РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2021/1773 НА КОМИСИЯТА

от 28 юни 2021 година

съгласно Директива (ЕС) 2016/680 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство

(нотифицирано под номер C(2021) 4801)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета ([1]), и по-специално член 36, параграф 3 от нея,

като има предвид, че:

1. ВЪВЕДЕНИЕ

(1) В Директива (ЕС) 2016/680 се определят правилата за предаването на лични данни от компетентните органи в Съюза на трети държави и международни организации, доколкото това предаване попада в приложното ѝ поле. Правилата относно международното предаване на данни от компетентните органи са установени в глава V от Директива (ЕС) 2016/680, по-специално в членове 35—40. Въпреки че движението на лични данни към и от държави извън Европейския съюз е от съществено значение за ефикасното сътрудничество в областта на правоприлагането, трябва да се гарантира, че нивото на защита, което се предоставя на личните данни в Европейския съюз, не се излага на риск от такова предаване ([2]).

(2) Съгласно член 36, параграф 3 от Директива (ЕС) 2016/680 Комисията може да реши посредством акт за изпълнение, че дадена трета държава, територия или един или повече конкретни сектори в дадена трета държава, или дадена международна организация осигуряват адекватно ниво на защита. При това условие предаването на лични данни на трета държава може да се извършва, без да е необходимо допълнително разрешение (с изключение на случаите, когато друга държава членка, от която са получени данните, трябва да даде своето разрешение за предаването), както е предвидено в член 35, параграф 1 и съображение 66 от Директива (ЕС) 2016/680.

(3) Както е посочено в член 36, параграф 2 от Директива (ЕС) 2016/680, приемането на решение относно адекватното ниво на защита трябва да се основава на цялостен анализ на правовия ред на третата държава. В своята оценка Комисията трябва да определи дали въпросната трета държава гарантира ниво на защита, „по същество равностойно“ на осигуреното в рамките на Европейския съюз (съображение 67 от Директива (ЕС) 2016/680). Стандартът, спрямо който се оценява „равностойността по същество“, е определеният от законодателството на ЕС, по-специално от Директива (ЕС) 2016/680, както и от съдебната практика на Съда на Европейския съюз ([3]). Референтният документ на Европейския комитет по защита на данните за адекватното ниво на защита също е от значение в това отношение ([4]).

(4) Както бе изяснено от Съда на Европейския съюз, това не изисква установяване на идентично ниво на защита ([5]). По-специално средствата, до които въпросната трета държава прибягва за защита на личните данни, могат да са различни от прилаганите в Европейския съюз, стига те на практика да се окажат ефективни за осигуряването на адекватно ниво на защита ([6]). Поради това стандартът за адекватно ниво на защита не включва изискване за буквално възпроизвеждане на правилата на Съюза. Критерият се състои по-скоро в това дали чрез същността на правото на неприкосновеност на личния живот и неговото ефективно прилагане, надзор и изпълнение чуждестранната система като цяло осигурява необходимото ниво на защита ([7]).

([1]) ОВ L 119, 4.5.2016 г., стр. 89.

([2]) Вж. съображение 64 от Директива (ЕС) 2016/680.

([3]) Вж., като най-скорошна практика, решение по дело *Maximilian Schrems/Data Protection Commissioner* (C-311/18), ECLI:EU:C:2020:559 (решение по дело *Schrems II*).

([4]) Вж. Препоръка 01/2021 относно референтния документ за адекватното ниво на защита съгласно Директивата относно правоприлагането в областта на защитата на данните, приета през февруари 2021 г., която е достъпна на следния адрес: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_bg

([5]) Решение по дело *Maximilian Schrems/Data Protection Commissioner* (C-362/14), ECLI:EU:C:2015:650, т. 73 (решение по дело *Schrems*).

([6]) Решение по дело *Schrems*, т. 74.

