DECIZIA DE PUNERE ÎN APLICARE (UE) 2021/1773 A COMISIEI

din 28 iunie 2021

în temeiul Directivei (UE) 2016/680 a Parlamentului European și a Consiliului privind protecția adecvată a datelor cu caracter personal de către Regatul Unit al Marii Britanii și Irlandei de Nord

[notificată cu numărul C(2021) 4801]

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului ([1]), în special articolul 36 alineatul (3),

întrucât:

1. INTRODUCERE

(1) Directiva (UE) 2016/680 stabilește normele privind transferul datelor cu caracter personal de la autoritățile competente din Uniune către țări terțe și organizații internaționale, în măsura în care astfel de transferuri intră în domeniul său de aplicare. Normele privind transferurile internaționale de date de către autoritățile competente sunt prevăzute în capitolul V din Directiva (UE) 2016/680, în special la articolele 35-40. Deși fluxul de date cu caracter personal către și dinspre țări situate în afara Uniunii Europene este esențial pentru o cooperare eficientă în materie de asigurare a respectării legii, se impune garantarea faptului că nivelul de protecție acordat datelor cu caracter personal din Uniunea Europeană nu este diminuat de astfel de transferuri ([2]).

(2) În temeiul articolului 36 alineatul (3) din Regulamentul (UE) 2016/680, Comisia poate decide, prin intermediul unui act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare determinate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat. În astfel de condiții, transferurile de date cu caracter personal către o țară terță pot avea loc fără a fi necesară obținerea unei autorizații suplimentare (cu excepția cazului în care un alt stat membru de la care au fost obținute datele trebuie să autorizeze efectuarea transferului), astfel cum se prevede la articolul 35 alineatul (1) și în considerentul 66 din Directiva (UE) 2016/680.

(3) În conformitate cu articolul 36 alineatul (2) din Directiva (UE) 2016/680, adoptarea unei decizii privind caracterul adecvat al nivelului de protecție trebuie să se bazeze pe o analiză cuprinzătoare a ordinii juridice a țării terțe. În evaluare, Comisia trebuie să stabilească dacă țara terță în cauză garantează un nivel de protecție „echivalent în esență" celui asigurat în cadrul Uniunii Europene [considerentul 67 din Directiva (UE) 2016/680]. Standardul în raport cu care este evaluată „echivalența esențială" este cel stabilit de legislația UE, în special de Directiva (UE) 2016/680, precum și de jurisprudența Curții de Justiție a Uniunii Europene ([3]). Criteriile de referință privind caracterul adecvat al nivelului de protecție ale Comitetului european pentru protecția datelor sunt, de asemenea, importante în această privință ([4]).

(4) Conform clarificărilor aduse de Curtea de Justiție a Uniunii Europene, aceasta nu necesită găsirea unui nivel identic de protecție ([5]). În special, mijloacele la care țara terță în cauză recurge pentru protecția datelor cu caracter personal pot fi diferite de cele utilizate în cadrul Uniunii Europene, cu condiția ca acestea să se dovedească, în practică, eficace pentru asigurarea unui nivel adecvat de protecție ([6]). Prin urmare, standardul caracterului adecvat nu necesită o reproducere punct cu punct a normelor Uniunii. Mai curând, testul constă în a stabili dacă, prin esența drepturilor la viață privată și punerea în aplicare efectivă, supravegherea și exercitarea acestora, sistemul străin în cauză, în ansamblul său, oferă nivelul de protecție necesar ([7]).

([1]) JO L 119, 4.5.2016, p. 89.
([2]) A se vedea considerentul 64 din Directiva (UE) 2016/680.
([3]) A se vedea, cel mai recent, cauza C-311/18, Maximillian Schrems/Data Protection Commissioner („Schrems II") ECLI:EU:C:2020:559.
([4]) A se vedea Recomandările 01/2021 cu privire la criteriile de referință privind caracterul adecvat al nivelului de protecție în temeiul Directivei privind protecția datelor în materie de asigurare a respectării legii, adoptate în februarie 2021, disponibile la următoarea adresă: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_ro
([5]) Cauza C-362/14, Maximillian Schrems/Data Protection Commissioner („Schrems"), ECLI:EU:C:2015:650, punctul 73.
([6]) Schrems, punctul 74.
([7]) A se vedea Comunicarea Comisiei către Parlamentul European și Consiliu, „Schimbul de date cu caracter personal și protecția acestora într-o lume globalizată", COM(2017)7 din 10.1.2017, secțiunea 3.1, p. 6-7, disponibilă la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

(5) Comisia a analizat cu atenție legislația și practicile relevante din Regatul Unit al Marii Britanii și Irlandei de Nord (UK). Pe baza constatărilor prezentate în continuare, Comisia concluzionează că Regatul Unit asigură un nivel adecvat de protecție pentru datele cu caracter personal transferate de la autoritățile competente din Uniune, care intră în domeniul de aplicare al Directivei (UE) 2016/680, către autoritățile competente din Regatul Unit, care intră în domeniul de aplicare al Legii privind protecția datelor din 2018, partea 3 (DPA din 2018) ([8]).

(6) Prezenta decizie are ca efect faptul că astfel de transferuri pot avea loc fără a fi necesară obținerea unei autorizații suplimentare pentru o perioadă de patru ani, sub rezerva unei eventuale reînnoiri și fără a aduce atingere condițiilor prevăzute la articolul 35 din Directiva (UE) 2016/680.

2. NORME APLICABILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL DE CĂTRE AUTORITĂȚILE COMPETENTE ÎN SCOPUL ASIGURĂRII RESPECTĂRII DREPTULUI PENAL

2.1. Cadrul constituțional

(7) Regatul Unit este o democrație parlamentară. Acesta are un parlament suveran, care exercită o autoritate supremă asupra tuturor celorlalte instituții guvernamentale, un executiv ai cărui membri provin din parlament și care este responsabil în fața acestuia, precum și un sistem judiciar independent. Executivul își bazează autoritatea pe capacitatea sa de a atrage încrederea Camerei Comunelor alese și răspunde în fața ambelor camere ale Parlamentului (Camera Comunelor și Camera Lorzilor), care sunt responsabile de controlul Guvernului și de dezbaterea și adoptarea legilor. Parlamentul Regatului Unit a delegat Parlamentului scoțian, Parlamentului Țării Galilor (Senedd Cymru) și Adunării Irlandei de Nord responsabilitatea pentru legiferarea anumitor chestiuni interne din Scoția, Țara Galilor și Irlanda de Nord. În timp ce protecția datelor reprezintă o chestiune rezervată Parlamentului Regatului Unit, și anume aceeași legislație se aplică în întreaga țară, alte domenii de politică relevante pentru prezenta decizie sunt descentralizate. De exemplu, sistemele de justiție penală, inclusiv poliția (activitățile desfășurate de forțele de poliție) din Scoția și Irlanda de Nord sunt transferate Parlamentului scoțian și, respectiv, Adunării Irlandei de Nord ([9]).

(8) Deși Regatul Unit nu are o constituție codificată în sensul unui document constitutiv cu vechime, principiile sale constituționale au apărut de-a lungul timpului, provenind în special din jurisprudență și din convenție. Valoarea constituțională a anumitor statute, cum ar fi Magna Carta, Declarația drepturilor din 1689 (Bill of Rights 1689) și Legea privind drepturile omului din 1998 (Human Rights Act 1998), a fost recunoscută. Drepturile fundamentale ale persoanelor au fost dezvoltate, ca parte a constituției, prin intermediul common law, al statutelor și al tratatelor internaționale, în special al Convenției europene a drepturilor omului (CEDO), pe care Regatul Unit a ratificat-o în 1951. În 1987, Regatul Unit a ratificat, de asemenea, Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) ([10]).

(9) Legea privind drepturile omului din 1998 încorporează în legislația Regatului Unit drepturile cuprinse în CEDO. Legea respectivă acordă oricărei persoane drepturile și libertățile fundamentale prevăzute la articolele 2-12 și articolul 14 din Convenția europeană a drepturilor omului, la articolele 1-3 din Protocolul nr. 1 și la articolul 1 din Protocolul nr. 13, coroborate cu articolele 16-18 din CEDO. Aceasta include dreptul la respectarea vieții private și de familie, care, la rândul său, include și dreptul la protecția datelor, precum și dreptul la un proces echitabil ([11]). În special, în temeiul articolului 8 din Convenția europeană a drepturilor omului, nu este admis amestecul unei autorități publice în exercitarea dreptului la viață privată decât în măsura în care acest amestec este prevăzut de lege, dacă constituie o măsură care, într-o societate democratică, este necesară pentru siguranța națională, siguranța publică, bunăstarea economică a țării, apărarea ordinii și prevenirii faptelor penale, protejarea sănătății sau a moralei, ori protejarea drepturilor și libertăților altora.

([8]) Legea privind protecția datelor din 2018, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) UK Explanatory Framework for Adequacy Discussions (Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat), secțiunea F: Asigurarea respectării legii, disponibilă la următoarea adresă:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) Principiile Convenției 108 au fost transpuse inițial în legislația Regatului Unit prin Legea privind protecția datelor (DPA – Data Protection Act) din 1984, care a fost înlocuită de DPA din 1998 și apoi, la rândul său, de DPA din 2018 (coroborat cu RGPD al Regatului Unit). Regatul Unit a semnat, de asemenea, Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (cunoscută sub denumirea de „Convenția 108+") în 2018 și lucrează în prezent la ratificarea convenției.

([11]) Articolele 6 și 8 din CEDO (a se vedea, de asemenea, anexa 1 la Legea privind drepturile omului din 1998).

(10) În conformitate cu Legea privind drepturile omului din 1998, orice acțiune a autorităților publice trebuie să fie compatibilă cu un drept garantat de CEDO ([12]). În plus, legislația primară și cea secundară trebuie interpretate și puse în aplicare într-un mod compatibil cu respectivele drepturi ([13]). În măsura în care o persoană fizică consideră că drepturile sale, inclusiv dreptul la viață privată și la protecția datelor, au fost încălcate de autoritățile publice, aceasta poate obține reparații în fața instanțelor din Regatul Unit în temeiul Legii privind drepturile omului din 1998 și, în cele din urmă, după epuizarea căilor de atac naționale, poate obține reparații în fața Curții Europene a Drepturilor Omului pentru încălcarea drepturilor garantate de CEDO.

2.2. **Cadrul de protecție a datelor din Regatul Unit**

(11) Regatul Unit s-a retras din Uniunea Europeană la 31 ianuarie 2020. Pe baza Acordului privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice ([14]), dreptul Uniunii a continuat să se aplice pe teritoriul Regatului Unit pe parcursul perioadei de tranziție până la 31 decembrie 2020. Înainte de retragere și în cursul perioadei de tranziție, cadrul legislativ privind protecția datelor cu caracter personal în Regatul Unit care reglementează prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora, consta în părți relevante din Legea privind protecția datelor din 2018, care a transpus Directiva (UE) 2016/680.

(12) Pentru a pregăti ieșirea din UE, Guvernul Regatului Unit a adoptat European Union (Withdrawal) Act 2018 (EUWA) [Legea din 2018 privind Uniunea Europeană (retragere)] ([15]), care încorporează legislația direct aplicabilă a Uniunii în legislația Regatului Unit și a prevăzut că așa-numita „legislație națională derivată din dreptul Uniunii" continuă să producă efecte după încheierea perioadei de tranziție. Partea 3 din DPA din 2018 ([16]) care transpune Directiva (UE) 2016/680 constituie „legislație națională derivată din dreptul Uniunii" în temeiul EUWA. Potrivit EUWA, „legislația națională derivată din dreptul Uniunii" nemodificată trebuie să fie interpretată de instanțele din Regatul Unit în conformitate cu jurisprudența relevantă a Curții de Justiție a Uniunii Europene (Curtea de Justiție) și cu principiile generale ale dreptului Uniunii, întrucât acestea au produs efecte imediat înainte de încheierea perioadei de tranziție (denumite „jurisprudența menținută a Uniunii" și, respectiv, „principiile generale menținute ale dreptului Uniunii") ([17]).

(13) În temeiul EUWA, miniștrii Regatului Unit au competența de a introduce legislație secundară, prin intermediul instrumentelor statutare, pentru a introduce modificările necesare ale dreptului menținut al Uniunii care rezultă din retragerea Regatului Unit din Uniune. Această competență a fost exercitată prin Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 [Regulamentele din 2019 privind protecția datelor, a vieții private și comunicațiile electronice (modificări etc.) (ieșirea din UE)] (Regulamentele DPPEC) ([18]). Acestea modifică legislația Regatului Unit privind protecția datelor, inclusiv DPA din 2018, pentru a fi adecvată contextului național ([19]).

([12]) Secțiunea 6 din Legea privind drepturile omului din 1998.

([13]) Secțiunea 3 din Legea privind drepturile omului din 1998.

([14]) Acord privind retragerea Regatului Unit al Marii Britanii și Irlandei de Nord din Uniunea Europeană și din Comunitatea Europeană a Energiei Atomice 2019/C 384 I/01, XT/21054/2019/INIT (JO C 384 I, 12.11.2019, p. 1) (denumit în continuare „Acord de retragere"), disponibil la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

([15]) European Union (Withdrawal) Act 2018 [Legea din 2018 privind Uniunea Europeană (retragere)], disponibil la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Legea privind protecția datelor din 2018, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Secțiunea 6 din EUWA 2018.

([18]) Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 [Regulamentele din 2019 privind protecția datelor, a vieții private și comunicațiile electronice (modificări etc.) (ieșirea din UE)], disponibile la următoarea adresă: https://www.legislation.gov.uk/uksi/2019/419/contents/made, astfel cum au fost modificate prin DPPEC din 2020, disponibile la următoarea adresă: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) Regulamentele în materie de ieșire aduc o serie de modificări părții 3 din DPA din 2018. Multe dintre acestea sunt modificări de ordin tehnic, cum ar fi eliminarea trimiterilor la „statul membru" sau la „Directiva privind protecția datelor în materie de asigurare a respectării legii" [a se vedea, de exemplu, secțiunea 48 punctul 8 sau secțiunea 73 punctul 5 litera (a) din DPA din 2018 cu „dreptul intern"], astfel încât partea 3 să funcționeze efectiv ca drept intern după încheierea perioadei de tranziție. În unele cazuri au fost necesare alte tipuri de modificări, de exemplu referitor la „cine" adoptă „decizii privind caracterul adecvat al nivelului de protecție" în sensul cadrului legislativ al Regatului Unit privind protecția datelor (a se vedea secțiunea 74A din DPA din 2018), și anume secretarul de stat în locul Comisiei Europene.

(14) În consecință, standardele juridice privind prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora în Regatul Unit după perioada de tranziție în temeiul Acordului de retragere vor fi stabilite în continuare în părțile relevante ale DPA din 2018, dar astfel cum au fost modificate prin regulamentele DPPEC, în special în partea 3 a actului respectiv. Regulamentul general privind protecția datelor în vigoare în Regatul Unit (RGPD al Regatului Unit) nu se aplică acestui tip de prelucrare.

(15) Partea 3 din DPA din 2018 prevede normele privind prelucrarea datelor cu caracter personal în scopul asigurării respectării dreptului penal, inclusiv principiile privind protecția datelor, temeiurile juridice ale prelucrării (legalitatea), drepturile persoanelor vizate, obligațiile autorităților competente în calitate de operatori de date și restricțiile privind transferurile ulterioare. În același timp, normele aplicabile în materie de supraveghere, asigurare a respectării legii și măsuri de reparare aplicabile în sectorul asigurării respectării legii sunt prevăzute în părțile 5 și 6 din DPA din 2018.

(16) În plus, având în vedere rolul important jucat de forțele de poliție în sectorul asigurării respectării legii, ar trebui avute în vedere normele care reglementează activitățile polițienești. Întrucât activitatea polițienească este o chestiune descentralizată, diferite acte legislative care prezintă totuși adesea similitudini în materie de conținut sunt aplicabile activităților polițienești din (a) Anglia și Țara Galilor, (b) Scoția și (c) Irlanda de Nord ([20]). În plus, diferite tipuri de documente de orientare oferă clarificări suplimentare cu privire la modul în care competențele poliției se impun a fi utilizate. Există trei forme principale de orientări pentru poliție: 1) orientări statutare emise în temeiul legislației, cum ar fi Codul deontologic ([21]) și Codul de bune practici privind gestionarea informațiilor cu caracter polițienesc (Codul de bune practici privind MoPI) ([22]), emise în temeiul Legii privind poliția din 1996 ([23]) sau al codurilor PACE ([24]) emise în temeiul Legii britanice privind funcționarea Poliției și administrarea probelor penale (Police and Criminal Evidence Act) ([25]), 2) practici profesionale autorizate privind gestionarea informațiilor cu caracter polițienesc (Orientările APP privind gestionarea informațiilor cu caracter polițienesc) ([26]), emise de Colegiul de Poliție, și 3) orientări operaționale (publicate chiar de poliție). Consiliul național al responsabililor serviciilor de poliție (National Police Chiefs Council) (un organism de coordonare pentru toate forțele de poliție din Regatul Unit) publică orientări operaționale pe care toate forțele de poliție le-au aprobat și care, prin urmare, se aplică la nivel național ([27]). Scopul acestor orientări este de a asigura coerența între forțe în ceea ce privește modul de gestionare a informațiilor ([28]).

(17) Codul de bune practici privind gestionarea informațiilor cu caracter polițienesc a fost emis de secretarul de stat în 2005, făcând uz de competențele prevăzute la secțiunea 39A din Legea privind poliția din 1996 ([29]). Orice cod de bune practici emis în temeiul Legii privind poliția trebuie să fie aprobat de secretarul de stat și face obiectul consultării Agenției Naționale pentru Combaterea Criminalității înainte de a fi prezentat Parlamentului. Secțiunea 39A punctul 7 din Legea privind poliția prevede că poliția trebuie să țină seama în mod corespunzător de

([20]) Pentru o explicație mai detaliată privind forțele de poliție și competențele acestora în Regatul Unit, a se vedea: UK Explanatory Framework for Adequacy Discussions (Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat), secțiunea F: Asigurarea respectării legii (a se vedea nota de subsol 9).

([21]) Codul de bune practici în materie de principii și standarde de conduită profesională pentru profesioniștii din domeniul polițienesc din Anglia și Țara Galilor (*The Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales*), disponibil la următoarea adresă: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Codul deontologic al Serviciului de Poliție din Irlanda de Nord (*Police Service Northern Ireland Code of Ethic*), disponibil la următoarea adresă: https://www.nipolicingboard.org.uk/psni-code-ethics; Codul deontologic pentru activitățile polițienești din Scoția (*Code of Ethic for policing in Scotland*), disponibil la următoarea adresă: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) Codul de bune practici privind gestionarea informațiilor cu caracter polițienesc (*Code of Practice on the Management of Police Information*), disponibil la următoarea adresă:http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) Legea privind poliția din 1996, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Codurile de bune practici ale Legii britanice din 1984 privind funcționarea Poliției și administrarea probelor penale (*Police and Criminal Evidence Act* – PACE), disponibile la următoarea adresă: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([25]) Legea britanică din 1984 privind funcționarea Poliției și administrarea probelor penale (*Police and Criminal Evidence Act*), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1984/60/contents

([26]) Practici profesionale autorizate privind gestionarea informațiilor cu caracter polițienesc (*Authorised Professional Practice on the Management of Police Information*), disponibile la următoarea adresă: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Manualul privind protecția datelor pentru profesioniștii în materie de protecție a datelor în domeniul poliției (*Data Protection Manual for Police Data Protection Professionals*), disponibil la următoarea adresă: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) De exemplu, Codul de bune practici privind MoPI (a se vedea nota de subsol 22) se aplică în ceea ce privește păstrarea informațiilor serviciilor de poliție operaționale (a se vedea considerentul 47 din prezenta decizie).

([29]) Potrivit informațiilor furnizate de autoritățile Regatului Unit, în timpul discuțiilor privind caracterul adecvat al nivelului de protecție, Colegiul de Poliție era în curs de elaborare a unui Cod de bune practici de gestionare a informațiilor și a evidențelor pentru a înlocui MoPI. Proiectul de cod a fost publicat pentru consultare publică la 25 ianuarie 2021 și este disponibil la următoarea adresă: https://www.college.police.uk/article/information-records-management-consultation

codurile emise în temeiul legii, prin urmare poliția ar trebui să o respecte ([30]). În plus, orientările nestatutare (cum ar fi Orientările APP privind gestionarea informațiilor cu caracter polițienesc) trebuie să fie întotdeauna în concordanță cu Codul de bune practici privind gestionarea informațiilor cu caracter polițienesc, care este mai presus de acestea ([31]). În orice caz, deși ar putea exista anumite situații operaționale în care funcționarii poliției trebuie să se abată de la respectivele orientări, aceștia trebuie totuși să respecte cerințele DPA din 2018, partea 3 ([32]).

(18) Orientări suplimentare privind legislația Regatului Unit în materie de protecție a datelor în vederea prelucrării în sectorul asigurării respectării legii sunt furnizate de comisarul pentru informații („Information Commissioner" sau „ICO") ([33]) (pentru detalii suplimentare privind ICO, a se vedea considerentele 93-109). Deși nu au caracter juridic obligatoriu, instanțele ar fi obligate în contextul unei cauze să ia în considerare orice încălcare a orientărilor, deoarece acestea au o pondere interpretativă și demonstrează modul în care legislația privind protecția datelor este interpretată și pusă în practică de către comisar ([34]).

(19) În cele din urmă, astfel cum se menționează în considerentele 8-10, agențiile de aplicare a legii din Regatul Unit trebuie să asigure respectarea (CEDO) și a Convenției 108.

(20) Prin urmare, în ceea ce privește structura și componentele sale principale, cadrul juridic care reglementează prelucrarea datelor de către autoritățile de aplicare a dreptului penal din Regatul Unit este foarte similar cu cel aplicabil în UE. Aceasta include faptul că acest cadru nu se bazează numai pe obligațiile prevăzute în dreptul intern, care au fost conturate de dreptul Uniunii, ci și pe obligațiile consacrate în dreptul internațional public, în special prin aderarea Regatului Unit la CEDO și la Convenția 108, precum și prin recunoașterea de către acesta a competenței Curții Europene a Drepturilor Omului. Aceste obligații care decurg din instrumentele internaționale obligatorii din punct de vedere juridic, în special în ceea ce privește protecția datelor cu caracter personal, reprezintă, prin urmare, un element deosebit de important al cadrului juridic evaluat în prezenta decizie.

2.3. **Domeniul de aplicare material și teritorial**

(21) Domeniul de aplicare material al DPA din 2018, partea 3, coincide cu domeniul de aplicare al Directivei (UE) 2016/680, astfel cum este prevăzut la articolul 2 alineatul (2) din aceasta. Partea 3 se aplică prelucrării de către o autoritate competentă a datelor cu caracter personal, realizate integral sau parțial prin mijloace automatizate, precum și prelucrării de către o autoritate competentă prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care urmează să facă parte dintr-un sistem de evidență a datelor.

(22) În plus, pentru a se încadra în domeniul de aplicare al părții 3, operatorul trebuie să fie o „autoritate competentă", iar prelucrarea trebuie efectuată într-un „scop de aplicare a legii". Prin urmare, regimul de protecție a datelor care este evaluat în prezenta decizie se aplică tuturor activităților de asigurare a respectării legii desfășurate de aceste autorități competente.

(23) Conceptul de „autoritate competentă" este definit în secțiunea 30 din DPA ca fiind o persoană prevăzută în anexa 7 la DPA din 2018, precum și orice altă persoană, în măsura în care persoana are funcții statutare în oricare dintre scopurile de asigurare a respectării legii. Printre autoritățile competente enumerate în anexa 7 se numără nu numai forțele de poliție, ci și toate departamentele ministeriale ale guvernului Regatului Unit, precum și alte autorități cu atribuții de investigare (de exemplu, Comisarul Administrației Fiscale și Vamale din Regatul Unit – Commissioner

([30]) În cauza R/Comisarul Poliției Metropolitane [2014] EWCA Civ 585, statutul juridic al Codului de bune practici privind MoPI a fost confirmat, iar Lord Justice Laws a declarat că, în conformitate cu secțiunea 39A din Legea privind poliția din 1996, Comisarul Poliției Metropolitane este obligat să respecte Codul de bune practici privind MoPI și Orientările APP privind gestionarea informațiilor cu caracter polițienesc.

([31]) Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) verifică respectarea de către Poliție a Codului de bune practici privind MoPI.

([32]) A se vedea, în acest sens, poziția Colegiului de Poliție cu privire la respectarea orientărilor APP cu privire la toate elementele activității polițienești, care explică faptul că „APP este autorizată de organismul profesional de poliție (Colegiul de Poliție) ca sursă oficială de practică profesională în domeniul polițienesc. Funcționarii și personalul poliției trebuie să aibă în vedere APP în îndeplinirea responsabilităților care le revin. Cu toate acestea, pot exista circumstanțe în care există un motiv legitim din punct de vedere operațional pentru ca o Forță să se abată de la APP, cu condiția să existe o justificare clară în acest sens. Forța ar trebui să își asume responsabilitatea oricărui risc local și național de funcționare în afara orientărilor convenite la nivel național și, în cazul în care are loc un incident sau o anchetă în consecință (de exemplu, prin intermediul Biroului independent de conduită al poliției), Forța este răspunzătoare pentru orice risc.", disponibilă la următoarea adresă https://www.app.college.police.uk/faq-page/

([33]) Ghid privind prelucrarea datelor în scopul asigurării respectării legii, disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) A se vedea cauza Bridges/the Chief Constable of South Wales Police [2019] EWHC 2341 (Admin), în care, deși a luat act de caracterul nestatutar al orientărilor comisarului, Înalta Curte a declarat că „[î]n contextul analizării respectării sau nu de către un operator de date a obligației prevăzute la secțiunea 64 [de realizare a unei evaluări a impactului asupra protecției datelor în ceea ce privește prelucrarea cu risc ridicat], o instanță va ține seama de orientările emise de comisarul pentru informații cu privire la evaluările impactului asupra protecției datelor".

for Her Majesty's Revenue and Customs, Autoritatea Fiscală din Țara Galilor, Autoritatea pentru Concurență și Piețe sau Registrul funciar al Majestății Sale – Her Majesty's Land Register sau Agenția Națională pentru Combaterea Criminalității – National Crime Agency), agenții de urmărire penală, alte agenții de justiție penală și alți deținători sau organizații care desfășoară activități de asigurare a respectării legii ([35]). Partea 3 din DPA din 2018 se aplică în egală măsură instanțelor și tribunalelor atunci când acestea își exercită funcțiile judiciare, cu excepția părții referitoare la drepturile persoanei vizate și la supravegherea ICO ([36]). Lista autorităților competente prevăzută în anexa 7 nu este definitivă și poate fi actualizată de către secretarul de stat prin regulamente, ținând seama de modificările intervenite în materie de organizare a instituțiilor publice ([37]).

