig ténybelileg és jogilag indokoltak, a Bizottság e határozat alkalmazásának megszűnése előtt legkésőbb hat hónappal megindítja az e határozat annak időbeli hatálya elvileg további négy évvel történő meghosszabbításával történő módosítására irányuló eljárást. Az e határozatot módosító, említett végrehajtási jogi aktusokat az (EU) 2016/680 irányelv 58. cikkének (2) bekezdésében említett eljárással összhangban kell elfogadni.

7. **ZÁRÓ MEGÁLLAPÍTÁSOK**

(175) Az Európai Adatvédelmi Testület közzétette véleményét ([271]), amely e határozat kidolgozásakor figyelembevételre került.

(176) Az e határozatban előírt intézkedések összhangban vannak az (EU) 2016/680 irányelv 58. cikkével létrehozott bizottság véleményével.

(177) Az EUSZ-hez és az EUMSZ-hez csatolt, az Egyesült Királyságnak és Írországnak a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség tekintetében fennálló helyzetéről szóló 21. jegyzőkönyv 6a. cikkével összhangban Írországot nem kötelezik az (EU) 2016/680 irányelvben, ennélfogva az e végrehajtási határozatban meghatározott azon szabályok, amelyek a személyes adatoknak a tagállamok által, az EUMSZ harmadik része V. címe 4., illetve 5. fejezetének alkalmazási körébe tartozó tevékenységek során végzett kezelésére vonatkoznak, amennyiben Írországot nem kötelezik a büntetőügyekben folytatott igazságügyi együttműködés vagy a rendőrségi együttműködés formáira vonatkozó olyan szabályok, amelyek megkívánják az EUMSZ 16. cikk alapján megállapított rendelkezések betartását. Emellett az Írország tekintetében az (EU) 2020/1745 tanácsi végrehajtási határozat ([272]) erejénél fogva az (EU) 2016/680 irányelvet 2021. január 1-jétől ideiglenesen hatályba kell léptetni és alkalmazni kell Írországban. Ezért ez a végrehajtási határozat kötelezi Írországot azon schengeni vívmányok tekintetében, amelyekben részt vesz, ugyanazokkal a feltételekkel, mint amelyek az (EU) 2020/1745 végrehajtási határozat meghatározottak szerint az (EU) 2016/680 irányelv Írországban történő alkalmazására vonatkoznak.

(178) Az Európai Unióról szóló szerződéshez és az Európai Unió működéséről szóló szerződéshez csatolt, Dánia helyzetéről szóló 22. jegyzőkönyv 2. és 2a. cikkével összhangban Dániát nem kötik az (EU) 2016/680 irányelvben meghatározott szabályok, és következésképpen ez a végrehajtási határozat, és a személyes adatok tagállamok általi, az EUMSZ harmadik része V. címe 4. fejezetének vagy 5. fejezetének hatálya alá tartozó tevékenységek végrehajtása során történő kezeléséhez kapcsolódóan alkalmazásuk rá nem vonatkozik. Tekintettel azonban arra, hogy az (EU) 2016/680 irányelv a schengeni vívmányokra épül, Dánia az említett jegyzőkönyv 4. cikkével összhangban 2016. október 26-án értesítést küldött az (EU) 2016/680 irányelv végrehajtására vonatkozó döntéséről. Dánia ezért a nemzetközi jog alapján köteles e végrehajtási határozat végrehajtására.

(179) Izland és Norvégia tekintetében ez a végrehajtási határozat az Európai Unió Tanácsa, valamint az Izlandi Köztársaság és a Norvég Királyság között kötött, e két államnak a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodás ([273]) értelmében a schengeni vívmányok rendelkezéseinek továbbfejlesztését képezi.

(180) Svájc tekintetében ez a végrehajtási határozat az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról kötött megállapodás ([274]) értelmében a schengeni vívmányok rendelkezéseinek továbbfejlesztését képezi.