([7]) Съобщение на Комисията до Европейския парламент и Съвета „Обмен и защита на личните данни в един глобализиран свят“ (COM (2017) 7 от 10.1.2017 г.), раздел 3.1, стр. 6—7, достъпно на следния адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:52017DC0007&from=BG

(5) Комисията анализира внимателно съответното законодателство и практиката на Обединеното кралство. Въз основа на своите констатации, изложени по-долу, Комисията стига до заключението, че Обединеното кралство осигурява адекватно ниво на защита на личните данни, предавани от компетентните органи в Съюза, попадащи в обхвата на Директива (ЕС) 2016/680, на компетентните органи в Обединеното кралство, попадащи в обхвата на част 3 от Закона за защита на данните от 2018 г. (ЗЗД от 2018 г.) ([8]).

(6) В резултат на настоящото решение подобно предаване може да се извършва за период от четири години, без да е необходимо допълнително разрешение, като е възможно подновяване, и без да се засягат условията, предвидени в член 35 от Директива (ЕС) 2016/680.

2. ПРАВИЛА, КОИТО СЕ ПРИЛАГАТ ЗА ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ ОТ КОМПЕТЕНТНИТЕ ОРГАНИ ЗА ЦЕЛИТЕ НА НАКАЗАТЕЛНОТО ПРАВОПРИЛАГАНЕ

2.1. Конституционна уредба

(7) Обединеното кралство е парламентарна демокрация. То има суверенен парламент, който е върховен спрямо всички останали държавни институции, изпълнителна власт, представителите на която се избират от парламента и се отчитат пред него, и независима съдебна власт. Изпълнителната власт черпи правомощията си от способността си да се ползва от доверието на избраната Камара на общините и се отчита пред двете камари на парламента (Камарата на общините и Камарата на лордовете), които отговарят за контрола върху правителството и за обсъждането и приемането на закони. Парламентът на Обединеното кралство е делегирал законодателни правомощия на парламента на Шотландия, парламента на Уелс (Senedd Cymru) и Събранието на Северна Ирландия по някои вътрешни въпроси в Шотландия, Уелс и Северна Ирландия. Макар защитата на данните да е въпрос, който е от компетентността на парламента на Обединеното кралство, т.е. едно и също законодателство се прилага в цялата страна, други области на политиката, свързани с настоящото решение, са делегирани. Например правомощията, свързани с наказателно-правните системи на Шотландия и Северна Ирландия, включително полицейската дейност (дейностите, извършвани от полицейските служби), са делегирани съответно на парламента на Шотландия и на Събранието на Северна Ирландия ([9]).

(8) Въпреки че Обединеното кралство не разполага с кодифицирана конституция в смисъла на утвърден учредителен документ, с течение на времето се е оформил обликът на неговите конституционни принципи, произтичащи по-специално от съдебната практика и конвенциите. Някои нормативни актове, като например Магна харта (Magna Carta), Законът за правата (Bill of Rights) от 1689 г. и Законът за правата на човека (Human Rights Act) от 1998 г., имат призната конституционна стойност. Като част от конституцията, основните права на физическите лица са развити чрез общото право, нормативните актове и международните договори, по-специално Европейската конвенция за правата на човека (ЕКПЧ), която Обединеното кралство ратифицира през 1951 г. Обединеното кралство също така ратифицира Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108) през 1987 г. ([10]).

(9) Със Закона за правата на човека от 1998 г. правата, съдържащи се в ЕКПЧ, се въвеждат в правото на Обединеното кралство. По силата на този закон на всяко физическо лице се предоставят основните права и свободи, предвидени в членове 2—12 и в член 14 от ЕКПЧ, както и в членове 1—3 от Първия протокол към нея и в член 1 от Тринадесетия протокол към нея, във връзка с членове 16—18 от ЕКПЧ. Това включва правото на зачитане на личния и семейния живот, което на свой ред обхваща правото на защита на данните и правото на справедлив съдебен процес ([11]). По-специално, съгласно член 8 от ЕКПЧ държавните власти могат да се намесват в ползването на правото на неприкосновеност на личния живот само в случаите, предвидени в закона, когато това е необходимо в едно демократично общество в интерес на националната и обществената сигурност или на икономическото благосъстояние на страната, за предотвратяване на безредици или престъпления, за защита на здравето и морала или на правата и свободите на другите.