(24) Prelucrarea în cauză trebuie să aibă, de asemenea, un „scop de asigurare a respectării legii", definit ca fiind prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora ([38]). Prelucrarea de către o autoritate competentă nu este reglementată de partea 3 din DPA din 2018 în cazul în care aceasta nu are loc în scopul asigurării respectării legii. Aceasta va fi situația, de exemplu, atunci când Autoritatea pentru Concurență și Piețe investighează cazuri care nu sunt incriminate (de exemplu, fuziuni între societăți). În acest caz se vor aplica RGPD al Regatului Unit, coroborat cu partea 2 din DPA din 2018, deoarece prelucrarea datelor cu caracter personal de către autoritățile competente se efectuează în alte scopuri decât cele de asigurare a respectării legii. Pentru a stabili regimul de protecție a datelor aplicabil (partea 3 sau partea 2 din DPA din 2018) în ceea ce privește prelucrarea datelor cu caracter personal în cauză, autoritatea competentă, și anume operatorul de date, trebuie să analizeze dacă „scopul principal" al unei astfel de prelucrări este unul dintre scopurile de asigurare a respectării legii în temeiul DPA din 2018.

(25) În ceea ce privește domeniul de aplicare teritorial al părții 3 din DPA din 2018, secțiunea 207 punctul 2 prevede că DPA se aplică prelucrării datelor cu caracter personal în contextul activităților unei persoane care deține un sediu pe întreg teritoriul Regatului Unit. Aceasta include autoritățile publice ale teritoriilor Angliei, Țării Galilor, Scoției și Irlandei de Nord care intră în domeniul de aplicare material al părții 3 din DPA din 2018 ([39]).

2.3.1. *Definiția datelor cu caracter personal și a prelucrării*

(26) Conceptele-cheie de date cu caracter personal și prelucrare sunt definite în secțiunea 3 din DPA din 2018 și se aplică în tot cuprinsul DPA. Definițiile respectă îndeaproape definițiile corespunzătoare prevăzute la articolul 3 din Directiva (UE) 2016/680. În temeiul DPA din 2018, date cu caracter personal înseamnă orice informații privind o persoană în viață identificată sau identificabilă ([40]). În temeiul secțiunii 3 punctul 3 din DPA din 2018, o persoană fizică este identificabilă dacă poate fi identificată, direct sau indirect, pe baza informațiilor, inclusiv prin referire la un nume sau la un element de identificare, sau prin referire la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale. Noțiunea de „prelucrare" este definită ca o operațiune sau un set de operațiuni efectuate asupra informațiilor, sau asupra seturilor de informații, cum ar fi (a) colectarea, înregistrarea, organizarea, structurarea sau stocarea; (b) adaptarea sau modificarea; (c) extragerea, consultarea sau utilizarea; (d) dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod; (e) alinierea sau combinarea; sau (f) restricționarea, ștergerea sau distrugerea. În plus, legea definește „prelucrarea datelor sensibile" ca fiind „(a) prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice sau apartenența la un sindicat; (b) prelucrarea datelor genetice sau a datelor biometrice, în scopul identificării unice a unei persoane fizice; (c) prelucrarea datelor cu caracter personal privind sănătatea; (d) prelucrarea datelor cu caracter personal privind viața sexuală sau orientarea sexuală a unei persoane fizice" ([41]). În acest sens, secțiunea 205 din DPA din 2018 prevede definiția „datelor biometrice" ([42]), a „datelor privind sănătatea" ([43]) și a „datelor genetice" ([44]).

([35]) Printre acestea, anexa 7 la DPA din 2018 enumeră directorii procurorilor, directorul procurorilor din Irlanda de Nord sau comisarul pentru informații.

([36]) Secțiunea 43 punctul 3 din DPA din 2018.

([37]) Secțiunea 30 punctul 3 din DPA din 2018. Serviciile de informații (Serviciul Secret de Informații, Serviciul de Securitate și Cartierul General pentru Comunicații al Guvernului Regatului Unit) nu sunt autorități competente (a se vedea secțiunea 30 punctul 2 din DPA din 2018), iar partea 3 din DPA din 2018 nu se aplică niciuneia dintre activitățile desfășurate de acestea. Activitățile lor intră în domeniul de aplicare al DPA din 2018, partea 4.

([38]) Secțiunea 31 din DPA din 2018.

([39]) Aceasta înseamnă că DPA din 2018 și, prin urmare, prezenta decizie nu se aplică teritoriilor dependente ale Coroanei Britanice și celorlalte teritorii de peste mări ale Regatului Unit, cum ar fi, de exemplu, Insulele Falkland și teritoriul Gibraltarului.

([40]) Datele cu caracter personal referitoare la persoana decedată nu intră în domeniul de aplicare al DPA din 2018.

([41]) Secțiunea 35 punctul 8 din DPA din 2018.

([42]) „Date biometrice" înseamnă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice, referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice.

([43]) „Date privind sănătatea" înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv acordarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.

([44]) „Date genetice" înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea respectivei persoane fizice, astfel cum rezultă în special în urma unei analize a unei probe biologice prelevate de la acea persoană fizică.

(27) Secțiunea 32 din DPA din 2018 clarifică definițiile termenilor „operator” și „persoană împuternicită de către operator” în contextul prelucrării datelor cu caracter personal în scopul asigurării respectării legii, urmând îndeaproape definițiile echivalente din Directiva (UE) 2016/680. Operator înseamnă autoritatea competentă care stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal. În cazul în care prelucrarea este prevăzută de lege, operatorul este autoritatea competentă căreia legea respectivă îi impune o astfel de obligație. O persoană împuternicită de către operator este definită ca fiind orice persoană care prelucrează datele cu caracter personal în numele operatorului (alta decât o persoană care este angajat al operatorului).

2.4. **Garanții, drepturi și obligații**

2.4.1. *Legalitatea și corectitudinea prelucrării*

(28) În conformitate cu secțiunea 35 din DPA din 2018, prelucrarea datelor cu caracter personal trebuie să aibă caracter legal și echitabil, într-un mod similar cu articolul 4 alineatul (1) litera (a) din Directiva (UE) 2016/680. În conformitate cu secțiunea 35 punctul 2 din DPA din 2018, prelucrarea datelor cu caracter personal în oricare dintre scopurile de asigurare a respectării legii este legală numai dacă se întemeiază pe lege și fie persoana vizată și-a dat consimțământul pentru prelucrare în acest scop, fie prelucrarea este necesară pentru îndeplinirea unei sarcini în acest scop de către o autoritate competentă.

2.4.1.1. Prelucrarea în temeiul legii

(29) În mod similar cu articolul 8 din Directiva (UE) 2016/680, pentru a se asigura legalitatea unei prelucrări care intră sub incidența DPA din 2018, partea 3, o astfel de prelucrare trebuie să fie „bazată pe lege”. Prelucrarea „legală” înseamnă prelucrarea autorizată fie prin lege, fie prin common law sau prin prerogative regale ([45]).

(30) Competențele autorităților competente sunt, în general, reglementate prin statute, ceea ce înseamnă că funcțiile și competențele acestora sunt stabilite în mod clar în legislațiile adoptate de Parlament ([46]). În anumite cazuri, poliția, precum și alte autorități competente enumerate în anexa 7 la DPA din 2018 se pot baza pe common law pentru prelucrarea datelor ([47]). Common law s-a dezvoltat prin precedente stabilite prin hotărâri ale instanțelor. Common law este relevantă în contextul competențelor de care dispune poliția, care derivă din această sursă de drept datoria sa principală de a proteja publicul prin depistarea și prevenirea criminalității ([48]). Cu toate acestea, forțele de poliție au atât

([45]) Notele explicative la DPA din 2018, punctul 181, disponibile la următoarea adresă: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf

([46]) Agenția Națională pentru Combaterea Criminalității, de exemplu, are conferite competențe în temeiul Legii privind criminalitatea și instanțele (*Crime and Courts Act*) din 2013, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2013/22/contents. În mod similar, competențele Agenției pentru Standarde Alimentare sunt prevăzute în Legea privind standardele alimentare (*Food Standards Act*) din 1999, disponibilă la următoarea adresă:https://www.legislation.gov.uk/ukpga/1999/28/contents. Alte exemple includ Legea din 1985 privind urmărirea penală a infractorilor (*Prosecution of Offenders Act*), care a creat Ministerul Public (*Crown Prosecution Service*) (a se vedea https://www.legislation.gov.uk/ukpga/1985/23/contents); Comisarii desemnați în temeiul Legii fiscale și vamale din 2005 (*Revenue and Customs Act*), care au instituit Administrația Fiscală și Vamală din Regatul Unit (*Her Majesty's Revenue and Customs*) (a se vedea https://www.legislation.gov.uk/ukpga/2005/11/contents); Legea din 1995 privind procedura penală (Scoția), care a creat Comisia scoțiană de revizuire a cauzelor penale (a se vedea https://www.legislation.gov.uk/ukpga/1995/46/contents); Legea justiției din 2002 (Irlanda de Nord), care a instituit Ministerul Public în Irlanda de Nord (a se vedea https://www.legislation.gov.uk/ukpga/2002/26/contents) și Oficiul de combatere a cazurilor grave de fraudă a fost creat, fiindu-i conferite competențe în temeiul Legii justiției penale din 1987 (a se vedea https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) De exemplu, potrivit informațiilor furnizate de autoritățile Regatului Unit, în cadrul Ministerului Public (*Crown Office and Procurator Fiscal Service*), responsabil cu urmărirea penală a cauzelor din Scoția, Lord Advocate, care este șeful sistemului de urmărire penală din Scoția, are competența de a investiga decesele și de a urmări penal infracțiunile în temeiul common law, în timp ce o parte din atribuțiile sale sunt prevăzute în statut. În plus, Coroana și, prin extensie, diverse guverne, departamente și miniștri, își întemeiază, de asemenea, competențele pe baza unei combinații de legi, de common law și de prerogative regale (acestea sunt competențe în domeniul common law conferite Coroanei, dar care sunt exercitate de miniștri).

([48]) *UK Explanatory Framework for adequacy Discussions* (Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat), secțiunea F: Asigurarea respectării legii, pagina 8 (a se vedea nota de subsol 9).

competențe în domeniul common law, cât și competențe legislative ([49]) pentru a îndeplini o astfel de obligație. În cazul în care poliția are o competență statutară, aceasta înlocuiește orice competență în domeniul common law ([50]).

(31) Extinderea competențelor și obligațiilor în domeniul common law ale funcționarului de poliție a fost recunoscută de instanțe ca incluzând „toate măsurile care se dovedesc necesare pentru menținerea păcii, prevenirea infracțiunilor sau protejarea bunurilor împotriva vătămărilor cauzate de infracțiuni” ([51]). Competențele în domeniul common law nu sunt competențe necalificate. Acestea sunt supuse unei serii de limitări, inclusiv limitelor stabilite de instanțe ([52]) și de lege, în special Legea privind drepturile omului din 1998 (Human Rights Act) și Legea privind egalitatea din 2010 (Equality Act) ([53]). În plus, pentru autoritățile competente care prelucrează date în temeiul DPA din 2018, partea 3, aceasta include exercitarea competențelor în domeniul common law în conformitate cu cerințele prevăzute în DPA din 2018 ([54]). În plus, o decizie de a efectua orice tip de prelucrare a datelor trebuie să ia în considerare cerințele orientărilor aplicabile, cum ar fi Codul de bune practici privind MoPI, precum și orientările specifice uneia dintre țările din Regatul Unit ([55]). Guvernul și serviciile de poliție operaționale emit o serie de documente de orientare pentru a se asigura că funcționarii de poliție își exercită competențele în limitele stabilite de common law sau de statutul relevant ([56]).

(32) Prerogativele regale reprezintă o altă componentă a „legii” și se referă la anumite competențe conferite Coroanei, care pot fi exercitate de puterea executivă și care nu se bazează pe statut, ci decurg din suveranitatea monarhului ([57]). Există foarte puține exemple de prerogative relevante în contextul asigurării respectării legii. Printre acestea se numără, de exemplu, cadrul de asistență judiciară reciprocă ce permite schimbul de date de către un secretar de stat

([49]) Actele legislative cheie care prevăd regimul principalelor competențe polițienești (arestarea, perchezițiile, autorizarea menținerii în detenție, amprentarea, prelevarea probelor biologice, interceptarea mandatelor, accesul la datele de comunicare) sunt: (i) pentru Anglia și Țara Galilor, Legea din 1984 privind funcționarea Poliției și administrarea probelor penale (*Police and Criminal Evidence Act*) (PACE), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1984/60/contents [astfel cum a fost modificată prin Legea din 2012 privind apărarea libertăților (*Protection of Freedoms Act*) (PoFA)], disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2012/9/contents) și Legea din 2016 privind competențele de investigare (*Investigatory Powers Act*) (IPA), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2016/25/contents), (ii) pentru Scoția, Legea scoțiană privind justiția penală din 2016, disponibilă la următoarea adresă: https://www.legislation.gov.uk/asp/2016/1/contents, și Legea scoțiană privind procedura penală din 1995, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/1995/46/contents (iii) pentru Irlanda de Nord, Ordinul nord-irlandez din 1989 privind funcționarea Poliției și administrarea probelor penale (*Police and Criminal Evidence Order*), disponibil la următoarea adresă: https://www.legislation.gov.uk/nisi/1989/1341/contents

([50]) Autoritățile Regatului Unit au explicat că supremația dreptului material este consacrată de mult timp în Regatul Unit, încă de la pronunțarea hotărârii în cauza Entick/Carrington [1765] EWHC KB J98, care a recunoscut că există limitări ale exercitării competențelor de către puterea executivă și a stabilit principiul conform căruia competențele în domeniul common law și competențele prerogative ale monarhului și guvernului sunt subordonate legii țării.

([51]) A se vedea cauza Rice/Connolly [1966] 2 QB 414.

([52]) A se vedea cauza R(Catt)/Association of Chief police Officers [2015] AC 1065, în care, în ceea ce privește competența poliției de a obține și de a deține informații cu privire la o persoană fizică (care a comis o infracțiune), Lord Sumption a susținut că, în temeiul common law, poliția are competența de a obține și de a stoca informații în scopuri polițienești, și anume, în general, pentru menținerea ordinii publice și prevenirea și depistarea infracțiunilor. Aceste competențe nu autorizează metode intruzive de obținere a informațiilor, cum ar fi intrarea pe proprietăți private sau acte (altele decât arestarea în temeiul competențelor în domeniul common law) care ar constitui un atac. Judecătorul a considerat că, în această cauză, competențele în domeniul common law sunt în mare măsură suficiente pentru a autoriza obținerea și stocarea tipului de informații publice în cauză cu privire la aceste recursuri.

([53]) Legea privind egalitatea din 2010, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) Pentru un exemplu de cauză în care competențele în domeniul common law ale poliției sunt evaluate în cadrul DPA din 1998, a se vedea hotărârea Înaltei Curți în cauza Bridges/the Chief Constable of South Wales Police (a se vedea nota de subsol 33). A se vedea, de asemenea, cauzele Vidal-Hall/Google Inc [2015] EWCA Civ 311 și Richard/BBC [2018] EWHC 1837 (Ch).

([55]) A se vedea, de exemplu, orientările Serviciului de Poliție din Irlanda de Nord cu privire la instrucțiunile serviciului de gestionare a evidențelor, disponibile la următoarea adresă: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Camera Comunelor a publicat un document de informare care stabilește principalele competențe legale și în domeniul common law ale serviciului de poliție din Anglia și Țara Galilor (a se vedea https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Potrivit acestui document, de exemplu, în vreme ce competențele de a menține „pacea Coroanei” reprezintă competențe derivate din common law, ca și „utilizarea forței”, „competențele de oprire de către poliție în vederea efectuării unui control și de percheziție” derivă întotdeauna din Statut. În plus, guvernul scoțian furnizează pe site-ul său web informații cu privire la competențele poliției în materie de arestare și de oprire în vederea efectuării unui control și de percheziție (a se vedea https://www.gov.scot/policies/police/police-powers/).

([57]) Potrivit informațiilor furnizate de autoritățile Regatului Unit, prerogativele exercitate de guvern includ, de exemplu, elaborarea și ratificarea tratatelor, aplicarea diplomației, utilizarea forțelor armate pe teritoriul Regatului Unit pentru a menține pacea în sprijinul poliției.

cu țări terțe în scopul asigurării respectării aplicării legii, iar competența de a face schimb de date în acest mod nu este întotdeauna prevăzută în statut ([58]). Prerogativele regale sunt supuse principiilor common law ([59]) și sunt subordonate statutului, prin urmare, se află sub rezerva limitelor prevăzute de Legea privind drepturile omului din 1998 și de DPA din 2018 ([60]).

(33) În mod similar cu articolul 8 din Directiva (UE) 2016/680, regimul din Regatul Unit prevede că, pentru a respecta principiul legalității, autoritățile competente ar trebui să se asigure că, atunci când prelucrarea se bazează pe lege, aceasta trebuie să fie, de asemenea, „necesară" pentru îndeplinirea unei sarcini în scopul asigurării respectării legii. ICO oferă orientări în acest sens, clarificând faptul că „trebuie să fie o modalitate specifică și proporțională de atingere a scopului. Temeiul legal nu se va aplica dacă puteți atinge obiectivul în mod rezonabil prin alte mijloace mai puțin intruzive. Nu este suficient să susțineți că prelucrarea este necesară deoarece ați ales să vă desfășurați activitatea într-un anumit mod. Întrebarea este dacă prelucrarea este necesară pentru scopul declarat" ([61]).

2.4.1.2. Prelucrarea pe baza „consimțământului" persoanei vizate

(34) Astfel cum se menționează în considerentul 28, secțiunea 35 alineatul (2) din DPA din 2018 prevede posibilitatea prelucrării datelor cu caracter personal pe baza „consimțământului" persoanei fizice.

(35) Cu toate acestea, consimțământul nu pare a fi un temei juridic relevant pentru operațiunile de prelucrare care intră în domeniul de aplicare al prezentei decizii. În fapt, operațiunile de prelucrare care fac obiectul prezentei decizii vor viza întotdeauna datele care au fost transferate în temeiul Directivei (UE) 2016/680 de către o autoritate competentă a unui stat membru către o autoritate competentă din Regatul Unit. Prin urmare, acestea nu vor implica, de regulă, tipul de interacțiune (colectare) directă între o autoritate publică și persoanele vizate care se poate baza pe consimțământ în temeiul secțiunii 35 punctul 2 litera (a) din DPA din 2018.

(36) Deși recurgerea la consimțământ nu este, prin urmare, considerată relevantă pentru evaluarea efectuată în temeiul prezentei decizii, trebuie remarcat, din motive de exhaustivitate, faptul că, într-un context de asigurare a respectării legii, prelucrarea nu se bazează niciodată exclusiv pe consimțământ, întrucât o autoritate competentă trebuie să aibă întotdeauna o competență subiacentă care să îi permită să prelucreze datele ([62]). Mai precis, și în mod similar cu ceea ce este permis în temeiul Directivei (UE) 2016/680 ([63]), aceasta înseamnă că respectivul consimțământ servește drept condiție suplimentară pentru a permite anumite operațiuni de prelucrare limitate și specifice care altfel nu ar putea fi efectuate, de exemplu colectarea și prelucrarea unui eșantion de ADN al unei persoane fizice care nu are calitatea de suspect. În acest caz, prelucrarea nu ar fi efectuată în cazul în care consimțământul nu este acordat sau este retras ([64]).

([58]) În acest sens, a se vedea evaluarea regimului de transfer ulterior al Regatului Unit în considerentele 74-87.

([59]) A se vedea cauza Bancoult/Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, în care instanțele au considerat că prerogativa de a emite ordine în Consiliu era, de asemenea, supusă motivelor obișnuite de control jurisdicțional.

([60]) A se vedea cauza Attorney-General/De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, în care instanța a considerat că prerogativele nu pot fi exercitate atunci când le înlocuiesc competențele legale; cauza Laker Airways Ltd/Department of Trade [1977] QB 643, în care instanța a constatat că prerogativele nu pot fi utilizate pentru a aduce atingere dreptului material; cauza R/Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, în care instanța a considerat că prerogativele nu pot fi utilizate în cazul în care acestea intră în conflict cu legislația adoptată, chiar și atunci când legislația adoptată nu este încă în vigoare; cauza R (Miller)/Secretary of State for Exiting the European Union [2017] UKSC 5, în care instanța a confirmat capacitatea dreptului material de a ajusta și de a elimina prerogativele. Pentru o perspectivă generală asupra relației dintre prerogativele regale și competențele statutare sau în domeniul common law, a se vedea nota de informare a Camerei Comunelor, disponibilă la următoarea adresă: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) Ghid privind prelucrarea datelor în scopul asigurării respectării legii, „Care este sensul primului principiu?" disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Acest lucru rezultă din formularea dispoziției relevante din DPA din 2018, potrivit căreia prelucrarea datelor cu caracter personal în oricare dintre scopurile de asigurare a respectării legii este legală numai dacă și în măsura în care „aceasta se întemeiază pe lege" și fie (a) persoana vizată și-a dat consimțământul pentru prelucrare în acest scop, fie (b) prelucrarea este necesară pentru îndeplinirea unei sarcini în acest scop de către o autoritate competentă.

([63]) A se vedea considerentele 35 și 37 din Directiva (UE) 2016/680.

([64]) Autoritățile Regatului Unit au explicat că un exemplu de situație în care consimțământul poate constitui o bază adecvată pentru prelucrare ar fi cazul în care poliția obține un eșantion de ADN în legătură cu o persoană dispărută pentru a-l compara cu un trup neînsuflețit eventual găsit. În astfel de circumstanțe, ar fi inadecvat ca poliția să oblige persoana vizată să furnizeze un eșantion; în schimb, poliția ar trebui să solicite consimțământul persoanei fizice, care este acordat în mod liber și poate fi retras în orice moment. În cazul în care consimțământul este retras, datele nu mai pot fi prelucrate, cu excepția cazului în care s-a stabilit un nou temei juridic pentru continuarea prelucrării eșantionului (de exemplu, persoana vizată a devenit suspectă). Un alt exemplu ar putea apărea atunci când o forță de poliție investighează o infracțiune în care o victimă (ar putea fi victima unei tâlhării, a unei infracțiuni sexuale, a violenței domestice, rude ale unei omucideri sau alte victime ale infracțiunilor) ar putea beneficia de o trimitere la serviciul de sprijinire a victimelor (o organizație de caritate independentă dedicată sprijinirii persoanelor afectate de acte de criminalitate și de incidente traumatice). În astfel de circumstanțe, poliția va transmite serviciului de sprijinire a victimelor doar informații cu caracter personal referitoare la nume și date de contact, numai cu consimțământul victimei în acest sens.

(37) În cazurile în care se impune consimțământul persoanei fizice, acest consimțământ trebuie să fie lipsit de ambiguitate și să implice o acțiune pozitivă fără echivoc ([65]). Forțele de poliție trebuie să aibă la dispoziție o declarație de confidențialitate care să includă, printre altele, informațiile necesare referitoare la utilizarea valabilă a consimțământului. În plus, unele dintre acestea publică materiale suplimentare privind modul în care respectă legislația privind protecția datelor, inclusiv modul și momentul în care ar utiliza consimțământul ca temei juridic ([66]).

2.4.1.3. Prelucrarea datelor sensibile

(38) Ar trebui să existe garanții specifice în cazul în care sunt prelucrate „categorii speciale" de date. În acest sens, în mod similar cu dispozițiile articolului 10 din Directiva (UE) 2016/680, partea 3 din DPA din 2018 prevede garanții mai solide pentru așa-numita „prelucrare a datelor sensibile" ([67]).

(39) În conformitate cu secțiunea 35 punctul 3 din DPA din 1998, datele cu caracter sensibil pot fi prelucrate de autoritățile competente în scopul asigurării respectării legii numai în două cazuri: (1) persoana vizată și-a dat consimțământul pentru prelucrare în scopul asigurării respectării legii și, în momentul în care prelucrarea este efectuată, operatorul dispune de un document de politică adecvat ([68]) sau (2) prelucrarea este strict necesară în scopul asigurării respectării legii, prelucrarea îndeplinește cel puțin una dintre condițiile din anexa 8 la DPA din 2018 și, la momentul efectuării prelucrării, operatorul dispune de un document de politică adecvat ([69]).

(40) În ceea ce privește primul caz și astfel cum se explică în considerentul 38, recurgerea la consimțământ nu este considerată relevantă în cazul transferului care face obiectul prezentei decizii ([70]).

(41) Atunci când prelucrarea datelor cu caracter sensibil nu se bazează pe consimțământ, aceasta poate fi efectuată utilizând una dintre condițiile enumerate în anexa 8 la DPA din 2018. Aceste condiții se referă la prelucrarea necesară în scopuri prevăzute de lege; administrarea justiției; protecția intereselor vitale ale persoanei vizate sau ale altei persoane fizice; protejarea copiilor și a persoanelor expuse riscului; acțiuni în justiție; acte judiciare; prevenirea fraudei; arhivarea; în cazul în care datele cu caracter personal sunt făcute publice în mod manifest de către persoana vizată. Cu excepția cazului în care datele sunt făcute publice în mod manifest, toate condițiile prevăzute în anexa 8 sunt supuse unui test de „strictă necesitate". Astfel cum a clarificat ICO, „strict necesar în acest context înseamnă că prelucrarea trebuie să corespundă unei nevoi sociale presante, pe care nu o puteți realiza în mod rezonabil prin

([65]) Nu există o definiție separată a „consimțământului" în scopul prelucrării datelor cu caracter personal în temeiul părții 3 din DPA din 2018. ICO a oferit orientări cu privire la noțiunea de „consimțământ" în temeiul DPA din 2018, partea 3, clarificând faptul că acesta are același înțeles și ar trebui să fie aliniat la definiția prevăzută în RGPD, în special „consimțământul trebuie să fie acordat în mod liber, specific și în cunoștință de cauză și trebuie să existe o alegere reală în ceea ce privește acceptarea prelucrării datelor" [Ghid privind prelucrarea datelor în scopul asigurării respectării legii, „Care este sensul primului principiu?" (a se vedea nota de subsol 64) și Ghidul privind protecția datelor în materie de consimțământ, disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) A se vedea, de exemplu, informațiile de pe pagina web a poliției din Lincolnshire (https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) sau de pe pagina web a poliției din West Yorkshire (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Secțiunea 35 punctul 8 din DPA din 2018.

([68]) Secțiunea 35 punctul 4 din DPA din 2018.

([69]) Secțiunea 35 punctul 5 din DPA din 2018.