(181) Liechtenstein tekintetében ez a végrehajtási határozat az Európai Unió, az Európai Közösség, a Svájci Államszövetség és a Liechtensteini Hercegség közötti, a Liechtensteini Hercegségnek az Európai Unió, az Európai Közösség és a Svájci Államszövetség közötti, a Svájci Államszövetségnek a schengeni vívmányok végrehajtására, alkalmazására és fejlesztésére irányuló társulásáról szóló megállapodáshoz való csatlakozásáról szóló jegyzőkönyv ([275]) értelmében a schengeni vívmányok rendelkezéseinek továbbfejlesztését képezi,

---

([271]) 15/2021 vélemény az Európai Bizottságnak a személyes adatok Egyesült Királyságban történő megfelelő védelméről szóló, az (EU) 2016/680 irányelv szerinti végrehajtási határozattervezetéről, elérhető a következő linken: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en.

([272]) A Tanács (EU) 2020/1745 rendelete (2020. november 18.) a schengeni vívmányok adatvédelmi rendelkezéseinek hatályba léptetéséről, valamint a schengeni vívmányok bizonyos rendelkezéseinek ideiglenes hatályba léptetéséről (HL L 393., 2020.11.23., 3. o.).

([273]) HL L 176., 1999.7.10., 36. o.

([274]) HL L 53., 2008.2.27., 52. o.

([275]) HL L 160., 2011.6.18., 21. o.

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

Az (EU) 2016/680 irányelv 36. cikkének alkalmazásában az Egyesült Királyság megfelelő szintű védelmet biztosít az Európai Unióból az Egyesült Királyság bűncselekmények megelőzéséért, kivizsgálásáért, felderítéséért vagy üldözéséért, vagy a büntetőjogi szankciók végrehajtásáért felelős hatóságainak továbbított személyes adatok tekintetében.

2. cikk

Az érintett tagállam haladéktalanul tájékoztatja a Bizottságot, amikor a személyes adataik kezelése tekintetében az egyének védelme érdekében a tagállam illetékes felügyeleti hatóságai gyakorolják az (EU) 2016/680 irányelv 47. cikke értelmében vett hatáskörüket az Egyesült Királyság hatóságainak az 1. cikkben meghatározott alkalmazási körön belüli adattovábbítások tekintetében.

3. cikk

(1) A Bizottság folyamatosan figyelemmel kíséri az e határozat alapját képező jogi keret alkalmazását – ideértve az újbóli adattovábbítások lebonyolításának és az egyéni jogok gyakorlásának feltételeit – annak értékelése céljából, hogy Egyesült Királyság az 1. cikk értelmében továbbra is megfelelő szintű védelmet biztosít-e.

(2) A tagállamok és a Bizottság tájékoztatják egymást az olyan esetekről, amikor az információügyi biztos vagy bármely egyéb illetékes egyesült királyságbeli hatóság nem biztosítja az e határozat alapjául szolgáló jogi keretnek való megfelelést.

(3) A tagállamok és a Bizottság tájékoztatják egymást bármely arra utaló körülményről, hogy az egyesült királyságbeli hatóságoknak az egyének személyes adataik védelméhez fűződő jogába történő beavatkozása túllépi a feltétlenül szükséges mértéket vagy nem létezik hatékony jogvédelem az említett beavatkozásokkal szemben.

(4) Ha a Bizottság arra utaló jeleket észlel, hogy a megfelelő szintű védelem már nem biztosított, a Bizottság tájékoztatja az Egyesült Királyság illetékes hatóságait, és felfüggesztheti, hatályon kívül helyezheti vagy módosíthatja ezt a határozatot.

(5) A Bizottság felfüggesztheti, hatályon kívül helyezheti vagy módosíthatja ezt a határozatot, ha az Egyesült Királyság kormánya együttműködésének hiánya miatt nem tudja megállapítani, hogy az 1. cikkben szereplő megállapítás fennáll-e.

4. cikk

Ez a határozat 2025. június 27-én hatályát veszti, kivéve, ha az (EU) 2016/680 irányelv 58. cikkének (2) bekezdésében említett eljárással összhangban meghosszabbítják.

5. cikk

Ennek a határozatnak a tagállamok a címzettjei.

Kelt Brüsszelben, 2021. június 28-án.

a Bizottság részéről
Didier REYNDERS
a Bizottság tagja