([8]) Закон за защита на данните от 2018 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел F: Правоприлагане (UK Explanatory Framework for Adequacy Discussion, section F: Law enforcement), достъпна на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) Първоначално принципите на Конвенция № 108 бяха въведени в правото на Обединеното кралство чрез Закона за защита на данните (Data Protection Act) от 1984 г., който беше заменен от ЗЗД от 1998 г., а след това от ЗЗД от 2018 г. (във връзка с ОРЗД на Обединеното кралство). Обединеното кралство също така подписа Протокола за изменение на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (известна като „Конвенция 108+“) през 2018 г. и понастоящем работи по ратифицирането на Конвенцията.

([11]) Членове 6 и 8 от ЕКПЧ (вж. също приложение 1 към Закона за правата на човека от 1998 г.).

(10) В съответствие със Закона за правата на човека от 1998 г. всяко действие на публичните органи трябва да бъде съвместимо с право, гарантирано съгласно ЕКПЧ ([12]). Освен това първичното законодателство и подзаконовите актове трябва да се тълкуват и прилагат по начин, който е съвместим с тези права ([13]). В случай че дадено лице счита, че неговите права, включително правото на неприкосновеност на личния живот и защита на данните, са били нарушени от публични органи, то може да получи правна защита пред съдилищата на Обединеното кралство съгласно Закона за правата на човека от 1998 г., а впоследствие — след изчерпване на националните средства за правна защита — може да получи правна защита пред Европейския съд по правата на човека за нарушения на правата, гарантирани от ЕКПЧ.

2.2. **Уредбата на Обединеното кралство за защита на данните**

(11) Обединеното кралство се оттегли от Съюза на 31 януари 2020 г. Въз основа на Споразумението за оттеглянето на Обединеното кралство Великобритания и Северна Ирландия от Европейския съюз и Европейската общност за атомна енергия ([14]) правото на Съюза продължи да се прилага в Обединеното кралство по време на преходния период до 31 декември 2020 г. Преди оттеглянето и по време на преходния период правната уредба относно защитата на личните данни в Обединеното кралство, уреждаща обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване, се състоеше от съответните части от Закона за защита на данните от 2018 г., с който е транспонирана Директива (ЕС) 2016/680.

(12) С цел подготвяне на излизането от ЕС правителството на Обединеното кралство прие Закона от 2018 г. за оттеглянето от Европейския съюз (EUWA) ([15]), с който пряко приложимите законодателни актове на Съюза бяха включени в правото на Обединеното кралство и се предвиди, че т. нар. „произтичащо от правото на ЕС национално законодателство“ ще продължи да поражда действие след края на преходния период. Съгласно EUWA част 3 от ЗЗД от 2018 г. ([16]), с който се транспонира Директива (ЕС) 2016/680, представлява „произтичащо от правото на ЕС национално законодателство“. По силата на EUWA „произтичащото от правото на ЕС национално законодателство“, което не е изменено, трябва да се тълкува от съдилищата на Обединеното кралство съгласно съответната съдебна практика на Съда на Европейския съюз (Съда) и общите принципи на правото на Съюза, тъй като те са били в сила непосредствено преди края на преходния период (наричани съответно „запазена съдебна практика на ЕС“ и „запазени общи принципи на правото на ЕС“) ([17]).

(13) Съгласно EUWA министрите на Обединеното кралство имат правомощието чрез нормативни актове да създават вторично законодателство във връзка с въвеждането на необходими изменения в запазеното законодателство на ЕС, произтичащи от оттеглянето на Обединеното кралство от Съюза. Това правомощие беше упражнено с Наредбите от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС) ([18]). С тях се изменя законодателството на Обединеното кралство за защита на данните, включително ЗЗД от 2018 г., с цел привеждане в съответствие с националния контекст ([19]).

([12]) Член 6 от Закона за правата на човека от 1998 г.

([13]) Член 3 от Закона за правата на човека от 1998 г.