([70]) Din motive de exhaustivitate, trebuie remarcat faptul că, atunci când prelucrarea se bazează pe consimțământ, acesta trebuie să fie acordat în mod liber, specific și în cunoștință de cauză și trebuie să existe o alegere specifică în ceea ce privește acceptarea datelor prelucrate. În plus, atunci când prelucrează date pe baza consimțământului persoanei vizate, operatorul trebuie să dispună de un „document de politică adecvat" (appropriate policy document – APD). Secțiunea 42 din DPA din 2018 prezintă cerințele pe care trebuie să le îndeplinească APD. În aceasta se precizează că documentul trebuie cel puțin să explice procedurile operatorului de asigurare a respectării principiilor privind protecția datelor și să explice politicile operatorului în ceea ce privește păstrarea și ștergerea datelor cu caracter personal. În conformitate cu secțiunea 42 din DPA din 2018, aceasta înseamnă că operatorul trebuie să prezinte un document care (a) explică procedurile operatorului de asigurare a conformității cu principiile privind protecția datelor; și (b) explică politicile operatorului în ceea ce privește păstrarea și ștergerea datelor cu caracter personal prelucrate pe baza consimțământului persoanei vizate sau indicând perioada probabilă de păstrare a acestor date cu caracter personal. În special, documentul de politică prevede că operatorul, respectându-și obligația de înregistrare a activităților de prelucrare, ar trebui să includă întotdeauna elementele menționate la literele (a) și (b). ICO a publicat un model de document (Ghid privind prelucrarea datelor în scopul asigurării respectării legii. „Condiții de prelucrare a datelor sensibile", disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) și pot lua măsuri de asigurare a respectării legii în cazul în care operatorii nu îndeplinesc aceste cerințe. APD este, de asemenea, consultat de instanțe atunci când se iau în considerare posibile încălcări ale DPA din 2018. De exemplu, în cauza recentă R (Bridges)/Chief Constable of South Wales Police, instanțele au analizat APD-ul operatorului și au constatat că acesta este adecvat, însă ar fi avut nevoie de mai multe detalii. Prin urmare, poliția din sudul Țării Galilor a revizuit APD și l-a actualizat în conformitate cu noile orientări ale ICO (a se vedea nota de subsol 33). În plus, în conformitate cu secțiunea 42 punctul 3 din DPA din 2018, APD ar trebui să facă obiectul unei revizuiri periodice de către operator. În cele din urmă, ca o garanție suplimentară, în conformitate cu secțiunea 42 punctul 4 din DPA din 2018, operatorul are obligația de a ține o evidență consolidată a activităților de prelucrare, inclusiv elemente suplimentare față de obligația generală care îi revine operatorului de a ține evidențe ale activităților de prelucrare prevăzute în secțiunea 61 din DPA din 2018.

mijloace mai puțin intruzive" ([71]). În plus, unele condiții fac obiectul unor restricții suplimentare. De exemplu, pentru a se baza pe condiția „scopurilor statutare" și pe „condiția de salvgardare" (anexa 8, punctul 1 și punctul 4), trebuie să fie îndeplinit un test suplimentar privind interesul public substanțial. În plus, în ceea ce privește condițiile referitoare la protecția copilului (anexa 8, punctul 4), persoana vizată trebuie, de asemenea, să aibă o anumită vârstă și să fie considerată ca fiind expusă riscului. În plus, operatorul poate aplica condiția prevăzută la punctul 4 din anexa 8 numai în cazul unor circumstanțe specifice ([72]). În mod similar, există restricții în ceea ce privește condițiile privind „actele judiciare" și „prevenirea fraudei" (punctele 7 și, respectiv, 8 din anexa 8). Ambele sunt aplicabile numai anumitor operatori. În cazul actelor judiciare, numai o instanță sau o altă autoritate judiciară poate utiliza o astfel de condiție, iar în cazul prevenirii fraudei numai operatorii care sunt organizații antifraudă se pot baza pe această condiție.

(42) În cele din urmă, atunci când prelucrarea se bazează pe una dintre condițiile enumerate în anexa 8 și, respectiv, în conformitate cu secțiunea 42 din DPA din 2018, trebuie să existe un „document de politică adecvat" – care să explice procedurile operatorului de asigurare a conformității cu principiile privind protecția datelor și politicile operatorului în ceea ce privește păstrarea și ștergerea datelor cu caracter personal – și se aplică obligațiile privind ținerea unei evidențe consolidate.

2.4.2. *Limitarea scopului*

(43) Datele cu caracter personal ar trebui să fie prelucrate într-un scop anume și să fie utilizate ulterior numai în măsura în care acest lucru nu este incompatibil cu scopul prelucrării. Acest principiu privind protecția datelor este garantat de secțiunea 36 din DPA din 2018. Această dispoziție, în mod similar cu articolul 4 alineatul (1) litera (b) din Directiva (UE) 2016/680, prevede că (a) scopul asigurării respectării legii pentru care datele cu caracter personal sunt colectate în orice moment trebuie să fie determinat, explicit și legitim și (b) datele cu caracter personal colectate astfel nu trebuie să fie prelucrate într-un mod incompatibil cu scopul pentru care au fost colectate.

(44) În cazul în care autoritățile competente prelucrează date în scopul asigurării respectării legii, acesta poate viza arhivarea, cercetarea științifică sau istorică și scopurile statistice ([73]). În aceste cazuri, DPA din 2018 clarifică, de asemenea, faptul că arhivarea (sau prelucrarea în scopuri de cercetare științifică sau istorică și în scopuri statistice) nu este permisă în cazul în care aceasta este efectuată cu privire la deciziile luate în legătură cu o anumită persoană vizată sau în cazul în care aceasta este susceptibilă să îi cauzeze prejudicii sau suferințe substanțiale ([74]).

2.4.3. *Exactitatea și reducerea la minimum a datelor*

(45) Datele trebuie să fie exacte și, dacă este cazul, actualizate. De asemenea, trebuie să fie adecvate, relevante și neexcesive în raport cu scopurile în care sunt prelucrate. În mod similar cu articolul 4 alineatul (1) literele (c), (d) și (e) din Directiva (UE) 2016/680, aceste principii sunt asigurate în secțiunile 37 și 38 din DPA din 2018. Trebuie luate toate măsurile care se impun pentru a se asigura că datele cu caracter personal inexacte ([75]) sunt

([71]) Ghid privind prelucrarea datelor în scopul asigurării respectării legii, „Condiții de prelucrare a datelor sensibile" (a se vedea nota de subsol 70).

([72]) Prelucrarea se efectuează fără consimțământul persoanei vizate atunci când: (a) consimțământul pentru prelucrare nu poate fi acordat de persoana vizată; (b) nu se poate aștepta în mod rezonabil ca operatorul să obțină consimțământul persoanei vizate pentru prelucrare; (c) prelucrarea trebuie efectuată fără consimțământul persoanei vizate, deoarece obținerea consimțământului persoanei vizate ar aduce atingere dispoziției privind protecția menționată la subpunctul 1 litera (a).

([73]) A se vedea secțiunea 41 punctul 1 din DPA din 2018.

([74]) A se vedea secțiunea 41 punctul 2 din DPA din 2018.

([75]) Secțiunea 205 din DPA din 2018 definește termenul „inexact" ca referindu-se la date cu caracter personal „incorecte sau înșelătoare". Autoritățile Regatului Unit au explicat că este tipic faptul că datele referitoare la cercetările penale vor fi adesea incomplete, dar indiferent de acest lucru, pot fi exacte.

șterse sau rectificate fără întârziere ([76]), având în vedere scopul asigurării respectării legii pentru care sunt prelucrate ([77]), precum și pentru a se asigura că datele cu caracter personal inexacte, incomplete sau care nu mai sunt actualizate nu sunt transmise sau puse la dispoziție în oricare dintre scopurile de asigurare a respectării legii ([78]).

(46) În plus, în mod similar cu articolul 7 din Directiva (UE) 2016/680, regimul de protecție a datelor din Regatul Unit prevede că, pe cât posibil, trebuie să se facă o distincție între datele cu caracter personal bazate pe fapte și datele cu caracter personal bazate pe evaluări personale ([79]). Atunci când este relevant și în măsura posibilului, trebuie făcută o distincție clară între datele cu caracter personal referitoare la diferite categorii de persoane vizate, cum ar fi suspecți, persoane condamnate pentru comiterea unei infracțiuni, victime ale unei infracțiuni și martori ([80]).

2.4.4. *Limitarea stocării*

(47) În conformitate cu articolul 5 din Directiva (UE) 2016/680, în principiu, datele ar trebui să fie păstrate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor pentru care sunt prelucrate datele cu caracter personal. În conformitate cu secțiunea 39 din DPA din 2018 și în mod similar cu articolul 5 din directiva menționată, este interzisă păstrarea datelor cu caracter personal prelucrate în oricare dintre scopurile de asigurare a respectării legii pe o perioadă care depășește perioada necesară îndeplinirii scopului pentru care sunt prelucrate. Regimul juridic din Regatul Unit impune stabilirea unor termene adecvate pentru revizuirea periodică a necesității de a continua stocarea datelor cu caracter personal pentru oricare dintre scopurile de asigurare a respectării legii. Norme suplimentare privind practicile legate de păstrarea datelor cu caracter personal și termenele aplicabile au fost stabilite în legislația relevantă și în orientările care reglementează competențele și funcționarea serviciului de poliție. De exemplu, în Anglia și Țara Galilor, Codul de bune practici privind MoPI al Colegiului de Poliție, împreună cu Orientările APP privind gestionarea informațiilor cu caracter polițienesc, oferă un cadru pentru a asigura un proces coerent de păstrare, revizuire și eliminare bazat pe riscuri pentru gestionarea informațiilor serviciilor de poliție operaționale ([81]). Acest cadru stabilește așteptări clare în cadrul serviciului cu privire la modul în care ar trebui create, partajate, utilizate și gestionate informațiile la nivelul și între forțele de poliție individuale și alte agenții ([82]). Poliția trebuie să respecte Codul de bune practici, iar conformitatea este verificată de Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services ([83]).

(48) Serviciul de Poliție din Irlanda de Nord (PSNI) nu este obligat prin lege să respecte Codul de bune practici privind MoPI. Cu toate acestea, cadrul MoPI adoptat în 2011 este completat de un manual PSNI ([84]), care stabilește politici și proceduri privind modul în care Codul de bune practici privind MoPI este aplicat în Irlanda de Nord.

([76]) Secțiunea 38 punctul 1 litera (b) din DPA din 2018.

([77]) În conformitate cu Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, „acest lucru asigură recunoașterea atât a drepturilor persoanelor vizate, cât și a nevoilor operaționale ale agențiilor responsabile de asigurarea respectării legii. Punctul de mai sus a fost analizat cu atenție în cursul etapelor de elaborare a proiectului de lege privind protecția datelor, întrucât pot exista motive operaționale specifice și limitate pentru care datele nu pot fi rectificate. Cel mai probabil, acest lucru se va întâmpla dacă datele cu caracter personal inexacte în cauză trebuie păstrate în forma lor originală în scopuri probatorii" (a se vedea Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea F: Asigurarea respectării legii, pagina 21, a se vedea nota de subsol 9).

([78]) Secțiunea 38 punctul 4 din DPA din 2018. În plus, în temeiul secțiunii 38 punctul 5 din DPA din 2018, calitatea datelor cu caracter personal trebuie verificată înainte ca acestea să fie transmise sau puse la dispoziție, în toate cazurile de transmitere a datelor cu caracter personal, informațiile necesare ce permit destinatarului să evalueze gradul de exactitate, de exhaustivitate și de fiabilitate a datelor, precum și măsura în care acestea sunt actualizate trebuie incluse și, în cazul în care, după transmiterea datelor cu caracter personal, rezultă că datele au fost incorecte sau că transmiterea a fost ilegală, destinatarul trebuie să fie informat fără întârziere.

([79]) Secțiunea 38 punctul 2 din DPA din 2018.

([80]) Secțiunea 38 punctul 3 din DPA din 2018.

([81]) Acest cadru asigură coerența în ceea ce privește aplicarea stocării datelor cu caracter personal obținute. Perioada de reexaminare depinde de tipul de infracțiuni, care sunt împărțite în 4 grupe: (1) anumite aspecte legate de protecția publică; (2) alte infracțiuni violente și grave de natură sexuală; (3) toate celelalte infracțiuni; (4) diverse. Mai multe detalii sunt disponibile în Orientările APP privind gestionarea informațiilor cu caracter polițienesc (a se vedea nota de subsol 26).

([82]) Potrivit informațiilor furnizate de autoritățile Regatului Unit, alte organizații sunt libere să respecte principiile Codului de bune practici al MoPI dacă doresc, de exemplu, Administrația Fiscală și Vamală din Regatul Unit și Agenția Națională pentru Combaterea Criminalității adoptă în mod voluntar multe dintre principiile Codului de bune practici privind MoPI pentru a asigura coerența în materie de asigurare a respectării legii. În general, majoritatea organizațiilor vor pune la dispoziția personalului lor politici și orientări specifice pentru întregul personal cu privire la modul de gestionare a datelor cu caracter personal, ca parte a rolului lor și adaptate în funcție de fiecare organizație în parte. Aceasta ar include, de obicei, și formarea obligatorie.

([83]) Codul de bune practici privind MoPI a fost emis prin utilizarea competențelor prevăzute în Legea privind poliția din 1996, care permite Colegiului de Poliție să emită coduri de bune practici în legătură cu funcționarea eficientă a poliției. Orice cod de bune practici elaborat în temeiul legii trebuie să fie aprobat de secretarul de stat și face obiectul consultării Agenției Naționale pentru Combaterea Criminalității înainte de a fi transmis Parlamentului. Secțiunea 39A punctul 7 din Legea privind poliția din 1996 prevede că poliția trebuie să țină seama în mod corespunzător de codurile emise în temeiul Legii privind poliția din 1996.

([84]) Manualul PSNI privind MoPI, capitolele 1-6.

(49) În Scoția, forțele de poliție se bazează pe procedura operațională standard privind păstrarea evidențelor (SOP) ([85]), care sprijină politica de gestionare a evidențelor ([86]) Serviciului de Poliție din Scoția. SOP stabilește norme specifice de păstrare a evidențelor deținute de serviciul de poliție din Scoția.

(50) În plus față de cerința generală de revizuire a evidențelor care se aplică pe întreg teritoriul Regatului Unit, sunt furnizate detalii suplimentare în normele localizate. Pentru a da câteva exemple, în ceea ce privește Anglia și Țara Galilor, Legea privind funcționarea Poliției și administrarea probelor penale, astfel cum a fost modificată prin Legea din 2012 privind apărarea libertăților (PoFA), prevede păstrarea amprentelor digitale și a profilurilor ADN, precum și un regim specific pentru persoanele fizice care nu au fost condamnate ([87]). De asemenea, PoFA a creat funcția de comisar pentru păstrarea și utilizarea materialelor biometrice (denumit în continuare „comisarul pentru biometrie") ([88]). Normele specifice privind imaginile de custodie sunt prevăzute în revista „Custody Image Review" din 2017 ([89]). În ceea ce privește Scoția, Legea scoțiană privind procedura penală din 1995 prevede normele pentru obținerea și păstrarea amprentelor digitale și a probelor biologice ([90]). La fel ca în cazul Angliei și Țării Galilor, legislația reglementează păstrarea datelor biometrice în diferite cazuri ([91]).

2.4.5. *Securitatea datelor*

(51) Datele cu caracter personal ar trebui prelucrate într-un mod care să le asigure securitatea, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale. În acest scop, autoritățile publice trebuie să ia măsurile tehnice sau organizatorice adecvate pentru a proteja datele cu caracter personal împotriva eventualelor amenințări. Aceste măsuri trebuie să fie evaluate luând în considerare cunoștințele actuale și costurile aferente.

(52) Aceste principii sunt reflectate în secțiunea 40 din DPA din 2018, potrivit căreia, în mod similar cu articolul 4 alineatul (1) litera (f) din Directiva (UE) 2016/680, datele cu caracter personal prelucrate pentru oricare dintre scopurile de asigurare a respectării legii trebuie prelucrate într-un mod care să asigure securitatea adecvată a datelor cu caracter personal, prin luarea de măsuri tehnice sau organizatorice corespunzătoare. Aceasta include protecția

([85]) Procedura operațională standard privind păstrarea evidențelor (SOP), disponibilă la următoarea adresă: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) Pentru mai multe detalii privind gestionarea evidențelor, a se vedea informațiile referitoare la registrele naționale din Scoția, disponibile la următoarea adresă: https://www.nrscotland.gov.uk/record-keeping/records-management

([87]) Perioadele de păstrare variază în funcție de faptul dacă o persoană fizică a fost condamnată sau nu (secțiunile 63I-63KI din PACE din 1984). De exemplu, în cazul unui adult condamnat pentru o infracțiune înregistrabilă, amprentele sale digitale și profilul său ADN pot fi păstrate pe o perioadă nedeterminată [secțiunea 63I punctul 2 din PACE din 1984], în timp ce păstrarea este limitată în timp dacă persoana condamnată are sub 18 ani, infracțiunea este o infracțiune „minoră" care poate fi înregistrată, iar persoana nu a fost condamnată anterior (secțiunea 63K din PACE din 1984). Păstrarea în cazul unei persoane arestate sau acuzate, dar necondamnate, este limitată în timp la trei ani (secțiunea 63F din PACE din 1984). Prelungirea acestei perioade de păstrare trebuie să fie aprobată de autoritatea judiciară [secțiunea 63F punctul 7 din PACE din 1984]. În cazul persoanelor arestate sau acuzate, dar care nu au fost condamnate pentru infracțiuni minore, nu este posibilă reținerea acestora (secțiunea 63D și secțiunea 63H din PACE din 1984).

([88]) Secțiunea 20 din PoFA din 2012 creează poziția comisarului pentru biometrie. Printre alte funcții, comisarul pentru biometrie decide dacă poliția poate păstra sau nu înregistrările profilurilor ADN și amprentele digitale obținute de la persoanele arestate, dar care nu sunt acuzate de o infracțiune calificată (secțiunea 63G din PACE din 1984). În plus, comisarul pentru biometrie are responsabilitatea generală de a supraveghea păstrarea și utilizarea ADN-ului și a amprentelor digitale, precum și păstrarea din motive de securitate națională (secțiunea 20 punctul 2 din PoFA din 2012). Comisarul pentru biometrie este numit în temeiul Codului privind numirile publice [codul este disponibil la următoarea adresă: Codul de guvernanță pentru numirile publice – GOV.UK (www.gov.uk)], iar condițiile numirii sale indică în mod clar faptul că acesta poate fi demis din funcție de către ministrul de interne numai în anumite circumstanțe definite în mod strict; printre acestea se numără neexercitarea atribuțiilor sale pentru o perioadă de trei luni, condamnarea pentru săvârșirea unei infracțiuni sau nerespectarea condițiilor numirii sale.

([89]) Review of the Use and Retention of Custody Images (Revizuirea utilizării și păstrării imaginilor de custodie), disponibil la următoarea adresă: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) Secțiunea 18 și următoarele din Legea scoțiană privind procedura penală din 1995.

([91]) Perioadele de păstrare variază în funcție de condamnarea sau nu a persoanei (secțiunea 18 punctul 3 din Legea scoțiană privind procedura penală din 1995) sau de calitatea sa de minor. În acest din urmă caz, perioada de păstrare este de 3 ani de la condamnarea în cadrul audierii copiilor (secțiunea 18E punctul 8 din Legea scoțiană privind procedura penală din 1995). Datele persoanelor arestate, dar care nu au fost condamnate nu pot fi păstrate (secțiunea 18 punctul 3 din Legea scoțiană privind procedura penală din 1995), cu excepția cazurilor specifice și în funcție de gravitatea infracțiunii (secțiunea 18A din Legea scoțiană privind procedura penală din 1995). Legea din 2020 privind comisarul scoțian pentru biometrie (*The Scottish Biometrics Commissioner Act 2020*) (a se vedea https://www.legislation.gov.uk/asp/2020/8/contents) creează poziția de comisar scoțian pentru biometrie, care trebuie să pregătească și să revizuiască coduri de bune practici (aprobate de Parlamentul scoțian) în ceea ce privește dobândirea, păstrarea, utilizarea și distrugerea datelor biometrice în scopul justiției penale și al poliției (secțiunea 7 din Legea din 2020 privind comisarul scoțian pentru biometrie).

datelor împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale ([92]). Secțiunea 66 din DPA din 2018 precizează în continuare că fiecare operator și fiecare persoană împuternicită de operator trebuie să pună în aplicare măsuri tehnice și organizatorice corespunzătoare pentru a asigura un nivel de securitate corespunzător riscurilor care decurg din prelucrarea datelor cu caracter personal. Conform notelor explicative, operatorul trebuie să evalueze riscurile și să pună în aplicare măsuri de securitate corespunzătoare pe baza acestei evaluări, de exemplu criptarea sau niveluri specifice de autorizare de securitate pentru personalul care prelucrează datele ([93]). De asemenea, evaluarea trebuie să țină seama, de exemplu, de natura datelor prelucrate și de orice alți factori sau circumstanțe relevante care ar putea afecta securitatea prelucrării.

(53) Regimul care reglementează respectarea principiilor de securitate a datelor este foarte asemănător cu cel stabilit la articolele 29-31 din Directiva (UE) 2016/680. În special, în cazul unei încălcări a securității datelor cu caracter personal în legătură cu datele cu caracter personal pentru care operatorul este responsabil, în conformitate cu secțiunea 67 punctul 1 din DPA din 2018, operatorul trebuie, fără întârzieri nejustificate și, dacă este posibil, în termen de 72 de ore de la data la care a luat cunoștință de încălcare, să notifice încălcarea securității datelor cu caracter personal comisarului pentru informații ([94]). Obligația de notificare nu se aplică atunci când este puțin probabil ca încălcarea securității datelor cu caracter personal să genereze un risc pentru drepturile și libertățile persoanelor fizice ([95]). Operatorul trebuie să documenteze faptele referitoare la eventuale încălcări ale securității datelor cu caracter personal, efectele acesteia și măsurile de remediere adoptate într-un mod care să permită comisarului pentru informații să verifice conformitatea cu DPA ([96]). În cazul în care o persoană împuternicită de operator ia cunoștință de o încălcare a securității, aceasta trebuie să informeze operatorul fără întârzieri nejustificate ([97]).

(54) În conformitate cu secțiunea 68 punctul 1 din DPA din 2018, în cazul în care o încălcare a securității datelor cu caracter personal este susceptibilă să prezinte un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul trebuie să informeze persoana vizată cu privire la încălcare, fără întârzieri nejustificate ([98]). Notificarea trebuie să includă aceleași informații ca și notificarea către comisarul pentru informații descrisă în considerentul 53. Această obligație nu se aplică în cazul în care operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcare. De asemenea, nu se aplică în cazul în care operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze. În cele din urmă, operatorul nu are obligația de a notifica persoana vizată în cazul în care acest lucru ar implica un efort disproporționat ([99]). În acest caz, informațiile trebuie puse la dispoziția persoanei vizate într-un alt mod la fel de eficient, de exemplu, prin intermediul unei comunicări publice ([100]). În cazul în care operatorul nu a informat persoana vizată cu privire la încălcare, comisarul pentru informații, după ce a fost notificat în temeiul secțiunii 67 din DPA și după analizarea probabilității încălcării care generează un risc ridicat, poate solicita operatorului să notifice persoana vizată cu privire la încălcare ([101]).

([92]) În conformitate cu notele explicative la DPA din 2018 (a se vedea nota de subsol 45), operatorul trebuie, în special: să conceapă și să își organizeze securitatea astfel încât să corespundă naturii datelor cu caracter personal pe care le deține și prejudiciului care ar putea rezulta dintr-o încălcare a securității; să stabilească în mod clar cine este responsabil în cadrul organizației lor pentru asigurarea securității informațiilor; să se asigure că dispun de securitatea fizică și tehnică adecvată, susținută de politici și proceduri solide și de personal de încredere și bine instruit și să fie pregătit să reacționeze rapid și eficace la eventuale situații de încălcare a securității.

([93]) Punctul 221 din notele explicative la DPA din 2018 (a se vedea nota de subsol 45).

([94]) Secțiunea 67 punctul 4 din DPA din 2018 prevede că notificarea trebuie să includă o descriere a caracterului încălcării securității datelor cu caracter personal (inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză), numele și datele de contact ale unui punct de contact, o descriere a consecințelor probabile ale încălcării securității datelor cu caracter personal și o descriere a măsurilor luate sau propuse spre a fi luate de operator pentru a remedia încălcarea securității datelor cu caracter personal (inclusiv, dacă este cazul, măsuri de atenuare a posibilelor efecte negative ale acesteia).

([95]) Secțiunea 67 punctul 2 din DPA din 2018.

([96]) Secțiunea 67 punctul 6 din DPA din 2018.

([97]) Secțiunea 67 punctul 9 din DPA din 2018.

([98]) În temeiul secțiunii 68 punctul 7 din DPA din 2018, operatorul poate restricționa, integral sau parțial, furnizarea de informații către persoana vizată în măsura în care și atât timp cât restricția constituie o măsură necesară și proporțională, ținând seama de drepturile fundamentale și de interesele legitime ale persoanei vizate, (a) pentru a nu obstrucționa cercetări, investigații sau proceduri oficiale ori judiciare; (b) pentru a nu prejudicia prevenirea, detectarea, investigarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale; (c) pentru a proteja securitatea publică; (d) pentru a proteja securitatea națională; (e) pentru a proteja drepturile și libertățile celorlalți.

([99]) Secțiunea 68 punctul 3 din DPA din 2018.

([100]) Secțiunea 68 punctul 5 din DPA din 2018.

([101]) Secțiunea 68 punctul 6 din DPA din 2018, sub rezerva prescripției prevăzute în secțiunea 68 punctul 8 din DPA din 2018.

2.4.6. *Transparența*

(55) Persoanele vizate trebuie să fie informate cu privire la principalele caracteristici ale prelucrării datelor lor cu caracter personal. Acest principiu privind protecția datelor este reflectat în secțiunea 44 din DPA din 2018, care, în mod similar cu articolul 13 din Directiva (UE) 2016/680, prevede că operatorul are obligația generală de a pune la dispoziția persoanelor vizate informații privind prelucrarea datelor lor cu caracter personal (fie prin punerea informațiilor la dispoziția publicului larg, fie prin orice alt mijloc) ([102]). Printre informațiile care trebuie puse la dispoziție se numără (a) identitatea și datele de contact ale operatorului; (b) datele de contact ale responsabilului cu protecția datelor, după caz; (c) scopurile în care sunt prelucrate datele cu caracter personal; (d) existența drepturilor persoanelor vizate de a solicita operatorului acces la datele cu caracter personal, rectificarea datelor cu caracter personal și ștergerea datelor cu caracter personal sau restricționarea prelucrării acestora și (e) existența dreptului de a depune o plângere în fața comisarului pentru informații și datele de contact ale comisarului ([103]).