([14]) Споразумение за оттеглянето на Обединеното кралство Великобритания и Северна Ирландия от Европейския съюз и Европейската общност за атомна енергия (2019/C 384 I/01, XT/21054/2019/INIT, ОВ C 384I, 12.11.2019 г., стр. 1—177) („Споразумение за оттегляне“), достъпно на следния адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=BG

([15]) Закон от 2018 г. за оттеглянето от Европейския съюз, достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Закон за защита на данните от 2018 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Член 6 от EUWA от 2018 г.

([18]) Наредби от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС), достъпни на следния адрес: https://www.legislation.gov.uk/uksi/2019/419/contents/made, изменени с Наредбите от 2020 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС), достъпни на следния адрес: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) С Наредбите за напускане се въвеждат редица изменения в част 3 от ЗЗД от 2018 г. Много от тези изменения представляват технически промени, като например заличаване на позоваванията на „държава членка“ или на „Директивата относно правоприлагането в областта на защитата на данните“ (вж. напр. член 48, параграф 8 или член 73, параграф 5, буква а) от ЗЗД от 2018 г., където се заменя с „национално право“), така че част 3 да се прилага ефективно като национално законодателство след края на преходния период. На някои места са били необходими други видове промени, например по отношение на това „кой“ приема „решения относно адекватното ниво на защита“ за целите на правната уредба на Обединеното кралство за защита на данните (вж. член 74A от ЗЗД от 2018 г.), т.е. министърът, а не Европейската комисия.

(14) Следователно съгласно Споразумението за оттегляне след преходния период правните стандарти относно обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност в Обединеното кралство и тяхното предотвратяване, ще продължат да бъдат определени в съответните части от ЗЗД от 2018 г., но изменени с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения, по-специално в част 3 от посочения акт. Общият регламент относно защитата на данните на Обединеното кралство (ОРЗД на Обединеното кралство) не се прилага за този вид обработване.

(15) В част 3 от ЗЗД от 2018 г. са предвидени правилата за обработването на лични данни за целите на наказателното правоприлагане, включително принципите за защита на данните, правните основания за обработването (законосъобразността), правата на субектите на данни, задълженията на компетентните органи в качеството им на администратори и ограниченията за последващо предаване. Същевременно приложимите правила относно надзора, привеждането в изпълнение и средствата за защита, приложими за сектора на правоприлагането, са предвидени в части 5 и 6 от ЗЗД от 2018 г.

(16) Също така, с оглед на съответната роля на полицейските служби в сектора на правоприлагането, следва да се вземат предвид правилата, уреждащи полицейската дейност. Тъй като полицейската дейност е делегиран въпрос, по отношение на нея в а) Англия и Уелс, б) Шотландия и в) Северна Ирландия ([20]) се прилагат различни законодателни актове, които обаче често са сходни по съдържание. Освен това в различни видове ръководства се предоставят допълнителни разяснения относно начина, по който следва да се използват правомощията на полицията. Съществуват три основни вида насоки в областта на полицейската дейност: 1) нормативни насоки, издадени съгласно законодателството, като Етичният кодекс ([21]) и Кодексът за поведение относно управлението на полицейска информация ([22]), издадени съгласно Закона за полицията от 1996 г. ([23]), или Кодексът за поведение на Закона за полицията и доказателствата в наказателния процес ([24]), издаден съгласно Закона за полицията и доказателствата в наказателния процес ([25]), 2) Ръководството за разрешена професионална практика относно управлението на полицейска информация ([26]), издадено от Полицейския колеж и 3) оперативните насоки (публикувани от самата полиция). Националният съвет на началниците на полицията (координационен орган за всички полицейски служби на Обединеното кралство) публикува оперативни насоки, които всички полицейски служби са одобрили и които следователно се прилагат на национално равнище ([27]). Целта на тези насоки е да се осигури съгласуваност между службите по отношение на начина, по който се управлява информацията ([28]).