(56) De asemenea, în cazuri specifice pentru a permite exercitarea drepturilor unei persoane vizate în temeiul DPA din 2018 (de exemplu, atunci când datele cu caracter personal care sunt prelucrate au fost colectate fără cunoștința persoanei vizate), operatorul trebuie să furnizeze persoanei vizate informații cu privire la (a) temeiul juridic al prelucrării; (b) informații cu privire la perioada pentru care vor fi stocate datele cu caracter personal sau, în cazul în care nu este posibil, criteriile utilizate pentru a stabili respectiva perioadă; (c) dacă este cazul, informații cu privire la categoriile de destinatari ai datelor cu caracter personal (inclusiv destinatarii din țări terțe sau organizații internaționale); (d) informații suplimentare necesare pentru a permite exercitarea drepturilor persoanei vizate în temeiul părții 3 din DPA din 2018 ([104]).

2.4.7. *Drepturi individuale*

(57) Persoanelor vizate trebuie să li se acorde o serie de drepturi opozabile. Partea 3 capitolul 3 din DPA din 2018 oferă persoanelor fizice drepturi de acces, de rectificare, de ștergere și de restricționare ([105]), care sunt comparabile cu cele prevăzute în capitolul 3 din Directiva (UE) 2016/680.

(58) Dreptul de acces este prevăzut la secțiunea 45 din DPA din 2018. În primul rând, o persoană fizică are dreptul de a obține o confirmare din partea operatorului dacă datele sale cu caracter personal sunt prelucrate sau nu ([106]). În al doilea rând, în cazul în care datele cu caracter personal sunt prelucrate, persoana vizată are dreptul de a accesa datele respective și de a primi următoarele informații cu privire la prelucrare: (a) scopurile și temeiurile juridice ale prelucrării; (b) categoriile de date în cauză; (c) destinatarul căruia i-au fost divulgate datele; (d) perioada de stocare a datelor cu caracter personal; (e) existența dreptului persoanei vizate la rectificarea și ștergerea datelor cu caracter personal; (f) dreptul de a depune o plângere și (g) orice informație privind originea datelor cu caracter personal în cauză ([107]).

(59) În conformitate cu secțiunea 46 din DPA din 2018, persoana vizată are dreptul de a solicita operatorului să rectifice datele cu caracter personal inexacte care o privesc. Operatorul trebuie să rectifice datele (sau, în cazul în care datele sunt inexacte deoarece sunt incomplete, să le completeze), fără întârzieri nejustificate. Dacă datele cu caracter personal trebuie să fie păstrate ca mijloace de probă, operatorul trebuie (în loc să rectifice datele cu caracter personal) să restricționeze prelucrarea acestora ([108]).

([102]) Ghidul privind prelucrarea datelor în scopul asigurării respectării legii prevede următoarele exemple: „Aveți pe site-ul dumneavoastră web o declarație generală de confidențialitate care cuprinde informații de bază despre organizație, scopul prelucrării datelor cu caracter personal, drepturile unei persoane vizate și dreptul acesteia de a depune o plângere la comisarul pentru informații. Ați primit informații potrivit cărora o persoană a fost prezentă în momentul săvârșirii unei infracțiuni. La prima intervievare a acestei persoane, trebuie să furnizați informațiile generice, precum și informațiile justificative suplimentare, pentru a permite exercitarea drepturilor sale. Puteți restricționa prelucrarea corectă a informațiilor pe care le furnizați numai dacă acestea vor afecta în mod negativ cercetarea pe care o întreprindeți" (Ghid privind prelucrarea datelor în scopul asigurării respectării legii, „Ce informații ar trebui să furnizăm unei persoane fizice?", disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Ghidul privind prelucrarea datelor în scopul asigurării respectării legii prevede că informațiile furnizate cu privire la prelucrarea datelor cu caracter personal trebuie să fie concise, inteligibile și ușor accesibile; sunt redactate într-un limbaj clar și simplu, adaptându-l la nevoile persoanelor vulnerabile, cum ar fi copiii, și sunt gratuite (Ghidul privind prelucrarea datelor în scopul asigurării respectării legii, „Cum ar trebui să furnizăm aceste informații?", disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Secțiunea 44 punctul 2 din DPA din 2018.

([105]) Pentru o analiză detaliată a drepturilor subiecților, a se vedea: Ghid privind prelucrarea datelor în scopul asigurării respectării legii în materie de drepturi individuale, disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Secțiunea 45 punctul 1 din DPA din 2018.

([107]) Secțiunea 45 punctul 2 din DPA din 2018.

([108]) Secțiunea 46 punctul 4 din DPA din 2018.

(60) Secțiunea 47 din DPA din 2018 oferă persoanelor fizice dreptul la ștergerea datelor și la restricționarea prelucrării. Operatorul trebuie ([109]) să șteargă datele cu caracter personal fără întârzieri nejustificate în cazul în care prelucrarea datelor cu caracter personal ar încălca oricare dintre principiile privind protecția datelor, temeiurile juridice ale prelucrării sau garanțiile legate de arhivare și de prelucrarea datelor sensibile. De asemenea, operatorul trebuie să șteargă datele dacă are o obligație legală în acest sens. Dacă datele cu caracter personal trebuie să fie păstrate ca mijloace de probă, operatorul trebuie (în loc să șteargă datele cu caracter personal) să restricționeze prelucrarea acestora ([110]). Operatorul trebuie să restricționeze prelucrarea datelor cu caracter personal în cazul în care o persoană vizată contestă exactitatea datelor cu caracter personal, dar nu este posibil să se stabilească dacă datele sunt exacte sau nu ([111]).

(61) În cazul în care o persoană vizată solicită rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării acestora, operatorul trebuie să informeze în scris persoana vizată dacă cererea a fost aprobată și, în cazul în care a fost refuzată, să informeze persoana vizată cu privire la motivele refuzului și căile de atac disponibile (dreptul persoanei vizate de a adresa o cerere comisarului pentru informații pentru a investiga dacă restricția a fost aplicată în mod legal, dreptul de a depune o plângere la comisarul pentru informații și dreptul de a solicita un ordin de conformitate unei instanțe) ([112]).

(62) În cazul în care operatorul rectifică datele cu caracter personal primite de la o altă autoritate competentă, acesta trebuie să informeze cealaltă autoritate ([113]). În cazul în care operatorul rectifică, șterge sau restricționează prelucrarea datelor cu caracter personal care au fost dezvăluite de către operator, operatorul trebuie să informeze destinatarii, iar destinatarii trebuie, în mod similar, să rectifice, să șteargă sau să restricționeze prelucrarea datelor cu caracter personal (în măsura în care aceștia își păstrează responsabilitățile în acest sens) ([114]).

(63) În plus, persoana vizată are dreptul de a fi informată fără întârzieri nejustificate de către operator cu privire la o încălcare a securității datelor cu caracter personal atunci când este posibil ca aceasta să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice ([115]).

(64) În ceea ce privește toate aceste drepturi ale persoanei vizate și în mod similar cu ceea ce se prevede la articolul 12 din Directiva (UE) 2016/680, operatorul are obligația de a se asigura că orice informație adresată persoanei vizate este furnizată într-o formă concisă, inteligibilă și ușor accesibilă ([116]) și, dacă este posibil, că informațiile ar trebui transmise în același format în care a fost primită cererea ([117]). Operatorul trebuie să se conformeze unei cereri a persoanei vizate fără întârzieri nejustificate sau, în orice caz, înainte, în principiu, de sfârșitul unei perioade de o lună de la depunerea cererii ([118]). În cazul în care operatorul are îndoieli întemeiate cu privire la identitatea unei persoane fizice, acesta poate solicita informații suplimentare și poate întârzia tratarea cererii până la stabilirea identității. Operatorul poate solicita o taxă rezonabilă sau poate refuza să acționeze atunci când consideră cererea ca fiind vădit nefondată ([119]). ICO a furnizat orientări cu privire la momentul în care o cerere este considerată în mod evident nefondată sau excesivă și cu privire la momentul în care poate fi solicitată o taxă ([120]).

(65) În plus, în temeiul secțiunii 53 punctul 4 din DPA din 2018, secretarul de stat poate stabili, prin reglementări, cuantumul maxim al unei taxe.

([109]) O persoană vizată poate solicita operatorului să șteargă datele cu caracter personal sau să restricționeze prelucrarea acestora (dar obligațiile operatorului de a șterge datele sau de a restricționa prelucrarea acestora se aplică indiferent dacă se face sau nu o astfel de solicitare).

([110]) Secțiunile 46 punctul 4 și 47 punctul 2 din DPA din 2018.

([111]) Secțiunea 47 punctul 3 din DPA din 2018.

([112]) Secțiunea 48 punctul 1 din DPA din 2018.

([113]) Secțiunea 48 punctul 7 din DPA din 2018.

([114]) Secțiunea 48 punctul 9 din DPA din 2018.

([115]) Secțiunea 68 din DPA din 2018.

([116]) Secțiunea 52 punctul 1 din DPA din 2018.

([117]) Secțiunea 52 punctul 3 din DPA din 2018.

([118]) Secțiunea 54 din DPA din 2018 definește sensul expresiei „perioadă de timp aplicabilă”, care înseamnă perioada de o lună sau perioada mai lungă care poate fi specificată în reglementări, începând cu momentul relevant (când operatorul primește cererea în cauză; atunci când operatorul primește informațiile (dacă există) solicitate în legătură cu o cerere în temeiul secțiunii 52 punctul 4 din DPA; sau atunci când se achită taxa (dacă există) percepută în legătură cu cererea în temeiul secțiunii 53 din DPA.

([119]) Secțiunea 53 punctul 1 din DPA din 2018.

([120]) În conformitate cu orientările ICO, un operator poate decide să perceapă taxe unei persoane vizate în cazul în care cererea acesteia este în mod evident nefondată sau excesivă, dar alege totuși să răspundă la aceasta. Taxa trebuie să fie rezonabilă și să poată justifica costul. Ghid privind prelucrarea datelor în scopul asigurării respectării legii, „Cereri vădit nefondate și excesive”, disponibil la următoarea adresă: 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. Restricționarea drepturilor persoanei vizate și obligațiile în materie de transparență

(66) În anumite circumstanțe, o autoritate competentă poate restricționa anumite drepturi ale persoanei vizate: dreptul de acces ([121]), de a fi informat ([122]), de a avea cunoștință cu privire la o încălcare a securității datelor cu caracter personal ([123]) și de a fi informat cu privire la motivul respingerii unei cereri de rectificare sau de ștergere ([124]). În mod similar cu regimul prevăzut în capitolul III din Directiva (UE) 2016/680, autoritatea competentă poate aplica restricția numai în cazul în care, având în vedere drepturile fundamentale și interesele legitime ale persoanei vizate, aceasta este necesară și proporțională: (a) pentru a nu obstrucționa cercetări, investigații sau proceduri oficiale ori judiciare; (b) pentru a nu prejudicia prevenirea, detectarea, investigarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale; (c) pentru a proteja securitatea publică; (d) pentru a proteja securitatea națională; (e) pentru a proteja drepturile și libertățile celorlalți.

(67) ICO a furnizat orientări cu privire la aplicarea acestor restricții. Potrivit acestor orientări, operatorii trebuie să efectueze o analiză de la caz la caz pentru a echilibra drepturile persoanei fizice cu prejudiciul cauzat de divulgare. În special, aceștia trebuie să justifice orice restricție aplicată ca fiind necesară și proporțională și pot limita ceea ce este prevăzut numai în cazul în care aceasta ar aduce atingere scopurilor menționate anterior ([125]).

(68) Există, de asemenea, o serie de alte orientări emise de autoritățile competente care oferă informații detaliate cu privire la toate aspectele legislației privind protecția datelor, inclusiv cu privire la aplicarea restricțiilor privind drepturile persoanelor vizate ([126]). De exemplu, în ceea ce privește secțiunea 45 punctul 4, Manualul privind protecția datelor elaborat de Consiliul național al responsabililor serviciilor de poliție prevede: „Este important de remarcat faptul că restricțiile pot fi aplicate numai în măsura în care este necesar și pot fi aplicate numai atât timp cât este necesar. Prin urmare, nu este permisă o aplicare generalizată a restricției la toate datele cu caracter personal ale solicitantului sau aplicarea permanentă a restricției. În ceea ce privește acest din urmă punct, este adesea necesar ca datele cu caracter personal colectate fără cunoștința persoanei vizate care are calitatea de suspect în cadrul unei anchete să fie protejate inițial împotriva divulgării lor, pentru a evita prejudicierea anchetei în timpul desfășurării anchetei, dar la o dată ulterioară nu ar exista niciun prejudiciu din cauza divulgării în cazul în care datele cu caracter personal ar fi fost divulgate persoanei fizice în timpul interviului. Forțele de poliție trebuie să adopte proceduri care să asigure aplicarea acestor restricții numai în măsura necesară și numai pe durata necesară” ([127]). Aceste orientări oferă, de asemenea, exemple de situații în care este probabil ca fiecare dintre restricții să fie aplicată ([128]).

(69) În plus, în ceea ce privește posibilitatea de a restricționa oricare dintre drepturile menționate mai sus pentru protecția „securității naționale”, un operator poate solicita un certificat semnat de un ministru din cadrul Cabinetului sau de procurorul general (sau de avocatul general pentru Scoția) care să ateste că restricționarea acestor drepturi este o măsură necesară și proporțională pentru protecția securității naționale ([129]). Guvernul Regatului Unit a emis orientări privind certificatele de securitate națională în temeiul DPA din 2018, care subliniază în special faptul că orice limitare a drepturilor persoanelor vizate în ceea ce privește protejarea securității naționale trebuie să fie proporțională și necesară ([130]) (pentru mai multe detalii privind certificatele de securitate națională, a se vedea considerentele 131-134).

([121]) Secțiunea 45 punctul 4 din DPA din 2018.
([122]) Secțiunea 44 punctul 4 din DPA din 2018.
([123]) Secțiunea 68 punctul 7 din DPA din 2018.
([124]) Secțiunea 48 punctul 3 din DPA din 2018.
([125]) A se vedea, de exemplu, Ghidul privind prelucrarea datelor în scopul asigurării respectării legii în materie de drept de acces, disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) A se vedea, de exemplu, Manualul privind protecția datelor pentru profesioniștii în materie de protecție a datelor în domeniul poliției emis de Consiliul național al responsabililor serviciilor de poliție (a se vedea nota de subsol 27) sau orientările furnizate de Oficiul de combatere a cazurilor grave de fraudă, disponibil la următoarea adresă: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) Manualul privind protecția datelor emis de Consiliul național al responsabililor serviciilor de poliție, pagina 140 (a se vedea nota de subsol 27).
([128]) Manualul privind protecția datelor emis de Consiliul național al responsabililor serviciilor de poliție prevede că „a nu obstrucționa cercetări, investigații sau proceduri oficiale ori judiciare” poate fi relevant în cazul datelor cu caracter personal prelucrate pentru anchete, acțiuni judiciare în materie de dreptul familiei, anchete de disciplină internă fără caracter penal și anchete precum ancheta independentă privind abuzul sexual asupra copiilor; în vreme ce „a proteja drepturile și libertățile celorlalți” este relevant pentru datele cu caracter personal care s-ar referi, de asemenea, la alte persoane, precum și la solicitant” (Manualul privind protecția datelor emis de Consiliul național al responsabililor serviciilor de poliție, pagina 140, a se vedea nota de subsol 27).
([129]) Secțiunea 79 din DPA din 2018.
([130]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, disponibile la următoarea adresă:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

(70) În plus, în cazul în care se aplică o restricție a dreptului unei persoane vizate, autoritatea competentă trebuie să informeze persoana vizată, fără întârzieri nejustificate, că drepturile sale au fost restricționate, motivele restricționării și căile de atac disponibile, cu excepția cazului în care furnizarea informațiilor respective ar submina motivul aplicării restricției ([131]). Ca o garanție suplimentară împotriva utilizării abuzive a restricțiilor, operatorul trebuie să înregistreze motivele restricționării informațiilor și să pună evidențele la dispoziția comisarului pentru informații, la cerere ([132]).

(71) În cazul în care operatorul refuză să furnizeze informații suplimentare privind transparența, sau accesul, ori refuză o cerere de rectificare, ștergere sau restricționare a prelucrării, persoana fizică poate solicita comisarului pentru informații să investigheze dacă operatorul a utilizat restricția în mod legal ([133]). De asemenea, persoana vizată poate depune o plângere la comisarul pentru informații sau poate sesiza o instanță să oblige operatorul să dea curs cererii ([134]).

2.4.7.2. Procesul decizional automatizat

(72) Secțiunile 49 și 50 din DPA din 2018 reglementează drepturile legate de procesul decizional automatizat și, respectiv, garanțiile care trebuie aplicate ([135]). În mod similar cu articolul 11 din Directiva (UE) 2016/680, operatorul poate lua o decizie semnificativă bazată exclusiv pe prelucrarea automată a datelor cu caracter personal numai dacă acest lucru este prevăzut sau autorizat prin lege ([136]). O decizie este semnificativă dacă ar produce un efect juridic negativ asupra persoanei vizate sau ar afecta în mod semnificativ persoana vizată ([137]).

(73) În cazul în care operatorul este obligat sau autorizat prin lege să ia o decizie semnificativă, secțiunea 50 din DPA din 2018 prevede garanțiile care se vor aplica unei astfel de decizii (care este definită ca o „decizie semnificativă eligibilă"). În cel mai scurt timp posibil din punct de vedere practic, operatorul trebuie să informeze persoana vizată cu privire la luarea unei astfel de decizii. Persoana vizată poate apoi, în termen de o lună, să solicite operatorului să reexamineze decizia sau să ia o nouă decizie care nu se bazează exclusiv pe prelucrarea automată. Operatorul trebuie să analizeze cererea și să informeze persoana vizată cu privire la rezultatul acestei analize. DPA din 2018 conferă secretarului de stat competența de a adopta regulamente pentru garanții suplimentare ([138]). Până în prezent nu au fost adoptate astfel de regulamente.

2.4.8. *Transferurile ulterioare*

(74) Nivelul de protecție acordat datelor cu caracter personal transferate de la o autoritate de aplicare a legii a unui stat membru către o autoritate de aplicare a legii din Regatul Unit nu trebuie să fie subminat de transferul suplimentar al acestor date către destinatari dintr-o țară terță. Astfel de „transferuri ulterioare", care, din perspectiva unei autorități de aplicare a legii din Regatul Unit, constituie transferuri internaționale din Regatul Unit, ar trebui să fie permise numai în cazul în care destinatarul suplimentar din afara Regatului Unit intră el însuși sub incidența unor norme care asigură un nivel de protecție similar cu cel garantat în cadrul ordinii juridice a Regatului Unit.

([131]) Secțiunea 44 punctele 5 și 6; secțiunea 45 punctele 5 și 6; secțiunea 48 punctul 4 din DPA din 2018.
([132]) Secțiunea 44 punctul 7; secțiunea 45 punctul 7; secțiunea 48 punctul 6 din DPA din 2018.
([133]) Secțiunea 51 din DPA din 2018.
([134]) Secțiunea 167 din DPA din 2018.
([135]) În ceea ce privește domeniul de aplicare al prelucrării automate, notele explicative la DPA din 2018 prevăd că: „aceste dispoziții se referă la un proces decizional complet automatizat și nu la prelucrarea automată. Prelucrarea automată (inclusiv crearea de profiluri) are loc atunci când se efectuează o operațiune asupra datelor fără a fi necesară intervenția umană. Acesta este utilizat în mod regulat în contextul asigurării respectării legii pentru a filtra seturi mari de date în cantități ușor de gestionat pe care un operator uman le poate utiliza ulterior. Procesul decizional automatizat este o formă de prelucrare automată și necesită ca decizia finală să fie luată fără interferențe umane". (Notele explicative la DPA, punctul 204, a se vedea nota de subsol 45).
([136]) Pe lângă măsurile de protecție prevăzute în DPA, există și alte restricții legislative în cadrul juridic al Regatului Unit, care se aplică agenților de aplicare a legii și care ar împiedica prelucrarea automată (inclusiv crearea de profiluri) care conduce la discriminare ilegală. Legea privind drepturile omului din 1998 încorporează în legislația Regatului Unit drepturile cuprinse în CEDO, inclusiv dreptul prevăzut la articolul 14 din convenție, și anume interzicerea discriminării. În mod similar, Legea privind egalitatea din 2010 interzice discriminarea persoanelor cu caracteristici protejate (care includ sexul, rasa, handicapul etc.).
([137]) Secțiunea 49 punctul 2 din DPA din 2018.
([138]) Secțiunea 50 punctul 4 din DPA din 2018.

(75) Regimul din Regatul Unit privind transferurile internaționale este reglementat de partea 3 capitolul 5 din DPA din 2018 ([139]) și reflectă abordarea adoptată în capitolul V din Directiva (UE) 2016/680. În special, pentru a transfera date cu caracter personal către o țară terță, o autoritate competentă trebuie să îndeplinească trei condiții: (a) transferul trebuie să fie necesar în scopul asigurării respectării legii; (b) transferul trebuie să se bazeze pe: (i) un regulament privind caracterul adecvat al nivelului de protecție în ceea ce privește țara terță, (ii) dacă nu se bazează pe un regulament privind caracterul adecvat al nivelului de protecție, existența unor garanții adecvate sau (iii) dacă nu se bazează pe o decizie privind caracterul adecvat al nivelului de protecție sau pe garanții adecvate, acesta trebuie să se întemeieze pe circumstanțe speciale: și (c) destinatarul transferului trebuie să fie: (i) o autoritate relevantă (și anume echivalentul unei autorități competente) din țara terță; (ii) o „organizație internațională relevantă", de exemplu un organism internațional care îndeplinește funcții corespunzătoare oricăruia dintre scopurile de asigurare a respectării legii; sau (iii) o persoană, alta decât o autoritate relevantă, dar numai în cazul în care transferul este strict necesar pentru îndeplinirea unuia dintre scopurile de asigurare a respectării legii; niciunul dintre drepturile și libertățile fundamentale ale persoanei vizate în cauză nu prevalează în fața interesului public care necesită transferul; transferul datelor cu caracter personal către o autoritate relevantă din țara terță ar fi ineficient sau inadecvat; iar destinatarul este informat cu privire la scopurile în care datele pot fi prelucrate ([140]).

(76) Secretarul de stat adoptă reglementări privind caracterul adecvat al nivelului de protecție în ceea ce privește o țară terță, un teritoriu sau un sector dintr-o țară terță, o organizație internațională sau o descriere ([141]) a țării, teritoriului, sectorului sau organizației respective. În ceea ce privește standardul care trebuie îndeplinit, secretarul de stat trebuie să evalueze dacă un astfel de teritoriu/sector sau o astfel de organizație asigură un nivel adecvat de protecție a datelor cu caracter personal. Secțiunea 74A punctul 4 din DPA din 2018 prevede că, în acest scop, secretarul de stat trebuie să ia în considerare o serie de elemente care le reflectă pe cele enumerate la articolul 36 din Directiva (UE) 2016/680 ([142]). În acest sens, de la încheierea perioadei de tranziție, partea 3 din DPA din 2018 constituie „legislație națională derivată din dreptul Uniunii" care, astfel cum s-a explicat, va fi interpretată de instanțele din Regatul Unit în conformitate cu jurisprudența relevantă a Curții de Justiție din perioada anterioară ieșirii Regatului Unit din Uniune și cu principiile generale ale dreptului Uniunii, întrucât acestea au produs efecte imediat înainte de încheierea perioadei de tranziție. Aceasta include standardul „echivalenței esențiale" care se va aplica, prin urmare, evaluărilor privind caracterul adecvat al nivelului de protecție efectuate de autoritățile Regatului Unit.

(77) În ceea ce privește procedura, regulamentele fac obiectul cerințelor de procedură „generale" prevăzute în secțiunea 182 din DPA din 2018. În cadrul acestei proceduri, secretarul de stat trebuie să consulte comisarul pentru informații atunci când propune elaborarea unor viitoare regulamente ale Regatului Unit privind caracterul adecvat al

([139]) Acest nou cadru a devenit aplicabil la sfârșitul perioadei de tranziție, inclusiv competența secretarului de stat de a adopta regulamente privind caracterul adecvat al nivelului de protecție. Cu toate acestea, regulamentele DPPEC (în special punctele 10-12 din anexa 21 introduse prin aceste regulamente la DPA din 2018) prevăd că anumite transferuri de date cu caracter personal la sfârșitul perioadei de tranziție sau ulterior sunt tratate ca și cum s-ar baza pe regulamente privind caracterul adecvat al nivelului de protecție. Aceste transferuri includ transferurile către țări terțe care fac obiectul unei decizii UE privind caracterul adecvat al nivelului de protecție la sfârșitul perioadei de tranziție și către statele membre ale UE, statele AELS și teritoriul Gibraltarului în temeiul aplicării Directivei privind protecția datelor în materie de asigurare a respectării legii în cazul prelucrării datelor în scopul asigurării respectării legii [statele AELS aplică Directiva (UE) 2016/680 ca urmare a obligațiilor ce le revin în temeiul acquis-ului Schengen]. Aceasta înseamnă că, la sfârșitul perioadei de tranziție, transferurile către aceste țări pot continua ca înainte de ieșirea din UE. După încheierea perioadei de tranziție, secretarul de stat trebuie să efectueze o revizuire a constatărilor privind caracterul adecvat al nivelului de protecție în termen de patru ani.

([140]) Secțiunile 73 și 77 din DPA din 2018.

([141]) Autoritățile Regatului Unit au explicat că descrierea unei țări sau a unei organizații internaționale se referă la o situație în care ar fi necesar să se efectueze o determinare specifică și parțială a caracterului adecvat cu restricții specifice (de exemplu, regulamente privind caracterul adecvat al nivelului de protecție în ceea ce privește numai anumite tipuri de transferuri de date).

([142]) A se vedea secțiunea 74A punctul 4 din DPA din 2018, care prevede că, atunci când evaluează caracterul adecvat al nivelului de protecție, „secretarul de stat trebuie, în special, să țină seama de (a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, normele de protecție a datelor, normele profesionale și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor căi de atac administrative și judiciare eficace pentru persoanele vizate ale căror date cu caracter personal sunt transferate; (b) existența și funcționarea eficientă a uneia sau mai multor autorități de supraveghere independente în țara terță sau sub jurisdicția cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de asigurare a respectării aplicării, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu comisarul și (c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente obligatorii din punct de vedere juridic, precum și din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal".

nivelului de protecție ([143]). Odată adoptate de secretarul de stat, aceste regulamente sunt prezentate Parlamentului și fac obiectul procedurii de „rezoluție negativă", în cadrul căreia ambele camere ale Parlamentului pot examina regulamentul și pot adopta o propunere de anulare a regulamentului în termen de 40 de zile ([144]).