(17) Кодексът за поведение относно управлението на полицейска информация беше издаден през 2005 г. от министъра, при използване на правомощията, предвидени в член 39A от Закона за полицията от 1996 г. ([29]). Всеки кодекс за поведение, издаден съгласно Закона за полицията, трябва да бъде одобрен от министъра, като преди внасянето му в парламента е необходимо да се проведе консултация с Националната агенция по престъпността (*National Crime Agency*). С член 39a, параграф 7 от Закона за полицията се въвежда изискване полицията надлежно да взема предвид

([20]) За по-подробно обяснение относно полицейските служби и техните правомощия в Обединеното кралство вж.: Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел F: Правоприлагане (вж. бележка под линия 9).

([21]) Кодекс за поведение относно принципите и стандартите за професионално поведение на полицейската професия в Англия и Уелс (Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales), достъпен на следния адрес: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; Етичен кодекс на полицейската служба на Северна Ирландия (Police Service Northern Ireland Code of Ethic), достъпен на следния адрес: https://www.nipolicingboard.org.uk/psni-code-ethics; Етичен кодекс за полицейската дейност в Шотландия (Code of Ethic for policing in Scotland), достъпен на следния адрес: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) Кодекс за поведение относно управлението на полицейска информация (Code of Practice on the Management of Police Information), достъпен на следния адрес: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) Закон за полицията (Police Act) от 1996 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Кодекс за поведение на Закона за полицията и доказателствата в наказателния процес от 1984 г. (Police and Criminal Evidence Act 1984 (PACE) codes of practice), достъпен на следния адрес: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice

([25]) Закон за полицията и доказателствата в наказателния процес (Police and Criminal Evidence Act) от 1984 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1984/60/contents

([26]) Ръководство за разрешена професионална практика относно управлението на полицейска информация (Authorised Professional Practice on the Management of Police Information), достъпно на следния адрес: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) Наръчник за защита на данните за полицейски специалисти в областта на защитата на данните (Data Protection Manual for Police Data Protection Professionals), достъпен на следния адрес: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) Напр. Кодексът за поведение относно управлението на полицейска информация (вж. бележка под линия 22) се прилага по отношение на съхраняването на оперативна полицейска информация (вж. съображение 47 от настоящото решение).

([29]) Според информацията, предоставена от органите на Обединеното кралство, по време на разговорите относно адекватното ниво на защита Полицейският колеж е бил в процес на изготвяне на Кодекс за поведение относно управлението на информация и регистри, който да замени Кодекса за поведение относно управлението на полицейска информация. Проектът на кодекс е публикуван за обществена консултация на 25 януари 2021 г. и е достъпен на следния адрес: https://www.college.police.uk/article/information-records-management-consultation

кодексите, издадени съгласно Закона, следователно от полицията се очаква да го спазва ([30]). Освен това ненормативните насоки (като Ръководството за разрешена професионална практика относно управлението на полицейска информация) трябва винаги да са съгласувани с Кодекса за поведение относно управлението на полицейска информация, който се ползва с приоритет спрямо него ([31]). Във всеки случай, макар че може да има определени оперативни ситуации, при които е необходимо да се отклонят от тези насоки, полицейските служители остават задължени да съблюдават изискванията, определени в част 3 от ЗЗД от 2018 г. ([32]).

(18) Допълнителни насоки относно законодателството на Обединеното кралство за защита на данните във връзка с обработването в сектора на правоприлагането се предоставят от комисаря по информацията (ICO) ([33]) (за повече подробности относно ICO вж. съображения 93—109). Въпреки че насоките не са правнообвързващи, по съдебно дело съдът ще бъде задължен да вземе предвид всяко тяхно нарушение, тъй като те имат тълкувателна тежест и показват как законодателството за защита на данните се тълкува и привежда в изпълнение на практика от комисаря ([34]).

(19) Накрая, както е посочено в съображения 8—10, правоприлагащите органи на Обединеното кралство трябва да осигурят спазването на ЕКПЧ и Конвенция № 108.

(20) Следователно по своята структура и основни компоненти правната уредба за обработването на данни от правоприлагащите органи в областта на наказателното право на Обединеното кралство е много сходна с тази, която се прилага в ЕС. Това включва и факта, че тази уредба се основава не само на предвидени в националното право задължения, които са съобразени с правото на ЕС, но и на задължения, залегнали в международното право, по-специално чрез присъединяването на Обединеното кралство към ЕКПЧ и Конвенция № 108, както и подчиняването му на юрисдикцията на Европейския съд по правата на човека. Следователно тези задължения, които произтичат от правнообвързващи международни инструменти, отнасящи се по-специално до защитата на личните данни, са особено важен елемент от правната уредба, която е предмет на оценка в настоящото решение.