(78) În conformitate cu secțiunea 74B punctul 1 din DPA din 2018, regulamentele privind caracterul adecvat al nivelului de protecție trebuie revizuite la intervale de cel mult patru ani, iar secretarul de stat trebuie să monitorizeze în permanență evoluțiile din țările terțe și la nivelul organizațiilor internaționale, care ar putea afecta deciziile de adoptare a unor regulamente privind caracterul adecvat al nivelului de protecție sau de modificare sau de revocare a unor astfel de regulamente. În cazul în care secretarul de stat constată că o anumită țară sau organizație nu mai asigură un nivel adecvat de protecție a datelor cu caracter personal, acesta trebuie, în măsura în care este necesar, să modifice sau să revoce regulamentele și să inițieze consultări cu țara terță sau cu organizația internațională în cauză pentru a remedia lipsa unui nivel adecvat de protecție.

(79) În mod similar cu prevederile articolului 37 din Directiva (UE) 2016/680, în absența unui regulament privind caracterul adecvat al nivelului de protecție, un transfer de date cu caracter personal în contextul sectorului asigurării respectării legii ar fi posibil atunci când sunt instituite garanții adecvate. Aceste garanții sunt asigurate fie prin (a) un act juridic obligatoriu care conține garanții adecvate pentru protecția datelor cu caracter personal, fie prin (b) o evaluare efectuată de operator care, după evaluarea tuturor circumstanțelor legate de transfer, concluzionează că există garanții adecvate pentru protecția datelor ([145]). În plus, atunci când transferurile se bazează pe garanții adecvate, DPA din 2018 prevede că, pe lângă rolul normal de supraveghere al ICO, autoritățile competente trebuie să furnizeze informații specifice cu privire la transferurile către ICO ([146]).

(80) În cazul în care un transfer nu se bazează pe o decizie privind caracterul adecvat al nivelului de protecție sau pe garanții adecvate, acesta poate avea loc numai în anumite circumstanțe specificate, denumite „circumstanțe speciale" ([147]). Acest lucru este valabil atunci când transferul este necesar: (a) pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane; (b) pentru protejarea intereselor legitime ale persoanei vizate; (c) pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unei țări terțe; (d) în cazuri individuale, în oricare dintre scopurile de asigurare a respectării legii; sau (e) în cazuri individuale, în scopuri juridice (de exemplu, în legătură cu proceduri judiciare sau pentru obținerea de consultanță juridică) ([148]). Se poate observa că literele (d) și (e) nu se aplică dacă drepturile și libertățile persoanei vizate prevalează asupra interesului public în ceea ce privește transferul ([149]). Acest set de circumstanțe corespunde situațiilor și condițiilor specifice care se califică drept „derogări" în temeiul articolului 38 din Directiva (UE) 2016/680.

(81) În aceste condiții, data, ora și motivul transferului, numele și orice altă informație pertinentă cu privire la destinatar, precum și o descriere a datelor cu caracter personal transferate trebuie să fie documentate și furnizate, la cerere, comisarului pentru informații ([150]).

(82) Secțiunea 78 din DPA din 2018 reglementează scenariul „transferurilor ulterioare", și anume atunci când datele cu caracter personal care au fost transferate din Regatul Unit către o țară terță sunt transferate ulterior către o altă țară terță sau către o organizație internațională. În conformitate cu secțiunea 78 punctul 1, operatorul care efectuează transferul din Regatul Unit trebuie să impună în cadrul transferului o condiție ca datele să nu fie transferate ulterior către o țară terță fără autorizarea operatorului care efectuează transferul. În plus, în conformitate cu secțiunea 78 punctul 3 și în mod similar cu ceea ce se prevede la articolul 35 alineatul (1) litera (e) din Directiva (UE) 2016/680, în cazul în care o astfel de autorizație este necesară, se aplică o serie de cerințe de fond. Mai precis, atunci când decide dacă să autorizeze sau nu transferul, o autoritate competentă trebuie să se asigure că transferul ulterior este

([143]) A se vedea Memorandumul de înțelegere dintre secretarul de stat al Ministerului pentru Digitalizare, Cultură, Mass-Media și Sport și Biroul comisarului pentru informații privind rolul ICO în legătură cu noua evaluare privind caracterul adecvat al nivelului de protecție din Regatul Unit, disponibil la următoarea adresă: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments

([144]) În acest termen de 40 de zile, ambele camere ale Parlamentului pot avea posibilitatea, dacă doresc, să voteze împotriva regulamentelor; în cazul în care se adoptă un astfel de vot, regulamentele vor înceta, în cele din urmă, să mai producă efecte juridice.

([145]) Secțiunea 75 din DPA din 2018.

([146]) În conformitate cu secțiunea 75 punctul 3 din DPA din 2018, în cazul în care are loc un transfer de date pe baza unor garanții adecvate: (a) transferul trebuie să fie documentat, (b) documentația trebuie furnizată comisarului la cerere și (c) documentația trebuie să includă, în special, (i) data și ora transferului, (ii) numele și orice alte informații pertinente cu privire la destinatar, (iii) justificarea transferului și (iv) o descriere a datelor cu caracter personal transferate.

([147]) Ghid privind prelucrarea datelor în scopul asigurării respectării legii, „Există circumstanțe speciale?", disponibil la următoarea adresă: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3

([148]) Secțiunea 76 din DPA din 2018.

([149]) Secțiunea 76 din DPA din 2018.

([150]) Secțiunea 76 punctul 3 din DPA din 2018.

necesar în scopul asigurării respectării legii și ar trebui să ia în considerare, printre alți factori, (a) gravitatea circumstanțelor care au condus la cererea de autorizare, (b) scopul pentru care datele cu caracter personal au fost transferate inițial și (c) standardele de protecție a datelor cu caracter personal care se aplică în țara terță sau în organizația internațională către care ar urma să fie transferate datele cu caracter personal.

(83) În plus, atunci când persoana vizată de un transfer ulterior din Regatul Unit a fost inițial transferată din Uniunea Europeană, se aplică garanții suplimentare.

(84) În primul rând, secțiunea 73 punctul 1 litera (b) din DPA din 2018 prevede – în mod similar cu articolul 35 alineatul (1) litera (c) din Directiva (UE) 2016/680 – că, în cazul în care datele cu caracter personal au fost transmise inițial sau puse în alt mod la dispoziția operatorului sau a unei alte autorități competente de către un stat membru, acel stat membru sau orice persoană cu sediul în statul membru respectiv care este o autoritate competentă în sensul Directivei (UE) 2016/680 trebuie să fi autorizat transferul în conformitate cu legislația statului membru.

(85) Cu toate acestea, în mod similar cu articolul 35 alineatul (2) din Directiva (UE) 2016/680, o astfel de autorizare nu este obligatorie atunci când (a) transferul este necesar pentru prevenirea unei amenințări imediate și grave la adresa securității publice a unui stat membru sau a unei țări terțe sau a intereselor fundamentale ale unui stat membru, iar (b) autorizarea nu poate fi obținută în timp util. În acest caz, autoritatea din statul membru care ar fi fost responsabilă de decizia de autorizare a transferului trebuie informată fără întârziere ([151]).

(86) În al doilea rând, aceeași abordare se aplică în cazul datelor transferate inițial din Uniunea Europeană către Regatul Unit, apoi transferate ulterior de Regatul Unit către o țară terță care le-ar transfera ulterior unei alte țări terțe. În acest caz, în conformitate cu secțiunea 78 punctul 4, autoritatea competentă din Regatul Unit nu poate autoriza acest din urmă transfer, în temeiul articolului 78 alineatul (1), cu excepția cazului în care „statul membru [care a transferat inițial datele în cauză] sau orice persoană cu sediul în statul membru respectiv care este o autoritate competentă în sensul Directivei privind protecția datelor în materie de asigurare a respectării legii a autorizat transferul în conformitate cu dreptul statului membru". Aceste garanții sunt importante, deoarece permit autorităților statelor membre să asigure continuitatea protecției, în conformitate cu legislația UE privind protecția datelor, de-a lungul „lanțului de transfer".

(87) Acest nou cadru pentru transferurile internaționale a devenit aplicabil la sfârșitul perioadei de tranziție ([152]). Cu toate acestea, punctele 10-12 din anexa 21 (introduse prin regulamentele DPPC) prevăd că, la sfârșitul perioadei de tranziție, anumite transferuri de date cu caracter personal sunt tratate ca și cum s-ar baza pe regulamente privind caracterul adecvat al nivelului de protecție. Aceste transferuri includ transferurile către un stat membru, un stat AELS, o țară terță care face obiectul unei decizii a UE privind caracterul adecvat al nivelului de protecție la încheierea perioadei de tranziție, precum și teritoriul Gibraltarului. În consecință, transferurile către aceste țări pot continua la fel ca înainte de retragerea Regatului Unit din Uniune. După încheierea perioadei de tranziție, secretarul de stat trebuie să efectueze o revizuire a acestor constatări privind caracterul adecvat al nivelului de protecție pe o perioadă de patru ani, și anume până la sfârșitul lunii decembrie 2024. Potrivit explicației furnizate de autoritățile Regatului Unit, deși secretarul de stat trebuie să efectueze o astfel de revizuire până la sfârșitul lunii decembrie 2024, dispozițiile tranzitorii nu includ o dispoziție de caducitate, iar dispozițiile tranzitorii relevante nu vor înceta în mod automat să producă efecte dacă revizuirea nu este finalizată până la sfârșitul lunii decembrie 2024.

2.4.9. *Responsabilitate*

(88) Conform principiului responsabilității, autorităților publice care prelucrează date li se solicită să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a-și respecta în mod efectiv obligațiile în materie de protecție a datelor și pentru a putea demonstra această conformitate, în special autorității de supraveghere competente.

(89) Acest principiu este reflectat în secțiunea 56 din DPA din 2018, care introduce o obligație generală de responsabilitate pentru operator, și anume obligația de a pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura și a fi în măsură să demonstreze că prelucrarea datelor cu caracter personal respectă cerințele părții 3 din DPA din 2018. Măsurile puse în aplicare trebuie să fie revizuite și actualizate atunci când este necesar și, în cazul în care sunt proporționale în materie de prelucrare, trebuie să includă politici adecvate de protecție a datelor.

([151]) Secțiunea 73 punctul 5 din DPA din 2018.

([152]) Aplicabilitatea acestui nou cadru trebuie interpretată în lumina articolului 782 din Acordul comercial și de cooperare între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice, pe de o parte, și Regatul Unit al Marii Britanii și Irlandei de Nord, pe de altă parte (JO L 444 din 31.12.2020, p. 14) („TCA UE-UK"), disponibil la următoarea adresă: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22020A1231(01)&from=RO

(90) În conformitate cu capitolul IV din Directiva (UE) 2016/680, secțiunile 55-71 din DPA din 2018 prevăd diferite mecanisme pentru a asigura responsabilitatea și pentru a permite operatorilor și persoanelor împuternicite de operatori să demonstreze conformitatea. În special, operatorii au obligația de a pune în aplicare măsuri de protecție a datelor începând cu momentul conceperii și în mod implicit, și anume de a se asigura că principiile privind protecția datelor sunt puse în aplicare în mod eficient și au obligația de a menține o evidență a tuturor categoriilor de activități de prelucrare aflate în responsabilitatea operatorului (inclusiv informații privind identitatea operatorului, datele de contact ale responsabilului cu protecția datelor, scopurile prelucrării, categoriile de destinatari ai divulgărilor și o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal), precum și de a păstra aceste evidențe la dispoziția comisarului pentru informații, la cerere. Operatorul și persoana împuternicită de operator trebuie, de asemenea, să înregistreze anumite operațiuni de prelucrare și să pună înregistrările la dispoziția comisarului pentru informații ([153]). De asemenea, operatorii au obligația specifică de a coopera cu comisarul pentru informații în vederea îndeplinirii sarcinilor acestuia.

(91) De asemenea, DPA din 2018 stabilește cerințe suplimentare privind prelucrarea, care este posibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. Printre acestea se numără obligația de a efectua evaluări ale impactului asupra protecției datelor și de a consulta comisarul pentru informații înainte de prelucrare, în cazul în care o astfel de evaluare indică faptul că prelucrarea ar genera un risc ridicat la adresa drepturilor și libertăților persoanelor fizice (în absența unor măsuri de atenuare a riscului).

(92) În plus, operatorii trebuie să numească un responsabil cu protecția datelor, cu excepția cazului în care operatorul este o instanță judecătorească sau o altă autoritate judiciară, care acționează în exercițiul funcției sale judiciare ([154]). Operatorul trebuie să se asigure că responsabilul cu protecția datelor este implicat în toate aspectele legate de protecția datelor cu caracter personal, are resursele necesare și are acces la datele cu caracter personal și la operațiunile de prelucrare și își poate îndeplini sarcinile în mod independent. Sarcinile responsabilului cu protecția datelor sunt prevăzute în secțiunea 71 din DPA din 2018, inclusiv furnizarea de informații și consiliere, monitorizarea conformității, precum și cooperarea cu comisarul pentru informații și îndeplinirea rolului de punct de contact al acestuia. În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor trebuie să țină seama de riscurile asociate operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

2.5. **Supraveghere și asigurarea respectării normelor**

2.5.1. *Supravegherea independentă*

(93) Pentru a garanta și în practică un nivel adecvat de protecție a datelor, trebuie instituită o autoritate de supraveghere independentă care să aibă competența de a monitoriza și de a asigura respectarea normelor de protecție a datelor. Această autoritate trebuie să acționeze cu deplină independență și imparțialitate în îndeplinirea sarcinilor sale și în exercitarea competențelor sale.

(94) În Regatul Unit, supravegherea și asigurarea respectării RGPD al Regatului Unit și a DPA din 2018 sunt efectuate de comisarul pentru informații ([155]). De asemenea, comisarul pentru informații supraveghează prelucrarea datelor cu caracter personal de către autoritățile competente care intră sub incidența părții 3 din DPA din 2018 ([156]). Comisarul pentru informații este o „întreprindere individuală” (Corporation Sole): o entitate juridică separată constituită dintr-o singură persoană. Comisarul pentru informații este sprijinit în activitatea sa de un birou. La 31 martie 2020, Biroul comisarului pentru informații avea 768 de angajați permanenți ([157]). Ministerul finanțator al comisarului pentru informații este Ministerul pentru Digitalizare, Cultură, Mass-Media și Sport ([158]).

([153]) Secțiunea 62 din DPA din 2018.
([154]) Secțiunea 69 din DPA din 2018.
([155]) Articolul 36 alineatul (2) litera (b) din Directiva (UE) 2016/680.
([156]) Secțiunea 116 din DPA din 2018.
([157]) Raportul anual și situațiile financiare pe 2019-2020 ale comisarului pentru informații, disponibile la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf
([158]) Un acord de gestionare reglementează relația dintre cele două entități. Responsabilitățile principale ale DCMS, în calitate de minister finanțator, includ în special: asigurarea faptului că ICO beneficiază de finanțare și de resurse adecvate; reprezentarea intereselor ICO în fața Parlamentului și a altor departamente guvernamentale; asigurarea existenței unui cadru național solid de protecție a datelor; și furnizarea de orientări și sprijin ICO cu privire la aspecte legate de întreprinderi, cum ar fi aspecte imobiliare, contracte de leasing și achiziții publice (Acordul de gestionare 2018-2021, disponibil la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Independența comisarului este stabilită în mod explicit la articolul 52 din RGPD al Regatului Unit, care reflectă cerințele prevăzute la articolul 52 alineatele (1)-(3) din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([159]). Comisarul trebuie să beneficieze de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu RGPD al Regatului Unit, să rămână independent de orice influență externă directă sau indirectă în legătură cu aceste sarcini și competențe și să nu solicite, nici să nu accepte instrucțiuni de la o parte externă. De asemenea, comisarul trebuie să se abțină de la a întreprinde acțiuni incompatibile cu atribuțiile sale, iar pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

(96) Condițiile pentru numirea și revocarea comisarului pentru informații sunt prevăzute în anexa 12 la DPA din 2018. Comisarul pentru informații este numit de Regină la recomandarea Guvernului, în urma unui concurs general echitabil. Candidatul trebuie să dețină calificările, aptitudinile și competențele corespunzătoare. În conformitate cu Codul de guvernanță privind numirile publice ([160]), o listă de candidați care pot fi numiți este întocmită de un comitet consultativ de evaluare. Înainte ca secretarul de stat din cadrul Ministerului pentru Digitalizare, Cultură, Mass-Media și Sport să ia o decizie finală, comisia specială competentă din cadrul Parlamentului trebuie să efectueze un control prealabil numirii. Poziția Comitetului este făcută publică ([161]).

(97) Comisarul pentru informații are un mandat de până la șapte ani. Comisarul pentru informații poate fi revocat din funcție de Majestatea Sa în urma unei propuneri („address") formulate de ambele camere ale Parlamentului ([162]). Nicio cerere de revocare a comisarului pentru informații nu poate fi prezentată niciunei camere a Parlamentului decât în cazul în care un ministru a prezentat un raport camerei respective în care afirmă că este convins că comisarul pentru informații este vinovat de comiterea unei abateri grave și/sau comisarul nu mai îndeplinește condițiile necesare pentru exercitarea funcțiilor sale ([163]).

(98) Finanțarea comisarului pentru informații provine din trei surse: (i) taxele pentru protecția datelor plătite de operatori, care sunt stabilite prin regulamentele secretarului de stat ([164]) și se ridică la 85-90 % din bugetul anual al Biroului ([165]); (ii) grantul sub formă de ajutor care poate fi plătit de guvern comisarului pentru informații și este utilizat în principal pentru finanțarea cheltuielilor de funcționare ale comisarului pentru informații în ceea ce privește sarcinile care nu au legătură cu protecția datelor ([166]) și (iii) taxele percepute pentru servicii ([167]). În prezent, nu se percep astfel de taxe.

(99) Funcțiile generale ale comisarului pentru informații în ceea ce privește prelucrarea datelor cu caracter personal care intră sub incidența părții 3 din DPA din 2018 sunt prevăzute în anexa 13 la DPA din 2018. Sarcinile includ monitorizarea și punerea în aplicare a părții 3 din DPA din 2018, promovarea sensibilizării publicului, consilierea Parlamentului, a guvernului și a altor instituții cu privire la măsurile legislative și administrative, promovarea sensibilizării operatorilor și a persoanelor împuternicite de operatori cu privire la obligațiile ce le revin, furnizarea de informații unei persoane vizate cu privire la exercitarea drepturilor persoanei vizate și desfășurarea de anchete.

([159]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([160]) Codul de guvernanță privind numirile publice, disponibil la următoarea adresă: https://www.gov.uk/government/publications/governance-code-for-public-appointments

([161]) Al doilea raport al sesiunii 2015-2016 a Comisiei pentru cultură, mass-media și sport a Camerei Comunelor, disponibil la următoarea adresă:https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([162]) „Address" este o propunere prezentată Parlamentului prin care se urmărește informarea monarhului cu privire la opiniile Parlamentului referitoare la o anumită chestiune.

([163]) Punctul 3 din anexa 12 la DPA din 2018.

([164]) Secțiunea 137 din DPA din 2018.

([165]) Secțiunile 137 și 138 din DPA din 2018 conțin o serie de garanții pentru a se asigura că taxele sunt stabilite la un nivel corespunzător. În special secțiunea 137 punctul 4 din DPA din 2018 enumeră aspectele pe care secretarul de stat trebuie să le ia în considerare atunci când elaborează regulamente care precizează suma pe care trebuie să o plătească diferitele organizații. Secțiunea 138 punctul 1 și secțiunea 182 din DPA din 2018 conțin, de asemenea, o cerință legală potrivit căreia secretarul de stat trebuie să se consulte cu comisarul pentru informații și cu alți reprezentanți ai persoanelor care pot fi afectate de regulamentele în cauză, înainte ca acestea să fie adoptate, astfel încât opiniile lor să poată fi luate în considerare. În plus, în temeiul secțiunii 138 punctul 2 din DPA din 2018, comisarul pentru informații are obligația de a monitoriza funcționarea regulamentelor privind taxele și poate prezenta secretarului de stat propuneri de modificare a regulamentelor. În cele din urmă, cu excepția cazului în care regulamentele sunt adoptate doar pentru a lua în considerare o creștere a indicelui prețurilor cu amănuntul (caz în care vor face obiectul procedurii de rezoluție negativă), regulamentele fac obiectul procedurii de rezoluție afirmativă și nu pot fi adoptate decât după ce au fost aprobate prin rezoluția fiecărei camere a Parlamentului.

([166]) Acordul de gestionare a clarificat următoarele: „Secretarul de stat poate efectua plăți către CI din banii furnizați de Parlament în temeiul punctului 9 din anexa 12 la DPA din 2018. După consultarea CI, DCMS va plăti către CI sumele corespunzătoare (grantul sub formă de ajutor) pentru costurile administrative ale ICO și pentru exercitarea funcțiilor CI în legătură cu o serie de funcții specifice, inclusiv libertatea de informare" (Acordul de gestionare 2018-2021, punctul 1.12, a se vedea nota de subsol 158).

([167]) Secțiunea 134 din DPA din 2018.

Pentru a menține independența sistemului judiciar, comisarul pentru informații nu este autorizat să își exercite funcțiile în legătură cu prelucrarea datelor cu caracter personal de către o persoană care acționează în exercițiul unei funcții judiciare sau de către o instanță sau tribunal care acționează în exercițiul funcției sale judiciare. Cu toate acestea, supravegherea sistemului judiciar este asigurată de organisme specializate, abordate în continuare.

2.5.1.1 Asigurarea respectării normelor, inclusiv sancțiuni

(100) Comisarul are competențe generale de investigare, de corecție, de autorizare și de consiliere în ceea ce privește prelucrarea datelor cu caracter personal cărora li se aplică partea 3 din DPA din 2018. Comisarul are competența de a notifica operatorul sau persoana împuternicită de operator cu privire la o presupusă încălcare a părții 3, de a emite avertismente în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile părții 3, precum și de a emite mustrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile părții 3. În plus, din proprie inițiativă sau la cerere, comisarul poate emite avize adresate Parlamentului Regatului Unit, guvernului sau altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal ([168]).

(101) În plus, comisarul are competența de:

— a ordona operatorului și persoanei împuternicite de operator (și, în anumite circumstanțe, oricărei alte persoane) să furnizeze informațiile necesare prin transmiterea unei notificări de informare („notificare de informare") ([169]);

— a efectua investigații și audituri prin transmiterea unei notificări de evaluare, care poate impune operatorului sau persoanei împuternicite de operator să permită comisarului să intre în incinte specificate, să inspecteze sau să examineze documente sau echipamente, să intervieveze persoane care prelucrează date cu caracter personal în numele operatorului („notificare de evaluare") ([170]);

— a obține în alt mod acces la documente ale operatorilor și ale persoanelor împuternicite de operatori și acces la sediile acestora în conformitate cu secțiunea 154 din DPA din 2018 („competențe de intrare și de inspecție");

— a exercita competențe corective, inclusiv prin avertismente și mustrări sau a emite ordine prin intermediul unei notificări de executare, care impune operatorilor/persoanelor împuternicite de operatori să întreprindă sau să se abțină de la a întreprinde anumite măsuri („notificare de executare") ([171]); precum și

— a emite amenzi administrative sub forma unei notificări de sancționare („notificare de sancționare") ([172]).

(102) Politica ICO privind acțiunile de reglementare stabilește circumstanțele în care comisarul va emite o notificare de informare, de evaluare, de executare și, respectiv, de sancționare ([173]). O notificare de executare poate impune cerințe pe care comisarul le consideră adecvate în scopul remedierii neîndeplinirii obligațiilor. O notificare de sancționare impune persoanei în cauză să plătească comisarului pentru informații o sumă specificată în notificare. O notificare de sancționare poate fi transmisă în cazul nerespectării anumitor dispoziții ale DPA din 2018 ([174]) sau poate fi transmisă unui operator sau unei persoane împuternicite de operator care nu a respectat o notificare de informare, o notificare de evaluare sau o notificare de executare.

(103) Mai precis, atunci când stabilește dacă să transmită o notificare de sancționare unui operator sau unei persoane împuternicite de operator și cuantumul sancțiunii, comisarul pentru informații trebuie să aibă în vedere aspectele enumerate în secțiunea 155 punctul 3 din DPA din 2018, inclusiv natura și gravitatea situației de nerespectare, caracterul intenționat sau neglijent al nerespectării, orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciile suferite de persoanele vizate, gradul de responsabilitate al

([168]) Punctul 2 din anexa 13 la DPA din 2018.
([169]) Secțiunea 142 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 143 din DPA din 2018).
([170]) Secțiunea 146 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 147 din DPA din 2018).
([171]) Secțiunile 149-151 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 152 din DPA din 2018).
([172]) Secțiunea 155 din DPA din 2018 (sub rezerva restricțiilor prevăzute în secțiunea 156 din DPA din 2018).
([173]) Politica privind acțiunile de reglementare, disponibilă la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([174]) În special, ICO poate emite o notificare de sancționare în cazul nerespectării cerințelor prevăzute în secțiunea 149 punctele 2, 3, 4 sau 5 din DPA din 2018.

operatorului sau al persoanei împuternicite de operator (ținându-se seama de măsurile tehnice și organizatorice puse în aplicare de operator sau de persoana împuternicită de operator), eventuale încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator; categoriile de date cu caracter personal afectate de situația de nerespectare și dacă sancțiunea ar fi eficace, proporțională și disuasivă.

(104) Cuantumul maxim al sancțiunii care poate fi impusă printr-o notificare de sancționare este de (a) 17 500 000 GBP pentru nerespectarea principiilor privind protecția datelor (secțiunile 35, 36, 37, secțiunea 38 punctul 1, secțiunea 39 punctul 1 și secțiunea 40 din DPA din 2018), a obligațiilor de transparență și a drepturilor individuale (secțiunile 44, 45, 46, 47, 48, 49, 52 și 53 din DPA din 2018) și a principiilor privind transferurile internaționale de date cu caracter personal (secțiunile 73, 75, 76, 77 sau 78 din DPA din 2018); și (b) 8 700 000 GBP în caz contrar ([175]). În cazul nerespectării unei notificări de informare, a unei notificări de evaluare sau a unei notificări de executare, cuantumul maxim al sancțiunii care poate fi impusă printr-o notificare de sancționare este de 17 500 000 GBP.