2.3. **Материален и териториален обхват**

(21) Материалният обхват на част 3 от ЗЗД от 2018 г. съвпада с този на Директива (ЕС) 2016/680, определен в член 2, параграф 2 от нея. Част 3 се прилага за обработването от компетентен орган на лични данни изцяло или частично с автоматични средства, както и за обработването от компетентен орган с други средства на лични данни, които са част от регистър с лични данни или са предназначени да съставляват част от такъв регистър.

(22) Също така, за да попадне в обхвата на посочената част 3, администраторът трябва да бъде „компетентен орган“, а обработването трябва да се извършва за „целите на правоприлагането“. Поради това режимът за защита на данните, който се оценява в настоящото решение, се прилага за всички дейности по правоприлагане на тези компетентни органи.

(23) Понятието „компетентен орган“ е определено в член 30 от ЗЗД като лице, посочено в приложение 7 към ЗЗД от 2018 г., както и всяко друго лице, доколкото това лице има законоустановени функции за някоя от целите на правоприлагането. Компетентните органи, изброени в приложение 7, включват не само полицейските служби, но и всички министерски ведомства на Обединеното кралство, както и други органи с функции по разследване (напр.

([30]) По дело R/the Commission of Police of the Metropolis [2014] EWCA Civ 585 правният статут на Кодекса за поведение относно управлението на полицейска информация е потвърден и съдия Laws обявява, че съгласно член 39A от Закона за полицията от 1996 г. комисарят от Столичната полицейска служба (Metropolitan Police) е длъжен да се придържа към Кодекса за поведение относно управлението на полицейска информация и Ръководството за разрешена професионална практика относно управлението на полицейска информация.

([31]) Полицията е обект на проверки по отношение на спазването на Кодекса за поведение относно управлението на полицейска информация от Кралския инспекторат на полицейските, противопожарните и спасителните служби (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services).

([32]) В тази връзка вж. позицията на Полицейския колеж относно спазването на Ръководството за разрешена професионална практика по отношение на всички елементи на полицейската дейност, в която се обяснява, че „Ръководството за разрешена професионална практика е одобрено от професионалния орган за полицейска дейност (Полицейския колеж) като официален източник на професионална практика в областта на полицейската дейност. От полицейските служители се очаква да вземат предвид Ръководството за разрешена професионална практика при изпълнението на отговорностите си. Възможно е обаче да съществуват обстоятелства, при които да е налице основателна оперативна причина дадена служба да се отклони от Ръководството за разрешена професионална практика, при условие че има ясна обосновка за това. Съответната служба носи отговорност за всеки риск от местен или национален характер, свързан с отклоняването от договорените на национално равнище насоки, а ако в резултат на това възникне инцидент или започне разследване (напр. чрез независимата служба за полицейско поведение (Independent Office of Police Conduct), службата носи отговорност за всеки риск.“ Повече информация може да бъде намерена на следния адрес: https://www.app.college.police.uk/faq-page/

([33]) Насоки за обработване на данни в областта на правоприлагането (Guide to Law Enforcement Processing), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) Вж. дело *Bridges/the Chief Constable of South Wales Police* [2019] EWHC 2341 (Admin), по което, макар да отбелязва ненормативния характер на насоките на комисаря, Висшият съд посочва, че „[к]огато преценява дали администратор на данни е спазил или не задължението по член 64 [да извърши оценка на въздействието върху защитата на данните във връзка с високорисково обработване на данни], съдът ще вземе предвид насоките, издадени от комисаря по информацията, по отношение на оценките на въздействието върху защитата на данните“.

комисаря на Кралската данъчна и митническа служба, органа по приходите на Уелс, Органа за защита на конкуренцията и пазарите, Кралския имотен регистър или Националната агенция по престъпността), органи за наказателно преследване, други органи за наказателно правосъдие и други субекти или организации, които извършват дейности по правоприлагане ([35]). Част 3 от ЗЗД от 2018 г. се прилага и за съдилищата и трибуналите, когато те упражняват своите правораздавателни функции, с изключение на частта, свързана с правата на субекта на данни и надзора от страна на ICO ([36]). Списъкът на компетентните органи, представен в приложение 7, не е окончателен и може да бъде актуализиран от министъра с наредби, като се вземат предвид промените в организацията на публичните служби ([37]).

(24) Въпросното обработване трябва също така да бъде за „целите на правоприлагането“, определяни като предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване ([38]). Обработването от компетентен орган не се урежда от част 3 от ЗЗД от 2018 г., когато не се извършва за целите на правоприлагането. Такъв например ще бъде случаят, когато Органът за защита на конкуренцията и пазарите разследва случаи, които не са инкриминирани (напр. сливания между дружества). В този случай ще се прилага ОРЗД на Обединеното кралство, заедно с част 2 от ЗЗД от 2018 г., тъй като обработването на лични данни от компетентните органи се извършва за цели, различни от целите на правоприлагането. При определянето на приложимия режим за защита на данните (част 3 или част 2 от ЗЗД от 2018 г.) по отношение на въпросното обработване на лични данни компетентният орган, т.е. администраторът, трябва да прецени дали „основната цел“ на това обработване е една от целите на правоприлагането съгласно ЗЗД от 2018 г.

(25) Що се отнася до териториалния обхват на част 3 от ЗЗД от 2018 г., в член 207, параграф 2 се предвижда, че ЗЗД се прилага за обработването на лични данни в контекста на дейността на лице, установено на територията на Обединеното кралство. Това включва публичните органи на територията на Англия, Уелс, Шотландия и Северна Ирландия, които попадат в материалния обхват на част 3 от ЗЗД от 2018 г. ([39]).

2.3.1. *Определение за лични данни и обработване*

(26) Ключовите понятия за лични данни и обработване са определени в член 3 от ЗЗД от 2018 г. и се прилагат в целия ЗЗД. Определенията следват стриктно съответните определения, установени в член 3 от Директива (ЕС) 2016/680. Съгласно ЗЗД от 2018 г. „лични данни“ означава всяка информация, свързана с идентифицирано живо физическо лице или живо физическо лице, което може да бъде идентифицирано ([40]). Съгласно член 3, параграф 3 от ЗЗД 2018 г. физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано, пряко или непряко, въз основа на информацията, включително чрез позоваване на име или идентификатор, или чрез позоваване на един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, икономическата, културната или социалната идентичност на това физическо лице. Понятието „обработване“ се определя като операция или съвкупност от операции, извършвани с информация или набор от информация, като: а) събиране, записване, организиране, структуриране или съхранение; б) адаптиране или промяна; в) извличане, консултиране или използване; г) разкриване чрез предаване, разпространяване или друга форма на осигуряване на достъп до данните; д) подреждане или комбиниране; или е) ограничаване, изтриване или унищожаване. Освен това в Закона „обработване на чувствителни данни“ се определя като: а) обработването на лични данни, разкриващо расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в професионални съюзи; б) обработването на генетични данни или биометрични данни с цел уникално идентифициране на физическото лице; в) обработването на данни за здравословното състояние; г) обработването на данни, свързани със сексуалния живот или сексуалната ориентация на физическото лице“ ([41]). В това отношение в член 205 от ЗЗД от 2018 г. се съдържат определенията за „биометрични данни“ ([42]), „данни за здравословното състояние“ ([43]) и „генетични данни“ ([44]).

([35]) Сред тях в приложение 7 към ЗЗД от 2018 г. са изброени главният прокурор, главният прокурор за Северна Ирландия и комисарят по информацията.

([36]) Член 43, параграф 3 от ЗЗД от 2018 г.