(105) Conform ultimelor sale rapoarte anuale [2018-2019 ([176]), 2019-2020 ([177])], comisarul pentru informații a efectuat o serie de investigații în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile de asigurare a respectării dreptului penal. De exemplu, comisarul a efectuat o investigație și a publicat un aviz în octombrie 2019 în ceea ce privește utilizarea de către autoritățile de aplicare a legii a tehnologiei de recunoaștere facială în locuri publice. Investigația s-a axat cu precădere pe utilizarea capacităților de recunoaștere facială în direct de către poliția din sudul Țării Galilor și de către Serviciul de poliție metropolitană (MPS). În plus, comisarul a investigat „matricea Gangs" ([178]) a MPS și a constatat o serie de încălcări grave ale legislației privind protecția datelor, care erau de natură să submineze încrederea publicului în matrice și în utilizarea datelor.

(106) În noiembrie 2018, comisarul pentru informații a emis o notificare de executare, iar ulterior MPS a luat măsurile necesare pentru a spori securitatea și responsabilitatea și pentru a se asigura că datele sunt utilizate în mod proporțional.

(107) Un alt exemplu de acțiune recentă de asigurare a respectării legii este amenda de 325 000 GBP aplicată ministerului public de către comisar în luna mai 2018, pentru pierderea unor DVD-uri necriptate care conțineau înregistrări ale interogatoriilor efectuate de poliție. Pe lângă acestea, comisarul pentru informații a desfășurat investigații cu privire la subiecte mai ample, de exemplu în prima jumătate a anului 2020, cu privire la utilizarea criminalisticii mobile în scopuri polițienești și la prelucrarea datelor victimelor de către poliție.

(108) Pe lângă competențele comisarului pentru informații în materie de asigurare a respectării legii, anumite încălcări ale legislației privind protecția datelor constituie infracțiuni și, prin urmare, pot face obiectul unor sancțiuni penale (secțiunea 196 din DPA din 2018). Acest lucru se aplică, de exemplu, obținerii sau divulgării datelor cu caracter personal fără consimțământul operatorului și permiterii divulgării datelor cu caracter personal unei alte persoane fără consimțământul operatorului ([179]); reidentificării informațiilor care sunt date cu caracter personal anonimizate fără consimțământul operatorului responsabil de anonimizarea datelor cu caracter personal ([180]); împiedicării intenționate a comisarului de a-și exercita competențele în ceea ce privește examinarea datelor cu caracter personal în conformitate cu obligațiile internaționale ([181]), prezentării de declarații false ca răspuns la o notificare de informare sau distrugerii informațiilor în legătură cu notificările de informare și de evaluare ([182]).

(109) În temeiul secțiunii 139 din DPA din 2018, comisarul pentru informații are, de asemenea, obligația de a prezenta în fața fiecărei camere a Parlamentului un raport general privind exercitarea funcțiilor sale în temeiul legii ([183]).

([175]) Secțiunea 157 din DPA din 2018.

([176]) Raportul anual și situațiile financiare pe 2018-2019 ale comisarului pentru informații, disponibile la următoarea adresă: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) Raportul anual pe 2019-2020 al comisarului pentru informații (a se vedea nota de subsol 157).

([178]) O bază de date care a înregistrat informații referitoare la presupușii membri ai unor grupări criminale și la victimele infracțiunilor săvârșite de grupări criminale.

([179]) Secțiunea 170 din DPA din 2018.

([180]) Secțiunea 171 din DPA din 2018.

([181]) Secțiunea 119 din DPA din 2018.

([182]) Secțiunile 144 și 148 din DPA din 2018.

([183]) Astfel cum se prevede în acordul de gestionare, raportul anual trebuie: (i) să vizeze orice întreprindere, filială sau asociere în participație aflată sub controlul ICO; (ii) să respecte Manualul de raportare financiară al Trezoreriei (FReM); (iii) să conțină o declarație privind guvernanța, care să stabilească modul în care contabilul a gestionat și a controlat resursele utilizate în cadrul organizației în cursul anului, demonstrând capacitatea organizației de a gestiona riscurile pentru îndeplinirea scopurilor și obiectivelor sale; și (iv) să prezinte principalele activități și performanțe din cursul exercițiului financiar precedent și să expună planurile previzionale sub formă de rezumat (Acordul de gestionare 2018-2021, punctul 3.26, a se vedea nota de subsol 158).

2.5.2. *Supravegherea sistemului judiciar*

(110) Supravegherea prelucrării datelor cu caracter personal de către instanțe și sistemul judiciar este dublă. În cazul în care un titular al unei funcții judiciare sau o instanță nu acționează în exercițiul unei funcții judiciare, supravegherea este asigurată de comisarul pentru informații. În cazul în care operatorul își desfășoară activitatea în exercițiul unei funcții judiciare, ICO nu își poate exercita funcțiile de supraveghere ([184]), iar supravegherea este efectuată de organisme speciale. Aceasta reflectă abordarea adoptată la articolul 32 din Directiva (UE) 2016/680.

(111) În special, în cel de al doilea scenariu, pentru instanțele din Anglia și Țara Galilor, precum și pentru Tribunalul de Primă Instanță și Tribunalul Superior din Anglia și Țara Galilor, această supraveghere este asigurată de Grupul pentru protecția datelor judiciare ([185]). În plus, președintele Curții Supreme (Lord Chief Justice) și președintele sistemului de tribunale (Senior President of Tribunals) au emis o declarație de confidențialitate ([186]) care stabilește modul în care instanțele din Anglia și Țara Galilor prelucrează datele cu caracter personal pentru o funcție judiciară. O declarație similară a fost emisă de autoritățile judiciare din Irlanda de Nord ([187]) și de cele din Scoția ([188]).

(112) În plus, în Irlanda de Nord, președintele Curții Supreme din Irlanda de Nord a numit un judecător din cadrul Înaltei Curți în calitate de judecător în materie de supraveghere a datelor (DSJ – Data Supervisory Judge) ([189]). Aceștia au emis, de asemenea, orientări pentru sistemul judiciar din Irlanda de Nord cu privire la acțiunile care trebuie întreprinse în cazul unei pierderi sau potențiale pierderi de date și la procesul de abordare a oricăror probleme care decurg din acest fapt ([190]).

(113) În Scoția, președintele Curții Supreme (Lord President) a numit un judecător în materie de supraveghere a datelor pentru a investiga orice plângeri pe motive de protecție a datelor. Acest fapt este prevăzut în normele privind plângerile judiciare, care le reflectă pe cele stabilite pentru Anglia și Țara Galilor ([191]).

(114) În cele din urmă, în cadrul Curții Supreme, unul dintre judecătorii Curții Supreme este desemnat să supravegheze protecția datelor.

([184]) Secțiunea 117 din DPA din 2018.

([185]) Grupul este responsabil de furnizarea de orientări și formare pentru sistemul judiciar. Acesta tratează, de asemenea, plângerile persoanelor vizate cu privire la prelucrarea datelor cu caracter personal de către instanțe, tribunale și persoane care acționează în exercițiul unei funcții judiciare. Grupul urmărește să ofere mijloacele prin care orice plângere ar putea fi soluționată. În cazul în care un reclamant nu a fost mulțumit de o decizie a grupului și a furnizat dovezi suplimentare, grupul ar putea să își reexamineze decizia. Deși grupul în sine nu impune sancțiuni financiare, în cazul în care grupul consideră că există o încălcare suficient de gravă a DPA din 2018, acesta o poate adresa Biroului de investigare a conduitei judiciare (JCIO – Judicial Conduct Investigation Office), care va investiga plângerea. În cazul în care plângerea este admisă, este de competența Lordului Cancelar (Lord Chancellor) și a președintelui Curții Supreme (sau a unui judecător de rang înalt delegat să acționeze în numele său) să decidă ce măsuri ar trebui luate împotriva titularului funcției. Acestea ar putea include, în ordinea gravității: recomandare formală, avertisment formal, mustrare și, în cele din urmă, revocare din funcție. În cazul în care o persoană este nemulțumită de modul în care JCIO a investigat plângerea, aceasta poate depune o plângere mai departe la Ombudsmanul pentru numiri și conduită judiciară (Judicial Appointments and Conduct Ombudsman) (a se vedea https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ombudsmanul are competența de a solicita JCIO să investigheze din nou o plângere și poate propune ca reclamantului să i se plătească despăgubiri în cazul în care consideră că a suferit prejudicii ca urmare a administrării defectuoase.

([186]) Declarația de confidențialitate a președintelui Curții Supreme și a președintelui sistemului de tribunale este disponibilă la următoarea adresă: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([187]) Declarația de confidențialitate emisă de președintele Curții Supreme din Irlanda de Nord este disponibilă la următoarea adresă: https://judiciaryni.uk/data-privacy

([188]) Declarația de confidențialitate pentru instanțele și tribunalele din Scoția este disponibilă la următoarea adresă: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([189]) DSJ furnizează îndrumări sistemului judiciar și investighează încălcările și/sau plângerile referitoare la prelucrarea datelor cu caracter personal de către instanțe sau persoane care acționează în exercițiul unei funcții judiciare.

([190]) În cazul în care plângerea sau încălcarea este considerată gravă, aceasta este înaintată responsabilului cu tratarea plângerilor judiciare (Judicial Complaints Officer) pentru investigații suplimentare în conformitate cu Codul de bune practici în materie de plângeri al președintelui Curții Supreme din Irlanda de Nord. Rezultatul unei astfel de plângeri ar putea include următoarele: clasarea plângerii, recomandare, formare sau mentorat, avertisment informal, avertisment formal, avertisment final, restricții de practică sau sesizarea unui tribunal statutar. Codul de bune practici în materie de plângeri emis de președintele Curții Supreme din Irlanda de Nord este disponibil la următoarea adresă: 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]) Orice plângere întemeiată este investigată de judecătorul în materie de supraveghere a datelor și înaintată președintelui Curții Supreme care are competența de a emite o recomandare, un avertisment formal sau o mustrare în cazul în care consideră că este necesar (există norme echivalente pentru membrii tribunalului, disponibile la următoarea adresă: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2)

2.5.3. *Căi de atac*

(115) Pentru a asigura o protecție adecvată și, în special, asigurarea respectării drepturilor individuale, persoanei vizate ar trebui să i se ofere căi de atac administrative și judiciare eficace, inclusiv despăgubiri pentru prejudiciile suferite.

(116) În primul rând, o persoană vizată are dreptul de a depune o plângere la comisarul pentru informații, în cazul în care consideră că, în ceea ce privește datele cu caracter personal care o vizează, există o încălcare a părții 3 din DPA din 2018 ([192]). Astfel cum se descrie în considerentele 100 și 109, comisarul pentru informații are competența de a evalua conformitatea operatorului și a persoanei împuternicite de operator cu DPA din 2018, de a le impune sau de a se abține de la luarea măsurilor necesare în caz de nerespectare și de a impune amenzi.

(117) În al doilea rând, DPA din 2018 prevede dreptul la o cale de atac împotriva comisarului pentru informații. În cazul în care comisarul nu „înregistrează progrese" ([193]) în ceea ce privește o plângere depusă de persoana vizată, reclamantul are acces la o cale de atac judiciară, deoarece acesta se poate adresa unui tribunal de primă instanță ([194]) pentru a obliga comisarul să ia măsurile adecvate pentru a răspunde plângerii sau pentru a informa reclamantul în legătură cu progresele înregistrate cu privire la plângere ([195]). În plus, orice persoană căreia i se transmite oricare dintre notificările de mai sus (notificare de informare, de evaluare, de executare sau de sancționare) din partea comisarului poate introduce o cale de atac în fața unui tribunal de primă instanță. În cazul în care tribunalul consideră că decizia comisarului nu este conformă cu legea sau că, în ceea ce privește comisarul pentru informații, acesta ar fi trebuit să își exercite puterea de apreciere în mod diferit, tribunalul trebuie să admită calea de atac sau să înlocuiască o altă notificare sau decizie pe care comisarul pentru informații ar fi putut să o emită sau să o adopte ([196]).

(118) În al treilea rând, persoanele fizice pot introduce o cale de atac împotriva operatorilor și a persoanelor împuternicite de operatori direct în fața instanțelor în temeiul secțiunii 167 din DPA din 2018. În cazul în care, la cererea unei persoane vizate, o instanță constată că a avut loc o încălcare a drepturilor persoanei vizate în temeiul legislației privind protecția datelor, instanța poate obliga operatorul în ceea ce privește prelucrarea, sau persoana împuternicită de operator care acționează în numele operatorului respectiv, să ia măsurile specificate în ordonanță sau să se abțină de la luarea măsurilor specificate în ordonanță. În plus, în temeiul secțiunii 169 din DPA din 2018, orice persoană care suferă un prejudiciu din cauza unei încălcări a unei cerințe prevăzute de legislația privind protecția datelor (inclusiv partea 3 din DPA din 2018), alta decât RGPD al Regatului Unit, are dreptul la despăgubiri din partea operatorului sau a persoanei împuternicite de operator pentru prejudiciul respectiv, cu excepția cazului în care operatorul sau persoana împuternicită de operator dovedește că operatorul sau persoana împuternicită de operator nu este responsabilă în niciun fel pentru evenimentul care a cauzat prejudiciul. Prejudiciul include atât pierderi financiare, cât și prejudicii care nu implică pierderi financiare, cum ar fi suferințele clinice.

(119) În al patrulea rând, orice persoană care consideră că drepturile sale, inclusiv dreptul la viață privată și la protecția datelor, au fost încălcate de autoritățile publice, poate obține reparații în fața instanțelor din Regatul Unit în temeiul Legii privind drepturile omului din 1998. Operatorii în temeiul părții 3 din DPA din 2018, și anume autoritățile competente, sunt întotdeauna autorități publice în sensul Legii privind drepturile omului din 1998. O persoană care susține că o autoritate publică a acționat (sau propune să acționeze) într-un mod care este incompatibil cu un drept conferit prin convenție și, prin urmare, ilegal în temeiul secțiunii 6 punctul 1 din Legea privind drepturile omului din 1998 poate introduce o acțiune împotriva autorității respective în fața instanței sau a tribunalului competent(e) sau poate invoca drepturile în cauză în cadrul oricărei proceduri judiciare, atunci când este (sau ar fi) victimă a actului ilegal ([197]).

([192]) Secțiunea 165 din DPA din 2018.

([193]) Secțiunea 166 din DPA din 2018 se referă în mod specific la următoarele situații: (a) comisarul nu ia măsurile adecvate pentru a răspunde plângerii, (b) comisarul nu furnizează reclamantului informații cu privire la evoluția plângerii sau la rezultatul acesteia înainte de sfârșitul perioadei de trei luni care începe în momentul în care comisarul a primit plângerea sau (c) în cazul în care examinarea plângerii de către comisar nu este finalizată în perioada respectivă, acesta nu furnizează reclamantului astfel de informații în cursul unei perioade ulterioare de trei luni.

([194]) Tribunalul de Primă Instanță este instanța competentă să soluționeze căile de atac introduse împotriva deciziilor luate de organismele de reglementare guvernamentale. În cazul deciziei comisarului pentru informații, camera competentă este „General Regulatory Chamber", care are jurisdicție asupra întregului teritoriu al Regatului Unit.

([195]) Secțiunea 166 din DPA din 2018.

([196]) Secțiunile 161 și 162 din DPA din 2018.

([197]) A se vedea cauza Brown/Commissioner of the Met 2016, în care instanța a oferit reparații reclamantei în contextul protecției datelor în cadrul unei acțiuni introduse împotriva poliției. Admițând cererile reclamantei de încălcare a obligațiilor prevăzute de DPA din 1998, instanța a constatat în favoarea reclamantei încălcarea HRA din 1998 (și a dreptului conex prevăzut la articolul 8 din CEDO) și fapta ilicită de abuz de informații private (pârâtul a recunoscut, în cele din urmă, că acestea încălcau DPA și CEDO, astfel încât hotărârea s-a concentrat pe căile de atac adecvate). Ca urmare a acestor încălcări, instanța a acordat reclamantei despăgubiri financiare.

(120) În cazul în care constată că un act al unei autorități publice este ilegal, instanța poate admite o astfel de reparație sau cale de atac sau poate dispune, în limitele competențelor sale, după cum consideră corect și adecvat ([198]). De asemenea, instanța poate declara că o dispoziție de drept primar este incompatibilă cu un drept garantat în temeiul CEDO.

(121) În cele din urmă, după epuizarea căilor de atac naționale, o persoană poate obține reparații în fața Curții Europene a Drepturilor Omului pentru încălcarea drepturilor garantate de CEDO.

2.6. **Transferul ulterior**

(122) Legislația Regatului Unit autorizează schimbul de date dintre o autoritate de aplicare a legii și alte autorități ale Regatului Unit în alte scopuri decât cele pentru care au fost colectate inițial (așa-numita „comunicare ulterioară"), sub rezerva anumitor condiții.

(123) În mod similar prevederilor de la articolul 4 alineatul (2) din Directiva (UE) 2016/680, secțiunea 36 punctul 3 din DPA din 2018 permite ca datele cu caracter personal colectate de o autoritate competentă în scopul asigurării respectării legii să poată fi prelucrate în continuare (fie de către operatorul inițial, fie de către un alt operator) în orice alt scop de asigurare a respectării legii, cu condiția ca operatorul să fie autorizat prin lege să prelucreze date în celălalt scop, iar prelucrarea să fie necesară și proporțională ([199]). În acest caz, toate garanțiile prevăzute în partea 3 din DPA din 2018 și analizate mai sus se aplică prelucrării efectuate de autoritatea destinatară.

(124) În ordinea juridică a Regatului Unit, diferite legi permit în mod explicit transferul ulterior. În special, (i) Legea privind economia digitală din 2017 permite schimbul de informații între autoritățile publice în mai multe scopuri, de exemplu în cazul oricărei fraude asupra sectorului public care ar implica pierderi sau un risc de pierdere pentru autoritățile publice ([200]) sau în cazul unei datorii către o autoritate publică sau către Coroană ([201]); (ii) Legea privind criminalitatea și instanțele din 2013, care permite schimbul de informații cu Agenția Națională pentru Combaterea Criminalității (NCA – National Crime Agency) ([202]) pentru combaterea, investigarea și urmărirea penală a infracțiunilor grave și a criminalității organizate; (iii) Legea privind formele grave de criminalitate din 2007, care permite autorităților publice să divulge informații organizațiilor antifraudă în scopul prevenirii fraudei ([203]).

(125) Aceste legi prevăd în mod explicit că schimbul de informații ar trebui să fie în conformitate cu principiile stabilite în DPA din 2018. În plus, Colegiul de Poliție (College of Policing) a emis practici profesionale autorizate privind schimbul de informații (Authorised Professional Practice on Information Sharing) ([204]) pentru a ajuta poliția să își respecte obligațiile în materie de protecție a datelor în temeiul RGPD al Regatului Unit, al DPA și al Legii privind drepturile omului din 1998. Conformitatea schimbului de informații cu cadrul juridic aplicabil în materie de protecție a datelor poate fi, desigur, supusă controlului jurisdicțional ([205]).

(126) În plus, în mod similar prevederilor de la articolul 9 din Directiva (UE) 2016/680, DPA din 2018 prevede că datele cu caracter personal colectate în orice scop de asigurare a respectării legii pot fi prelucrate într-un scop care nu este unul de asigurare a respectării legii atunci când prelucrarea este autorizată prin lege ([206]). Acest tip de schimb de informații se referă la două scenarii: 1) atunci când o autoritate de asigurare a respectării dreptului penal face schimb de date cu o autoritate de asigurare a respectării dreptului nepenal, alta decât o agenție de informații (cum ar fi, de exemplu, o autoritate financiară sau fiscală, o autoritate de concurență, un oficiu de asistență pentru bunăstarea

([198]) Secțiunea 8 punctul 1 din Legea privind drepturile omului din 1998.

([199]) Secțiunea 36 punctul 3 din DPA din 2018.

([200]) Secțiunea 56 din Legea privind economia digitală din 2017, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2017/30/contents

([201]) Secțiunea 48 din Digital Economy Act 2017 (Legea privind economia digitală din 2017).

([202]) Secțiunea 7 din Crime and Courts Act 2013 (Legea privind criminalitatea și instanțele din 2013), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2013/22/contents

([203]) Secțiunea 68 din Serious Crime Act 2007 (Legea privind formele grave de criminalitate din 2007), disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2007/27/contents

([204]) Practicile profesionale autorizate privind schimbul de informații sunt disponibile la următoarea adresă: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

([205]) A se vedea, de exemplu, cauza M/the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), în care Înaltei Curți i s-a solicitat să analizeze schimbul de date dintre poliție și un parteneriat de reducere a criminalității din sectorul afacerilor (BCRP – Business Crime Reduction Partnership), o organizație abilitată să gestioneze sistemul de notificare de excludere, interzicând persoanelor să intre în spațiile comerciale ale membrilor săi. Instanța a examinat schimbul de date, care a avut loc pe baza unui acord având ca scop protejarea publicului și prevenirea criminalității și, în cele din urmă, a concluzionat că majoritatea aspectelor legate de schimbul de date sunt legale, cu excepția unor informații sensibile partajate între poliție și BCRP. Un alt exemplu este cauza Cooper/NCA [2019] EWCA Civ 16, în care Curtea de Apel a admis schimbul de date dintre poliție și Agenția pentru combaterea formelor grave de criminalitate organizată (SOCA – Serious Organised Crime Agency), o agenție de aplicare a legii care face parte în prezent din NCA.

([206]) Secțiunea 36 punctul 4 din DPA din 2018.

tinerilor); 2) atunci când o autoritate de asigurare a respectării dreptului penal face schimb de date cu o agenție de informații. În primul scenariu, prelucrarea datelor cu caracter personal va intra sub incidența RGPD al Regatului Unit, precum și a părții 2 din DPA din 2018. Astfel cum se specifică în decizia adoptată în temeiul Regulamentului (UE) 2016/679, garanțiile prevăzute de RGPD al Regatului Unit și de partea 2 din DPA din 2018 oferă un nivel de protecție care este în esență echivalent cu cel oferit în Uniune ([207]).

(127) În al doilea scenariu, în ceea ce privește schimbul de date colectate între o autoritate de asigurare a respectării dreptului penal și o agenție de informații în scopuri de securitate națională, temeiul juridic care autorizează un astfel de schimb este Counter Terrorism Act 2008 (Legea privind combaterea terorismului din 2008) (CTA din 2008) ([208]). În temeiul CTA din 2008, orice persoană poate furniza informații oricărui serviciu de informații în scopul îndeplinirii oricăreia dintre funcțiile serviciului respectiv, inclusiv „securitatea națională".

(128) În ceea ce privește condițiile în care datele pot fi partajate în scopuri de securitate națională, Intelligence Services Act (Legea privind serviciile de informații) și Security Services Act (Legea privind serviciile de securitate) limitează capacitatea serviciilor de informații de a obține date la ceea ce este necesar pentru îndeplinirea funcțiilor lor legale. Autoritățile competente, care intră sub incidența părții 3 din DPA din 2018 și care doresc să facă schimb de date cu serviciile de informații vor trebui să ia în considerare o serie de factori/limitări, pe lângă funcțiile statutare ale agențiilor prevăzute în Legea privind serviciile de informații și în Legea privind serviciile de securitate ([209]). Secțiunea 20 din CTA din 2008 clarifică faptul că orice schimb de date în temeiul secțiunii 19 din CTA din 2008 trebuie să respecte în continuare legislația privind protecția datelor, ceea ce înseamnă că se aplică toate limitările și cerințele prevăzute în DPA din 2018. În plus, autoritățile de aplicare a legii și serviciile de informații sunt autorități publice în sensul Legii privind drepturile omului din 1998, iar acestea trebuie să se asigure că acționează în conformitate cu drepturile conferite în temeiul CEDO, inclusiv cu articolul 8. Cu alte cuvinte, aceste cerințe înseamnă că toate schimburile de date între agențiile de aplicare a legii și serviciile de informații trebuie să respecte legislația privind protecția datelor și Convenția europeană a drepturilor omului.

(129) Prelucrarea de către serviciile de informații a datelor cu caracter personal primite sau obținute de la autoritățile de aplicare a legii în scopuri de securitate națională face obiectul unei serii de condiții și garanții ([210]). Partea 4 din DPA din 2018 se aplică tuturor prelucrărilor efectuate de serviciile de informații sau în numele acestora. Aceasta

([207]) Decizia de punere în aplicare a Comisiei în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția adecvată a datelor cu caracter personal de către Regatul Unit al Marii Britanii și Irlandei de Nord, C(2021) 4800.

([208]) Secțiunea 19 din Legea din 2008 privind combaterea terorismului, disponibilă la următoarea adresă: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([209]) Secțiunea 2 punctul 2 din Legea privind serviciile de informații din 1994 (a se vedea https://www.legislation.gov.uk/ukpga/1994/13/contents) prevede următoarele: „Șeful Serviciului de Informații este responsabil de eficiența acestui serviciu, având datoria de a se asigura – (a) că există mecanisme pentru a garanta că Serviciul de Informații nu obține informații decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor sale și că nicio informație nu este divulgată de către acesta decât în măsura în care este necesar (i) în acest scop; (ii) în interesul securității naționale; (iii) în scopul prevenirii sau depistării infracțiunilor grave; sau (iv) în scopul oricăror proceduri penale; și (b) că Serviciul de Informații nu ia nicio măsură pentru a promova interesele niciunui partid politic din Regatul Unit", în timp ce secțiunea 2 punctul 2 din Legea privind serviciile de securitate din 1989 (a se vedea https://www.legislation.gov.uk/ukpga/1989/5/contents) prevede următoarele: „Directorul general este responsabil de eficiența Serviciului, având datoria de a se asigura – (a) că există mecanisme pentru a garanta că Serviciul nu obține informații decât în măsura în care acest lucru este necesar pentru îndeplinirea corespunzătoare a funcțiilor sale și că nicio informație nu este divulgată de către acesta decât în măsura în care este necesar în acest scop sau în scopul prevenirii sau depistării infracțiunilor grave sau în scopul oricăror proceduri penale; și (b) că Serviciul nu ia nicio măsură pentru a promova interesele niciunui partid politic; și (c) că există mecanisme, convenite cu directorul general al Agenției Naționale pentru Combaterea Criminalității, pentru coordonarea activităților Serviciului în temeiul secțiunii 1 punctul 4 din această lege cu activitățile forțelor de poliție, ale Agenției Naționale pentru Combaterea Criminalității și ale altor agenții de aplicare a legii".

([210]) Garanțiile și limitările competențelor serviciilor de informații sunt, de asemenea, reglementate de Investigatory Powers Act 2016 (Legea din 2016 privind competențele de investigare) care, împreună cu Regulation of Investigatory Powers Act 2000 (Legea din 2000 de reglementare a competențelor de investigare) pentru Anglia, Țara Galilor și Irlanda de Nord și cu Regulation of Investigatory Powers (Scotland) Act 2000 [Legea din 2000 de reglementare a competențelor de investigare (Scoția)] pentru Scoția prevăd temeiul juridic pentru utilizarea acestor competențe. Totuși, aceste competențe nu sunt relevante în contextul „transferului ulterior", deoarece se referă la colectarea directă a datelor cu caracter personal de către serviciile de informații. Pentru o evaluare a competențelor acordate agențiilor de informații în temeiul Legii privind competențele de investigare, a se vedea Decizia de punere în aplicare a Comisiei în temeiul Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția adecvată a datelor cu caracter personal de către Regatul Unit, C(2021) 4800.

stabilește principalele principii privind protecția datelor (legalitate, echitate și transparență ([211]); limitări legate de scop ([212]); reducerea la minimum a datelor ([213]); exactitate ([214]); limitări legate de stocare ([215]) și securitate ([216]), impune condiții pentru prelucrarea categoriilor speciale de date ([217]), prevede drepturi ale persoanelor vizate ([218]), impune protecția datelor începând cu momentul conceperii ([219]) și reglementează transferurile internaționale de date cu caracter personal ([220]).

(130) În același timp, secțiunea 110 din DPA din 2018 prevede o derogare de la dispozițiile specificate în partea 4 din DPA din 2018, în cazul în care o astfel de derogare este necesară pentru protejarea securității naționale. Secțiunea 110 punctul 2 din DPA din 2018 enumeră dispozițiile de la care se permite o derogare. Aceasta include principiile privind protecția datelor (cu excepția principiului legalității), drepturile persoanei vizate, obligația de a informa comisarul pentru informații cu privire la o încălcare a securității datelor, competențele de inspecție ale comisarului pentru informații în conformitate cu obligațiile internaționale, anumite competențe ale comisarului pentru informații în materie de asigurare a respectării legii, dispozițiile care fac din anumite încălcări ale protecției datelor o infracțiune, precum și dispozițiile referitoare la scopurile speciale ale prelucrării, cum ar fi scopurile jurnalistice, academice sau artistice. Această derogare poate fi invocată pe baza unei analize de la caz la caz ([221]). Astfel cum au explicat autoritățile Regatului Unit și după cum este confirmat de jurisprudența instanțelor Regatului Unit, „(a) un operator trebuie să ia în considerare consecințele reale pentru securitatea națională sau apărare dacă ar trebui să respecte dispoziția specifică privind protecția datelor și dacă ar putea respecta în mod rezonabil regula obișnuită fără a afecta securitatea națională sau apărarea” ([222]). Utilizarea corespunzătoare sau necorespunzătoare a derogării face obiectul supravegherii ICO ([223]).

([211]) În temeiul secțiunii 86 punctul 6 din DPA din 2018, pentru a stabili echitatea și transparența prelucrării, trebuie să se ia în considerare metoda prin care aceasta este obținută. În acest sens, cerința de echitate și transparență este îndeplinită dacă datele sunt obținute de la o persoană care este autorizată sau obligată în mod legal să le furnizeze.

([212]) În conformitate cu secțiunea 87 din DPA din 2018, scopurile prelucrării trebuie să fie determinate, explicite și legitime. Datele nu trebuie prelucrate într-un mod incompatibil cu scopurile pentru care sunt colectate. În temeiul secțiunii 87 punctul 3, o prelucrare suplimentară compatibilă a datelor cu caracter personal poate fi permisă numai dacă operatorul este autorizat prin lege să prelucreze datele în acest scop, iar prelucrarea este necesară și proporțională cu scopul secundar respectiv. Prelucrarea ar trebui considerată compatibilă în cazul în care aceasta constă în prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice și face obiectul unor garanții adecvate (secțiunea 87 punctul 4 din DPA din 2018).

([213]) Datele cu caracter personal trebuie să fie adecvate, relevante și neexcesive (secțiunea 88 din DPA din 2018).

([214]) Datele cu caracter personal trebuie să fie exacte și actualizate (secțiunea 89 din DPA din 2018).

([215]) Datele cu caracter personal nu trebuie păstrate mai mult decât este necesar (secțiunea 90 din DPA din 2018).

([216]) Al șaselea principiu privind protecția datelor este că datele cu caracter personal trebuie prelucrate într-un mod care să includă luarea unor măsuri de securitate adecvate în ceea ce privește riscurile care decurg din prelucrarea datelor cu caracter personal. Riscurile includ (dar nu se limitează la) accesul accidental sau neautorizat la datele cu caracter personal sau distrugerea, pierderea, utilizarea, modificarea sau divulgarea acestora (secțiunea 91 din DPA din 2018). Secțiunea 107 prevede, de asemenea, că (1) fiecare operator trebuie să pună în aplicare măsuri de securitate adecvate pentru riscurile care decurg din prelucrarea datelor cu caracter personal și (2) în cazul prelucrării automate, fiecare operator și fiecare persoană împuternicită de operator pun în aplicare măsuri preventive sau de atenuare pe baza unei evaluări a riscurilor.

([217]) Secțiunea 86 punctul 2 litera (b) și anexa 10 la DPA din 2018.

([218]) Partea 4 capitolul 3 din DPA din 2018, în special drepturile: de acces, rectificare și ștergere, de a se opune prelucrării și de a nu face obiectul procesului decizional automatizat, de a interveni în procesul decizional automatizat și de a fi informat cu privire la procesul decizional. În plus, operatorul trebuie să ofere persoanei vizate informații cu privire la prelucrarea datelor sale cu caracter personal.

([219]) Secțiunea 103 din DPA din 2018.

([220]) Secțiunea 109 din DPA din 2018. Transferurile de date cu caracter personal către organizații internaționale sau țări din afara Regatului Unit sunt posibile dacă transferul este o măsură necesară și proporțională întreprinsă în scopul îndeplinirii funcțiilor legale ale operatorului sau în alte scopuri prevăzute în anumite secțiuni din Legea privind serviciile de securitate din 1989 (Security Service Act 1989) și din Legea privind serviciile de informații din 1994 (Intelligence Services Act 1994).

([221]) A se vedea Baker/Secretary of State for the Home Department [2001] UKIT NSA2 („Baker/Secretary of State”).

([222]) Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: National Security Data Protection and Investigatory Powers Framework (Cadrul privind protecția datelor în materie de securitate națională și competențele de investigare), paginile 15-16, disponibil la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. A se vedea, de asemenea, Baker/Secretary of State (a se vedea nota de subsol 220 de mai sus), în care tribunalul a anulat un certificat de securitate națională emis de ministrul de interne și prin care se confirma aplicarea excepției privind securitatea națională, considerând că nu există niciun motiv pentru a prevedea o excepție generală de la obligația de a răspunde cererilor de acces și că permiterea unei astfel de excepții în toate circumstanțele, fără o analiză de la caz la caz, ar depăși ceea ce este necesar și proporțional pentru protecția securității naționale.

([223]) A se vedea memorandumul de înțelegere dintre ICO și UKIC, conform căruia „La primirea unei plângeri din partea unei persoane vizate, ICO va dori să se asigure că problema a fost tratată corect și, după caz, că aplicarea oricărei derogări a fost utilizată în mod corespunzător” (Memorandumul de înțelegere dintre Biroul comisarului pentru informații și serviciile de informații din Regatul Unit, punctul 16, disponibil la următoarea adresă: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) În plus, în ceea ce privește posibilitatea de a restricționa oricare dintre drepturile menționate anterior pentru protecția „securității naționale", secțiunea 79 din DPA din 2018 prevede posibilitatea ca un operator să poată solicita un certificat semnat de un ministru din cadrul Cabinetului sau de procurorul general, care să ateste că restricționarea acestor drepturi este o măsură necesară și proporțională pentru protecția securității naționale ([224]). Guvernul Regatului Unit a emis orientări privind certificatele de securitate națională în temeiul DPA din 2018, care subliniază în special faptul că orice limitare a drepturilor persoanelor vizate în ceea ce privește protejarea securității naționale trebuie să fie proporțională și necesară ([225]). Toate certificatele de securitate națională trebuie publicate pe site-ul internet al ICO ([226]).

(132) Certificatul ar trebui să fie emis pe o durată determinată de maximum cinci ani, astfel încât să fie revizuit periodic de către executiv ([227]). Certificatul identifică datele cu caracter personal sau categoriile de date cu caracter personal care fac obiectul derogării, precum și dispozițiile DPA din 2018 cărora li se aplică derogarea ([228]).

(133) Este important de remarcat faptul că certificatele de securitate națională nu oferă un temei suplimentar pentru restricționarea drepturilor privind protecția datelor din motive de securitate națională. Cu alte cuvinte, operatorul sau persoana împuternicită de operator poate invoca un certificat numai atunci când a ajuns la concluzia că este necesar să invoce derogarea în materie de securitate națională care trebuie aplicată de la caz la caz. Chiar dacă un certificat de securitate națională se aplică chestiunii în cauză, ICO poate investiga dacă invocarea derogării în materie de securitate națională a fost sau nu justificată într-un caz specific ([229]).

(134) Orice persoană direct afectată de emiterea certificatului poate introduce o cale de atac la Tribunalul Superior ([230]) împotriva certificatului ([231]) sau, în cazul în care certificatul identifică date prin intermediul unei descrieri generale, poate contesta aplicarea certificatului la o serie de date specifice ([232]).

(135) Tribunalul va examina decizia de emitere a certificatului și va decide dacă au existat motive întemeiate pentru emiterea certificatului ([233]). Acesta poate lua în considerare o gamă largă de aspecte, printre care se numără și necesitatea, proporționalitatea și legalitatea, având în vedere impactul asupra drepturilor persoanelor vizate și punând în balanță necesitatea de a proteja securitatea națională. În consecință, tribunalul poate stabili că certificatul nu se aplică datelor cu caracter personal specifice care fac obiectul căii de atac ([234]).

([224]) DPA din 2018 a abrogat posibilitatea de a elibera un certificat în temeiul secțiunii 28 punctul 2 din Legea privind protecția datelor din 1998. Cu toate acestea, posibilitatea de a emite „certificate vechi" există în continuare în măsura în care există o posibilitate de recurs istorică în temeiul Legii din 1998 [a se vedea punctul 17 din partea 5 a anexei 20 la DPA din 2018]. Totuși, această posibilitate pare foarte rară și se va aplica numai în cazuri limitate, cum ar fi, de exemplu, în cazul în care o persoană vizată formulează o cale de atac în ceea ce privește utilizarea derogării în materie de securitate națională în legătură cu prelucrarea de către o autoritate publică care a efectuat prelucrarea în temeiul Legii din 1998. Trebuie remarcat faptul că, în aceste cazuri, secțiunea 28 din DPA din 1998 se va aplica în întregime, incluzând, prin urmare, posibilitatea ca persoana vizată să conteste certificatul. În prezent, nu există niciun certificat de securitate națională eliberat în temeiul DPA din 1998.

([225]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională în temeiul Legii privind protecția datelor din 2018, disponibile la următoarea adresă: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018 -_National_Security_Certificates_Guidance.pdf

([226]) În conformitate cu secțiunea 130 din DPA din 2018, ICO poate decide să nu publice textul sau o parte a textului certificatului, în cazul în care acest lucru ar fi contrar interesului securității naționale sau ar fi contrar interesului public sau ar putea pune în pericol siguranța oricărei persoane. În aceste cazuri, ICO va publica totuși faptul că certificatul a fost eliberat.

([227]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, punctul 15, a se vedea nota de subsol 225.

([228]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, punctul 5, nota de subsol 225.

([229]) Secțiunea 102 din DPA din 2018 prevede că operatorul trebuie să fie în măsură să demonstreze că s-a conformat DPA din 2018. Aceasta implică faptul că un serviciu de informații ar trebui să demonstreze ICO faptul că, atunci când invocă derogarea, a luat în considerare circumstanțele specifice ale cazului. ICO publică, de asemenea, o evidență a certificatelor de securitate națională, care este disponibilă la următoarea adresă: este disponibilă la următoarea adresă: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/

([230]) Tribunalul Superior este instanța competentă să soluționeze căile de atac împotriva hotărârilor pronunțate de tribunalele administrative inferioare și are competențe specifice pentru soluționarea căilor de atac directe introduse împotriva deciziilor anumitor organisme guvernamentale.

([231]) Secțiunea 111 punctul 3 din DPA din 2018.

([232]) Secțiunea 111 punctul 5 din DPA din 2018.

([233]) În cauza Baker/Secretary of State (a se vedea nota de subsol 221), Information Tribunal a anulat un certificat de securitate națională emis de ministrul de interne, considerând că nu există niciun motiv pentru a prevedea o excepție generală de la obligația de a răspunde cererilor de acces și că permiterea unei astfel de excepții în toate circumstanțele, fără o analiză de la caz la caz, ar depăși ceea ce este necesar și proporțional pentru protecția securității naționale.

([234]) Orientările Guvernului Regatului Unit privind certificatele de securitate națională, punctul 25, nota de subsol 225.

(136) Un set diferit de restricții posibile se referă la cele care se aplică, în temeiul anexei 11 la DPA din 2018, anumitor dispoziții ale părții 4 din DPA din 2018 ([235]) pentru a proteja alte obiective importante de interes public general sau interese protejate, cum ar fi, de exemplu, privilegiul parlamentar, secretul profesional al avocatului, desfășurarea procedurilor judiciare sau eficacitatea de luptă a forțelor armate. Aplicarea acestor dispoziții fie este exceptată pentru anumite categorii de informații („bazată pe categorii"), fie este exceptată în măsura în care aplicarea acestor dispoziții ar putea aduce atingere interesului protejat („bazată pe prejudicii") ([236]). Derogările bazate pe prejudicii pot fi invocate numai în măsura în care aplicarea dispoziției enumerate privind protecția datelor ar putea aduce atingere interesului specific în cauză. Prin urmare, utilizarea unei derogări trebuie să fie întotdeauna justificată prin trimiterea la prejudiciul relevant care ar putea apărea în fiecare caz în parte. Derogările bazate pe categorii pot fi invocate numai în ceea ce privește categoria specifică, definită în mod strict, de informații pentru care se acordă derogarea. Acestea sunt similare, în ceea ce privește scopul și efectul, mai multor excepții de la RGPD al Regatului Unit (în temeiul anexei 2 la DPA din 2018) care, la rândul lor, reflectă cele prevăzute la articolul 23 din RGPD.

(137) Din cele de mai sus rezultă că există limitări și condiții în temeiul dispozițiilor legale aplicabile din Regatul Unit, astfel cum sunt interpretate, de asemenea, de instanțe și de comisarul pentru informații, pentru a se asigura că aceste derogări și restricții rămân în limitele a ceea ce este necesar și proporțional pentru protejarea securității naționale.

(138) Prelucrarea datelor cu caracter personal efectuată de serviciile de informații în temeiul părții 4 din DPA din 2018 este supravegheată de comisarul pentru informații ([237]).

(139) Funcțiile generale ale comisarului pentru informații în ceea ce privește prelucrarea datelor cu caracter personal de către serviciile de informații în temeiul părții 4 din DPA din 2018 sunt prevăzute în anexa 13 la DPA din 2018. Sarcinile includ, însă nu se limitează, în special, la monitorizarea și punerea în aplicare a părții 4 din DPA din 2018, promovarea sensibilizării publicului, consilierea Parlamentului, a guvernului și a altor instituții cu privire la măsurile legislative și administrative, promovarea sensibilizării operatorilor și a persoanelor împuternicite de operatori cu privire la obligațiile ce le revin, furnizarea de informații unei persoane vizate cu privire la exercitarea drepturilor persoanei vizate și desfășurarea de anchete.

(140) În ceea ce privește partea 3 din DPA din 2018, comisarul are competența de a informa operatorii cu privire la o presupusă încălcare și de a emite avertismente cu privire la probabilitatea ca o prelucrare să încalce normele și de a emite mustrări atunci când încălcarea este confirmată. De asemenea, acesta poate emite notificări de executare și de sancționare pentru încălcarea anumitor dispoziții ale legii ([238]). Cu toate acestea, spre deosebire de alte părți din DPA din 2018, comisarul nu poate emite o notificare de evaluare a securității naționale ([239]).

(141) În plus, secțiunea 110 din DPA din 2018 prevede o excepție de la utilizarea anumitor competențe ale comisarului atunci când acest lucru este necesar în scopul protejării securității naționale. Aceasta include competența comisarului de a emite (orice tip de) notificări în temeiul DPA (notificări de informare, de evaluare, de executare și de sancționare), competența de a efectua inspecții în conformitate cu obligațiile internaționale, competențe de

([235]) Acestea includ: (i) principiile privind protecția datelor prevăzute în partea 4, cu excepția legalității cerinței de prelucrare în temeiul primului principiu și a faptului că prelucrarea trebuie să îndeplinească una dintre condițiile relevante prevăzute în anexele 9 și 10; (ii) drepturile persoanelor vizate; și (iii) obligațiile legate de raportarea încălcărilor către ICO.

([236]) Conform Cadrului explicativ al Regatului Unit, excepțiile „bazate pe categorii" sunt: (i) informații cu privire la acordarea de distincții și demnități ale Coroanei; (ii) secretul profesional al avocatului; (iii) referințe confidențiale privind angajarea, formarea sau educația; și (iv) foi de examinare și note la examene. Excepțiile „bazate pe prejudicii" se referă la următoarele aspecte: (i) prevenirea sau depistarea infracțiunilor; arestarea și urmărirea penală a infractorilor; (ii) privilegiul parlamentar; (iii) proceduri judiciare; (iv) eficacitatea de luptă a forțelor armate ale Coroanei; (v) bunăstarea economică a Regatului Unit; (vi) negocierile cu persoana vizată; (vii) scopuri de cercetare științifică sau istorică ori scopuri statistice; (viii) arhivarea în interes public. Cadrul explicativ al Regatului Unit pentru dezbaterile privind caracterul adecvat, secțiunea H: Securitatea națională, pagina 13, a se vedea nota de subsol 222.

([237]) Secțiunea 116 din DPA din 2018.

([238]) În temeiul unei lecturi combinate a secțiunii 149 punctul 2 și a secțiunii 155 din DPA din 2018, notificările de punere în aplicare și de sancționare pot fi transmise unui operator sau unei persoane împuternicite de operator în legătură cu încălcări ale părții 4 capitolul 2 din DPA din 2018 (principiile prelucrării), ale unei dispoziții a părții 4 din DPA din 2018 ce conferă drepturi unei persoane vizate, ale cerinței de a comunica o încălcare a securității datelor cu caracter personal comisarului în temeiul secțiunii 108 din DPA din 2018 și ale principiilor privind transferurile de date cu caracter personal către țări terțe, țări care nu participă la convenție și organizații internaționale din secțiunea 109 din DPA din 2018. (Pentru detalii suplimentare privind notificările de executare și de sancționare, a se vedea considerentele 102 și 103).

([239]) În temeiul secțiunii 147 punctul 6 din DPA din 2018, comisarul pentru informații nu poate transmite o notificare de evaluare organismelor menționate la secțiunea 23 punctul 3 din Legea din 2000 privind liberul acces la informațiile de interes public. Printre acestea se numără Serviciul de Securitate (MI5), Serviciul Secret de Informații (MI6) și Cartierul General pentru Comunicații.

intrare și de inspecție, precum și norme privind infracțiunile ([240]). Astfel cum se explică în considerentul 136, aceste excepții se vor aplica numai dacă sunt necesare și proporționale și de la caz la caz. Aplicarea acestor excepții poate face obiectul unui control jurisdicțional ([241]).

(142) ICO și serviciile de informații din Regatul Unit au semnat un memorandum de înțelegere ([242]) care stabilește un cadru de cooperare cu privire la o serie de aspecte, inclusiv notificări privind încălcarea securității datelor și tratarea plângerilor persoanelor vizate. În special, acesta prevede că, la primirea unei plângeri, ICO va evalua dacă a fost invocată în mod corespunzător vreo derogare în materie de securitate națională. Răspunsurile la întrebările adresate de ICO în contextul examinării plângerilor individuale trebuie să fie furnizate în termen de 20 de zile lucrătoare prin Orientările Guvernului Regatului Unit privind certificatele de securitate națională în temeiul Legii privind protecția datelor, utilizând canale securizate adecvate, în cazul în care acestea implică informații clasificate. Din aprilie 2018 până în prezent, ICO a primit 21 de plângeri de la persoane fizice cu privire la serviciile de informații. Fiecare plângere a fost evaluată, iar rezultatul a fost comunicat persoanei vizate ([243]).

(143) În plus, Comisia pentru Informații și Securitate (ISC) exercită o supraveghere parlamentară asupra prelucrării datelor de către agențiile de informații. Această comisie își are temeiul juridic în Legea din 2013 privind justiția și securitatea (JSA din 2013) ([244]). Legea instituie ISC ca o comisie a Parlamentului Regatului Unit. ISC este alcătuită din membri care aparțin uneia dintre camerele Parlamentului și sunt numiți de prim-ministru după consultarea liderului opoziției ([245]). ISC trebuie să prezinte Parlamentului un raport anual privind îndeplinirea funcțiilor sale, precum și alte rapoarte pe care le consideră adecvate ([246]).

(144) Începând din 2013, ISC a beneficiat de competențe sporite, inclusiv supravegherea activităților operaționale ale serviciilor de securitate. În temeiul secțiunii 2 din JSA din 2013, ISC are sarcina de a supraveghea cheltuielile, administrarea, politicile și operațiunile agențiilor de securitate națională. JSA din 2013 specifică faptul că ISC este în

([240]) Dispozițiile care pot fi exceptate sunt: secțiunea 108 (informarea comisarului cu privire la încălcarea securității datelor cu caracter personal), secțiunea 119 (inspecție în conformitate cu obligațiile internaționale); secțiunile 142-154 și anexa 15 (Notificările comisarului și competențele de intrare și de inspecție); și secțiunile 170-173 (infracțiuni legate de datele cu caracter personal). În plus, în ceea ce privește prelucrarea de către serviciile de informații din anexa 13 (alte funcții generale ale comisarului), punctul 1 literele (a) și (g) și punctul 2.

([241]) A se vedea, de exemplu, cauza Baker/Secretary of State for the Home Department (a se vedea nota de subsol 221)

([242]) Memorandumul de înțelegere dintre ICO și serviciile de informații din Regatul Unit (a se vedea nota de subsol 231).

([243]) În șapte dintre aceste cazuri, ICO a recomandat reclamantului să prezinte problema în fața operatorului de date (acest lucru este valabil atunci când o persoană fizică a prezentat o problemă în fața ICO, dar ar fi trebuit să o prezinte mai întâi în fața operatorului de date), în unul dintre aceste cazuri, ICO a oferit consiliere generală operatorului de date (această procedură este utilizată atunci când acțiunile operatorului nu par să fi încălcat legislația, dar este posibil ca o îmbunătățire a practicilor să fi evitat prezentarea problemei în fața ICO), iar în celelalte 13 cazuri, operatorul nu a avut obligația de a întreprinde nicio acțiune (această procedură este utilizată atunci când problemele prezentate de persoana fizică intră sub incidența Legii privind protecția datelor din 2018 deoarece se referă la prelucrarea informațiilor cu caracter personal, dar, pe baza informațiilor furnizate de operator, nu par să fi încălcat legislația).

([244]) Astfel cum au explicat autoritățile Regatului Unit, JSA a extins domeniul de competență al ISC pentru a include un rol în supravegherea comunității serviciilor de informații dincolo de cele trei agenții și pentru a permite supravegherea retrospectivă a activităților operaționale ale agențiilor în chestiuni de interes național major.

([245]) Secțiunea 1 din JSA din 2013. Miniștrii nu sunt eligibili pentru statutul de membri. Membrii își exercită funcția în cadrul ISC pe durata mandatului Parlamentului în cursul căruia au fost numiți. Aceștia pot fi revocați printr-o rezoluție a Camerei prin care au fost numiți, în cazul în care nu mai au calitatea de membri sau devin miniștri. De asemenea, un membru poate demisiona.

([246]) Rapoartele și declarațiile comisiei sunt disponibile online la următoarea adresă: http://isc.independent.gov.uk/committee-reports. În 2015, ISC a publicat un raport privind „Dreptul la viață privată și securitatea: un cadru juridic modern și transparent" (*Privacy and Security: A modern and transparent legal framework*) (a se vedea: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf) în care a analizat cadrul juridic pentru tehnicile de supraveghere utilizate de agențiile de informații și a emis o serie de recomandări care au fost apoi luate în considerare și integrate în proiectul de lege privind competențele de investigare, care a fost transformat în lege, IPA 2016. Răspunsul guvernului la raportul privind dreptul la viață privată și securitatea este disponibil la următoarea adresă: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

măsură să desfășoare investigații cu privire la aspecte operaționale atunci când acestea nu se referă la operațiuni în curs ([247]). Memorandumul de înțelegere convenit între prim-ministru și ISC ([248]) precizează în detaliu elementele care trebuie luate în considerare atunci când se analizează dacă o activitate nu face parte din nicio operațiune în curs ([249]). De asemenea, ISC poate fi invitată să investigheze operațiunile în curs de desfășurare de către prim-ministru și poate revizui informațiile furnizate în mod voluntar de agenții.

(145) În conformitate cu anexa 1 la JSA din 2013, ISC poate solicita șefilor oricăruia dintre cele trei servicii de informații să divulge informații. Agenția trebuie să pună la dispoziție aceste informații, cu excepția cazului în care secretarul de stat își exercită un drept de veto în acest sens ([250]). Autoritățile Regatului Unit au explicat că, în practică, foarte puține informații nu sunt comunicate ISC ([251]).

(146) În ceea ce privește căile de atac, în primul rând, în temeiul secțiunii 165 punctul 2 din DPA din 2018, o persoană vizată poate depune o plângere la ICO în cazul în care consideră că, în ceea ce privește datele cu caracter personal care o privesc, există o încălcare a părții 4 din DPA din 2018, inclusiv orice utilizare abuzivă a derogărilor și restricțiilor în materie de securitate națională.

(147) În plus, în temeiul părții 4 din DPA din 2018, persoanele fizice au dreptul să solicite Înaltei Curți (sau Court of Session din Scoția) un ordin prin care să îi impună operatorului să respecte drepturile de acces la date ([252]), să se opună prelucrării ([253]) și să rectifice sau să șteargă datele.

(148) De asemenea, persoanele fizice au dreptul să solicite operatorului sau unei persoane împuternicite de operator ([254]) despăgubiri pentru prejudiciile suferite ca urmare a încălcării unei cerințe prevăzute în partea 4 din DPA din 2018. Prejudiciul include atât pierderi financiare, cât și prejudicii care nu implică pierderi financiare, cum ar fi suferințele clinice ([255]).

(149) În cele din urmă, o persoană fizică poate depune o plângere la Tribunalul cu competențe de investigare pentru orice comportament al agențiilor de informații din Regatul Unit ([256]) sau în numele acestora. Tribunalul cu competențe de investigare (Investigatory Powers Tribunal – IPT) este instituit prin Legea din 2000 de reglementare a competențelor de investigare pentru Anglia, Țara Galilor și Irlanda de Nord și prin Legea din 2000 de reglementare a competențelor de investigare (Scoția) pentru Scoția (RIPA din 2000) și este independent de puterea executivă ([257]). În conformitate cu secțiunea 65 din RIPA din 2000, membrii IPT sunt numiți de Majestatea Sa pentru o perioadă de cinci ani.

(150) Un membru al Tribunalului poate fi revocat din funcție de Majestatea Sa în urma unei propuneri („address") ([258]) formulate de ambele camere ale Parlamentului ([259]).

(151) Pentru a introduce o acțiune în fața IPT („cerință privind calitatea procesuală"), în conformitate cu secțiunea 65 din RIPA din 2000, o persoană fizică trebuie să aibă convingerea (i) că a avut loc un serviciu de informații în legătură cu ea, cu privire la oricare dintre bunurile sale, cu privire la orice comunicare trimisă de sau către ea ori care îi este destinată sau utilizarea oricărui serviciu poștal, serviciu de telecomunicații sau sistem de telecomunicații ([260]) și

([247]) Secțiunea 2 din JSA din 2013.
([248]) Memorandumul de înțelegere dintre prim-ministru și ISC, disponibil la următoarea adresă: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf
([249]) Memorandumul de înțelegere dintre prim-ministru și ISC, punctul 14, a se vedea nota de subsol 248.
([250]) Secretarul de stat se poate opune divulgării informațiilor numai în două cazuri: informațiile sunt sensibile și nu ar trebui divulgate ISC în interesul securității naționale; sau este vorba de informații de o asemenea natură încât, în cazul în care secretarul de stat ar fi solicitat să le prezinte în fața unei comisii departamentale restrânse a Camerei Comunelor, secretarul de stat ar considera (pentru motive care nu se limitează la securitatea națională) că nu ar trebui să facă acest lucru (punctul 4 subpunctul 2 din anexa 1 la JSA din 2013).
([251]) Cadrul explicativ al Regatului Unit – secțiunea H: Securitatea națională, p. 43.
([252]) Secțiunea 94 punctul 11 din DPA din 2018.
([253]) Secțiunea 99 punctul 4 din DPA din 2018.
([254]) Secțiunea 169 din DPA din 2018, care admite cererile depuse de „o persoană care suferă prejudicii ca urmare a încălcării unei cerințe a legislației privind protecția datelor".
([255]) Secțiunea 169 punctul 5 din DPA din 2018.
([256]) A se vedea secțiunea 65 punctul 2 litera (b) din RIPA.
([257]) În conformitate cu anexa 3 la RIPA din 2000, membrii trebuie să aibă o experiență judiciară specifică și să fie eligibili pentru o nouă numire.
([258]) În ceea ce privește noțiunea de „address", a se vedea nota de subsol 183.
([259]) Punctul 1 subpunctul 5 din anexa 3 la RIPA din 2000.
([260]) Secțiunea 65 punctul 4 din RIPA din 2000.

(ii) comportamentul a avut loc în „circumstanțe atacabile” ([261]) sau „a fost efectuat de către sau în numele serviciilor de informații” ([262]). Întrucât, în special, acest standard în materie de „convingere” a fost interpretat în sens destul de larg ([263]), sesizarea Tribunalului face obiectul unui nivel relativ scăzut de cerințe privind calitatea procesuală.

(152) În cazul în care Tribunalul examinează o plângere care îi este adresată, este de datoria Tribunalului să investigheze dacă persoanele împotriva cărora se face vreo acuzație în plângere au fost implicate în relații cu reclamantul, precum și să investigheze autoritatea care se presupune că a fost implicată în încălcări și dacă presupusul comportament a avut loc ([264]). În cazul în care Tribunalul judecă o procedură, acesta trebuie să aplice, în cadrul procedurii respective, aceleași principii care ar fi aplicate de o instanță cu privire la o cerere de control jurisdicțional ([265]).

(153) Tribunalul trebuie să informeze reclamantul dacă a fost luată o hotărâre în favoarea sa sau nu ([266]). În temeiul secțiunii 67 punctele 6 și 7 din RIPA din 2000, Tribunalul are competența de a emite ordine provizorii și de a pronunța orice hotărâre de despăgubire sau orice altă ordonanță pe care o consideră adecvată ([267]). În conformitate cu secțiunea 67A din RIPA din 2000, o hotărâre a Tribunalului poate fi atacată, sub rezerva autorizării de către Tribunal sau de către instanța de apel competentă.

(154) În special, persoanele fizice pot introduce o acțiune – și pot obține reparații – în fața IPT în cazul în care consideră că o autoritate publică a acționat (sau propune să acționeze) într-un mod care este incompatibil cu un drept conferit prin Convenția europeană a drepturilor omului, inclusiv dreptul la viață privată și protecția datelor cu caracter personal și, prin urmare, este ilegal în temeiul secțiunii 6 punctul 1 din Legea privind drepturile omului din 1998. IPT i s-a acordat competență judiciară exclusivă pentru toate cererile în baza Legii privind drepturile omului în legătură cu agențiile de informații. Astfel cum a remarcat High Court (Înalta Curte), aceasta înseamnă că „dacă a existat o încălcare a HRA cu privire la situația de fapt dintr-o anumită cauză, acest fapt poate fi invocat și soluționat, în principiu, de către un tribunal independent care poate avea acces la toate elementele relevante, inclusiv la materiale secrete. […] De asemenea, în acest context, avem în vedere faptul că IPT este în prezent supus posibilității de a introduce o cale de atac la o instanță de apel adecvată (în Anglia și Țara Galilor, aceasta este Curtea de Apel); iar Curtea Supremă a decis recent că IPT poate, în principiu, să facă obiectul unui control jurisdicțional: a se vedea R (Privacy International)/Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219” ([268]). În cazul în care constată că un act al unei autorități publice este ilegal, IPT poate admite o astfel de reparație sau cale de atac sau poate dispune, în limitele competențelor sale, după cum consideră corect și adecvat ([269]).

([261]) Astfel de circumstanțe se referă la comportamentul autorităților publice cu autoritate (de exemplu, un mandat, o autorizație/notificare pentru obținerea de comunicații etc.) sau dacă circumstanțele sunt de așa natură încât (indiferent dacă există sau nu o astfel de autoritate), nu ar fi fost adecvat ca respectivul comportament să aibă loc în lipsa acestuia sau, cel puțin, fără să se fi analizat în mod corespunzător dacă o astfel de autoritate ar trebui solicitată. Se consideră că un comportament autorizat de un comisar judiciar a avut loc în circumstanțe atacabile (secțiunea 65 punctul 7ZA din RIPA din 2000), în timp ce alte comportamente care au loc cu permisiunea unei persoane care deține funcții judiciare sunt considerate a nu fi avut loc în circumstanțe atacabile (secțiunea 65 punctele 7 și 8 din RIPA din 2000).

([262]) Potrivit informațiilor furnizate de autoritățile Regatului Unit, pragul redus pentru depunerea unei plângeri determină că nu este neobișnuit ca ancheta Tribunalului să stabilească faptul că reclamantul nu a făcut niciodată obiectul unei anchete desfășurate de către o autoritate publică. Cel mai recent raport statistic al IPT precizează că, în 2016, Tribunalul a înregistrat 209 plângeri, 52 % dintre acestea au fost considerate neserioase sau vexatorii, iar 25 % au rămas nesoluționate. Autoritățile Regatului Unit au explicat că acest lucru înseamnă fie că nu au fost utilizate activități/competențe disimulate în legătură cu reclamantul, fie că au fost utilizate tehnici ascunse, iar tribunalul a stabilit că activitatea este legală. În plus, 11 % au fost excluse din jurisdicție, retrase sau nevalabile, 5 % au fost prescrise, 7 % au fost stabilite în favoarea reclamantului. Raportul statistic al Tribunalului cu competențe de investigare din 2016, disponibil la următoarea adresă: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) A se vedea cauza Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH. În acest caz, IPT, făcând trimitere la jurisprudența Curții Europene a Drepturilor Omului, a statuat că, în ceea ce privește convingerea că orice comportament care intră sub incidența subsecțiunii 68 punctul 5 din RIPA din 2000 a fost efectuat de către sau în numele unui serviciu de informații, testul adecvat este de a stabili dacă există un temei pentru o astfel de convingere, inclusiv faptul că o persoană poate pretinde că este victima unei încălcări determinate de simpla existență a unor măsuri secrete sau a unei legislații care permite măsuri secrete, numai în cazul în care poate demonstra că, din cauza situației sale personale, aceasta poate fi expusă riscului de a face obiectul unor astfel de măsuri (a se vedea Human Rights Watch/Secretary of State, punctul 41).

([264]) Secțiunea 67 punctul 3 din RIPA din 2000.

([265]) Secțiunea 67 punctul 2 din RIPA din 2000.

([266]) Secțiunea 68 punctul 4 din RIPA din 2000.

([267]) Aceasta poate include un ordin prin care se solicită distrugerea oricăror înregistrări de informații deținute de orice autoritate publică în legătură cu o persoană.

([268]) Înalta Curte de Justiție, Liberty, [2019] EWHC 2057 (Admin), punctul 170.

([269]) Secțiunea 8 punctul 1 din Legea privind drepturile omului din 1998.

(155) După epuizarea căilor de atac naționale, o persoană poate obține reparații în fața Curții Europene a Drepturilor Omului pentru încălcarea drepturilor garantate de CEDO, inclusiv a dreptului la viață privată și la protecția datelor.

(156) Din cele de mai sus rezultă că partajarea de către autoritățile de aplicare a dreptului penal din Regatul Unit a datelor transferate în temeiul prezentei decizii cu alte autorități publice, inclusiv cu agențiile de informații, este încadrată de limitări și condiții care asigură faptul că o astfel de partajare ulterioară va fi necesară și proporțională și va face obiectul unor garanții specifice privind protecția datelor în temeiul DPA din 2018. În plus, prelucrarea datelor de către autoritățile publice în cauză este supravegheată de organisme independente, iar persoanele afectate au acces la căi de atac judiciare eficace.

3. **CONCLUZIE**

(157) Comisia consideră că partea 3 din DPA din 2018 asigură un nivel de protecție a datelor cu caracter personal transferate în scopul asigurării respectării dreptului penal de la autoritățile competente din Uniune către autoritățile competente din Regatul Unit care este în esență echivalent cu cel garantat de Directiva (UE) 2016/680.

(158) În plus, Comisia consideră că, în ansamblu, mecanismele de supraveghere și căile de atac prevăzute în legislația Regatului Unit permit detectarea și pedepsirea în practică a încălcărilor comise și pun la dispoziția persoanelor vizate căile de atac juridice necesare pentru a obține accesul la datele cu caracter personal care le privesc și, în cele din urmă, rectificarea sau ștergerea datelor respective.

(159) În cele din urmă, pe baza informațiilor disponibile cu privire la ordinea juridică a Regatului Unit, Comisia consideră că orice atingere adusă, în scopuri de interes public, inclusiv în contextul schimbului de date cu caracter personal între autoritățile de aplicare a legii și alte autorități publice, cum ar fi organismele de securitate națională, de autoritățile publice ale Regatului Unit drepturilor fundamentale ale persoanelor fizice ale căror date cu caracter personal sunt transferate din Uniunea Europeană în Regatul Unit, se va limita la ceea ce este strict necesar pentru îndeplinirea obiectivului legitim în cauză, cât și că există o protecție juridică eficace împotriva unor astfel de atingeri.

(160) Prin urmare, ar trebui să se decidă că Regatul Unit asigură un nivel adecvat de protecție în sensul articolului 36 alineatul (2) din Directiva (UE) 2016/680, interpretat în lumina Cartei drepturilor fundamentale.

(161) Această concluzie se bazează atât pe regimul intern relevant al Regatului Unit, cât și pe angajamentele sale internaționale, în special aderarea la Convenția europeană a drepturilor omului și recunoașterea competenței Curții Europene a Drepturilor Omului. Respectarea în continuare a acestor obligații internaționale este, prin urmare, un element deosebit de important al evaluării pe care se bazează prezenta decizie.

4. **EFECTELE PREZENTEI DECIZII ȘI ACȚIUNILE AUTORITĂȚILOR PENTRU PROTECȚIA DATELOR**

(162) Statele membre și organele acestora au obligația de a lua măsurile necesare pentru a se conforma actelor instituțiilor Uniunii, întrucât se presupune că aceste acte sunt legale și, prin urmare, produc efecte juridice atât timp cât nu expiră, sunt retrase, anulate în cadrul unei acțiuni în anulare sau declarate nule ca urmare a unei trimiteri preliminare sau a unei excepții de nelegalitate.

(163) În consecință, o decizie a Comisiei privind caracterul adecvat al nivelului de protecție, adoptată în temeiul articolului 36 alineatul (3) din Directiva (UE) 2016/680, este obligatorie pentru toate organele statelor membre cărora li se adresează, inclusiv pentru autoritățile de supraveghere independente ale acestora. În special, în cursul perioadei de aplicare a prezentei decizii, transferurile de la un operator sau de la o persoană împuternicită de operator din Uniune către operatori sau persoane împuternicite de operatori din Regatul Unit pot avea loc fără a fi necesară obținerea unei autorizații suplimentare.

(164) În același timp, ar trebui reamintit faptul că, în temeiul articolului 47 alineatul (5) din Directiva (UE) 2016/680 și astfel cum este explicat de Curtea de Justiție în hotărârea pronunțată în cauza Schrems, în cazul în care o autoritate națională de protecție a datelor pune sub semnul întrebării, inclusiv în urma primirii unei plângeri, compatibilitatea unei decizii a Comisiei privind caracterul adecvat al nivelului de protecție cu dreptul fundamental al unei persoane la viață privată și la protecția datelor, legislația națională trebuie să prevadă o cale de atac pentru a prezenta obiecțiile respective în fața unei instanțe naționale, care poate fi obligată să efectueze o trimitere preliminară către Curtea de Justiție ([270]).

([270]) Schrems, punctul 65.

5. **MONITORIZAREA, SUSPENDAREA, ABROGAREA SAU MODIFICAREA PREZENTEI DECIZII**

(165) În temeiul articolului 36 alineatul (4) din Directiva (UE) 2016/680, Comisia trebuie să monitorizeze în permanență evoluțiile relevante din Regatul Unit după adoptarea prezentei decizii pentru a evalua dacă aceasta garantează în continuare un nivel de protecție echivalent în esență. O astfel de monitorizare este deosebit de importantă în acest caz, întrucât Regatul Unit va administra, va aplica și va asigura respectarea unui nou regim de protecție a datelor ce nu mai intră sub incidența dreptului Uniunii, care ar putea evolua. În acest sens, se va acorda o atenție deosebită aplicării în practică a normelor Regatului Unit privind transferurile de date cu caracter personal către țări terțe, inclusiv prin încheierea de acorduri internaționale, impactului pe care aceasta l-ar putea avea asupra nivelului de protecție acordat datelor transferate în temeiul prezentei decizii, precum și eficacității exercitării drepturilor individuale în domeniile reglementate de prezenta decizie. Printre alte elemente, evoluțiile jurisprudenței și supravegherea de către ICO și alte organisme independente vor contribui la monitorizarea efectuată de Comisie.

(166) Pentru a facilita această monitorizare, autoritățile Regatului Unit ar trebui să informeze cu promptitudine și cu regularitate Comisia cu privire la orice modificare substanțială a ordinii juridice a Regatului Unit care are un impact asupra cadrului juridic care face obiectul prezentei decizii, precum și cu privire la orice evoluție a practicilor legate de prelucrarea datelor cu caracter personal evaluate în prezenta decizie, în special în ceea ce privește elementele menționate în considerentul 165.

(167) În plus, pentru a permite Comisiei să își exercite în mod eficace funcția de monitorizare, statele membre ar trebui să informeze Comisia cu privire la orice acțiune relevantă întreprinsă de autoritățile naționale de protecție a datelor, în special în ceea ce privește solicitările sau plângerile formulate de persoanele vizate din UE cu privire la transferul de date cu caracter personal din Uniunea Europeană către autorități competente din Regatul Unit. De asemenea, Comisia ar trebui să fie informată cu privire la orice indiciu potrivit căruia acțiunile autorităților publice ale Regatului Unit responsabile cu prevenirea, investigarea, detectarea sau aducerea în fața instanței a infracțiunilor, inclusiv acțiunile oricărui organism de supraveghere, nu asigură nivelul de protecție necesar.

(168) În cazul în care informațiile disponibile, în special informațiile care rezultă din monitorizarea prezentei decizii sau cele furnizate de autoritățile Regatului Unit sau ale statelor membre, arată că nivelul de protecție oferit de Regatul Unit ar putea să nu mai fie adecvat, Comisia ar trebui să informeze autoritățile Regatului Unit competente în acest sens și să solicite luarea unor măsuri adecvate într-un termen rezonabil specificat, care nu poate depăși trei luni. Dacă este necesar, acest termen poate fi prelungit cu o anumită perioadă de timp, ținând seama de natura problemei în cauză și/sau de măsurile care trebuie luate.

(169) În cazul în care, la expirarea termenului specificat, autoritățile competente ale Regatului Unit nu iau măsurile respective sau nu demonstrează în mod satisfăcător că prezenta decizie continuă să se bazeze pe un nivel adecvat de protecție, Comisia va iniția procedura menționată la articolul 58 alineatul (2) din Directiva (UE) 2016/680 în vederea suspendării sau abrogării parțiale sau integrale a prezentei decizii.

(170) Ca alternativă, Comisia va iniția această procedură în vederea modificării prezentei decizii, în special prin aplicarea unor condiții suplimentare transferurilor de date sau prin limitarea domeniului de aplicare al constatării referitoare la caracterul adecvat numai la transferurile de date pentru care se asigură în continuare un nivel adecvat de protecție.

(171) Din motive imperioase de urgență justificate corespunzător, Comisia va face uz de posibilitatea de a adopta, în conformitate cu procedura menționată la articolul 58 alineatul (3) din Directiva (UE) 2016/680, acte de punere în aplicare imediat aplicabile de suspendare, abrogare sau modificare a deciziei.

6. **DURATA ȘI REÎNNOIREA PREZENTEI DECIZII**

(172) Ar trebui să se țină seama de faptul că, odată cu încheierea perioadei de tranziție prevăzute în Acordul de retragere și de îndată ce dispoziția provizorie prevăzută la articolul 782 din Acordul comercial și de cooperare UE- Regatul Unit va înceta să se aplice, Regatul Unit va administra, va aplica și va asigura respectarea unui nou regim de protecție a datelor în raport cu cel în vigoare în perioada în care avea obligații în temeiul dreptului Uniunii Europene. Acest lucru poate implica, în special, amendamente sau modificări ale cadrului de protecție a datelor evaluat în prezenta decizie, precum și alte evoluții relevante.

(173) Prin urmare, este oportun să se prevadă că prezenta decizie se va aplica pentru o perioadă de patru ani de la intrarea sa în vigoare.

(174) În cazul în care, în special, informațiile obținute în urma monitorizării prezentei decizii arată că respectivele constatări referitoare la caracterul adecvat al nivelului de protecție asigurat în Regatul Unit sunt încă justificate de fapt și de drept, Comisia ar trebui, cel târziu cu șase luni înainte de încetarea aplicării prezentei decizii, să inițieze procedura de modificare a prezentei decizii prin extinderea domeniului său de aplicare temporal, în principiu, pentru o perioadă suplimentară de patru ani. Orice act de punere în aplicare de modificare a prezentei decizii urmează să fie adoptat în conformitate cu procedura menționată la articolul 58 alineatul (2) din Directiva (UE) 2016/680.

7. **CONSIDERAȚII FINALE**

(175) Comitetul european pentru protecția datelor și-a publicat avizul ([271]), care a fost luat în considerare la pregătirea prezentei decizii.

(176) Măsurile prevăzute de prezenta decizie sunt conforme cu avizul comitetului instituit în temeiul articolului 58 din Directiva (UE) 2016/680.

(177) În conformitate cu articolul 6a din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei în ceea ce privește spațiul de libertate, securitate și justiție, anexat la TUE și la TFUE, Irlandei nu îi revin obligații în temeiul normelor stabilite în Directiva (UE) 2016/680 și, prin urmare, în temeiul prezentei decizii de punere în aplicare, referitoare la prelucrarea datelor cu caracter personal de către statele membre în exercitarea activităților care intră în domeniul de aplicare al părții a treia titlul V capitolul 4 sau 5 din TFUE, atât timp cât Irlandei nu îi revin obligații în temeiul normelor Uniunii privind formele de cooperare judiciară în materie penală sau de cooperare polițienească care necesită respectarea dispozițiilor stabilite în temeiul articolului 16 din TFUE. În plus, în temeiul Deciziei de punere în aplicare (UE) 2020/1745 a Consiliului ([272]), Directiva (UE) 2016/680 urmează să fie pusă în aplicare și aplicată cu titlu provizoriu în Irlanda începând cu 1 ianuarie 2021. Prin urmare, Irlandei îi revin obligații în temeiul prezentei decizii de punere în aplicare, în aceleași condiții valabile în cazul aplicării Directivei (UE) 2016/680 în Irlanda, astfel cum se prevede în decizia de punere în aplicare (UE) 2020/1745, în ceea ce privește acquis-ul Schengen la care participă.

(178) În conformitate cu articolele 2 și 2a din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu este obligată să aplice normele prevăzute în Directiva (UE) 2016/680 și, prin urmare, în prezenta decizie de punere în aplicare și nici nu face obiectul aplicării lor care se referă la prelucrarea datelor cu caracter personal de către statele membre atunci când desfășoară activități care intră sub incidența părții a treia titlul V capitolul 4 sau capitolul 5 din TFUE. Cu toate acestea, având în vedere faptul că Directiva (UE) 2016/680 se întemeiază pe acquis-ul Schengen, Danemarca, în conformitate cu articolul 4 din protocolul respectiv, a notificat la data de 26 octombrie 2016 decizia sa de a pune în aplicare Directiva (UE) 2016/680. Prin urmare, Danemarca are obligația, în temeiul dreptului internațional, să pună în aplicare prezenta decizie de punere în aplicare.

(179) În ceea ce privește Islanda și Norvegia, prezenta decizie de punere în aplicare constituie o dezvoltare a dispozițiilor acquis-ului Schengen, astfel cum prevede Acordul încheiat de Consiliul Uniunii Europene și Republica Islanda și Regatul Norvegiei privind asocierea acestor două state la implementarea, aplicarea și dezvoltarea acquis-ului Schengen ([273]).

(180) În ceea ce privește Elveția, prezenta decizie de punere în aplicare constituie o dezvoltare a dispozițiilor acquis-ului Schengen, astfel cum prevede Acordul între Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană cu privire la asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([274]).

(181) În ceea ce privește Liechtenstein, prezenta decizie de punere în aplicare constituie o dezvoltare a dispozițiilor acquis-ului Schengen, astfel cum se prevede în Protocolul dintre Uniunea Europeană, Comunitatea Europeană, Confederația Elvețiană și Principatul Liechtenstein privind aderarea Principatului Liechtenstein la Acordul dintre Uniunea Europeană, Comunitatea Europeană și Confederația Elvețiană privind asocierea Confederației Elvețiene la punerea în aplicare, respectarea și dezvoltarea acquis-ului Schengen ([275]),

---

([271]) Avizul 15/2021 privind Proiectul de decizie de punere în aplicare a Comisiei Europene în temeiul Directivei (UE) 2016/680 privind protecția adecvată a datelor cu caracter personal în Regatul Unit, disponibil la adresa https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en

([272]) Decizia de punere în aplicare (UE) 2020/1745 a Consiliului din 18 noiembrie 2020 privind punerea în aplicare a dispozițiilor acquis-ului Schengen referitoare la protecția datelor și privind punerea în aplicare cu titlu provizoriu a unor dispoziții ale acquis-ului Schengen în Irlanda (JO L 393, 23.11.2020, p. 3).

([273]) JO L 176, 10.7.1999, p. 36.

([274]) JO L 53, 27.2.2008, p. 52.

([275]) JO L 160, 18.6.2011, p. 21.

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

În sensul articolului 36 din Directiva (UE) 2016/680, Regatul Unit garantează un nivel adecvat de protecție a datelor cu caracter personal transferate din Uniunea Europeană către autoritățile publice ale Regatului Unit responsabile cu prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor sau cu executarea pedepselor.

Articolul 2

Ori de câte ori autoritățile de supraveghere competente din statele membre, pentru a proteja persoanele fizice în ceea ce privește prelucrarea datelor cu caracter personal, își exercită competențele în temeiul articolului 47 din Directiva (UE) 2016/680 în ceea ce privește transferurile de date către autoritățile publice ale Regatului Unit care intră în domeniul de aplicare prevăzut la articolul 1, statul membru în cauză informează fără întârziere Comisia.

Articolul 3

(1) Comisia monitorizează în permanență aplicarea cadrului juridic pe care se bazează prezenta decizie, inclusiv condițiile în care se efectuează transferurile ulterioare și se exercită drepturile individuale, pentru a evalua dacă Regatul Unit continuă să asigure un nivel adecvat de protecție în sensul articolului 1.

(2) Statele membre și Comisia se informează reciproc cu privire la cazurile în care comisarul pentru informații, sau orice altă autoritate competentă a Regatului Unit nu asigură respectarea cadrului juridic pe care se bazează prezenta decizie.

(3) Statele membre și Comisia se informează reciproc atât cu privire la orice indiciu potrivit căruia atingerile aduse de autoritățile publice din Regatul Unit dreptului persoanelor fizice la protecția datelor cu caracter personal depășesc ceea ce este strict necesar, cât și cu privire la faptul că nu există o protecție juridică eficace împotriva unor astfel de atingeri.

(4) În cazul în care Comisia are indicii că nu mai este asigurat un nivel adecvat de protecție, Comisia informează autoritățile competente din Regatul Unit și poate suspenda, abroga sau modifica prezenta decizie.

(5) Comisia poate suspenda, abroga sau modifica prezenta decizie în cazul în care lipsa de cooperare a autorităților Regatului Unit împiedică Comisia să stabilească dacă este afectată constatarea de la articolul 1.

Articolul 4

Prezenta decizie expiră la 27 iunie 2025, cu excepția cazului în care este prelungită în conformitate cu procedura menționată la articolul 58 alineatul (2) din Directiva (UE) 2016/680.

Articolul 5

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles, 28 iunie 2021.

Pentru Comisie
Didier REYNDERS
Membru al Comisiei