([37]) Член 30, параграф 3 от ЗЗД от 2018 г. Разузнавателните служби (Службата за тайно разузнаване (Secret Intelligence Service), Службата за сигурност (Security Service) и Правителствената централа за комуникации (Government Communications Headquarters) не са компетентни органи (вж. член 30, параграф 2 от ЗЗД от 2018 г.) и част 3 от ЗЗД от 2018 г. не се прилага за никоя от техните дейности. Тези дейности попадат в обхвата на част 4 от ЗЗД от 2018 г.

([38]) Член 31 от ЗЗД от 2018 г.

([39]) Това означава, че ЗЗД от 2018 г., а следователно и настоящото решение не се прилагат за зависимите от Британската корона територии и другите отвъдморски територии на Обединеното кралство, като например Фолкландските острови и територията на Гибралтар.

([40]) Личните данни, свързани с починало лице, не попадат в обхвата на ЗЗД от 2018 г.

([41]) Член 35, параграф 8 от ЗЗД от 2018 г.

([42]) „Биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни.

([43]) „Данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние.

([44]) „Генетични данни“ означава лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация относно физиологията или здравето на това физическо лице и които са получени по-специално чрез анализ на биологична проба от въпросното физическо лице.

(27) В член 32 от ЗЗД от 2018 г. се изясняват определенията за „администратор“ и „обработващ лични данни“ в контекста на обработването на лични данни за целите на правоприлагането, като стриктно се следват съответстващите им определения в Директива (ЕС) 2016/680. „Администратор“ означава компетентният орган, който определя целите и средствата за обработването на лични данни. Когато обработването се изисква от закона, администраторът е компетентният орган, на когото се налага такова задължение по съответния закон. „Обработващ лични данни“ се определя като всяко лице, което обработва лични данни от името на администратора (различно от лице, което е служител на администратора).

2.4. **Гаранции, права и задължения**

2.4.1. *Законосъобразност и добросъвестност на обработването*

(28) Съгласно член 35 от ЗЗД от 2018 г. обработването на лични данни трябва да бъде законосъобразно и добросъвестно, подобно на изискването по член 4, параграф 1, буква а) от Директива (ЕС) 2016/680. В съответствие с член 35, параграф 2 от ЗЗД от 2018 г. обработването на лични данни за всяка от целите на правоприлагането е законосъобразно само ако е въз основа на правото и ако или субектът на данни е дал съгласие за обработването за тази цел, или обработването е необходимо за изпълнението на задача, осъществявана за тази цел от компетентен орган.

2.4.1.1. Обработване въз основа на правото

(29) Подобно на разпоредбите на член 8 от Директива (ЕС) 2016/680, за да се осигури законосъобразността на обработването, попадащо в обхвата на част 3 от ЗЗД от 2018 г., това обработване трябва да бъде „въз основа на правото“. „Законосъобразно“ обработване означава разрешено по силата на нормативен акт, общото право или кралски изключителни права ([45]).

(30) Правомощията на компетентните органи като цяло се уреждат от нормативни актове, което означава, че техните функции и правомощия са ясно определени в законодателни актове, приети от Парламента ([46]). В определени случаи полицията, както и други компетентни органи, изброени в приложение 7 към ЗЗД от 2018 г., могат да се осланят на общото право, за да обработват данни ([47]). Общото право е създадено чрез прецеденти, установени с решения на съдилищата. Общото право е от значение в контекста на правомощията на полицията, която черпи от този източник на правото основното си задължение да защитава обществеността, като разкрива и предотвратява престъпления ([48]). Полицейските служби обаче

([45]) Обяснителни бележки към ЗЗД от 2018 г., параграф 181, достъпни на следния адрес: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Националната агенция по престъпността например черпи правомощията си от Закона за престъпленията и съдилищата (Crime and Courts Act) от 2013 г., който е достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2013/22/contents. По подобен начин правомощията на Агенцията за стандартите за храните (Food Standards Agency) са предвидени в Закона за стандартите за храните (Food Standards Act) от 1999 г., който е достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1999/28/contents. Други примери включват Закона за наказателното преследване на извършителите (Prosecution of Offenders Act) от 1985 г., с който се създава Кралската прокуратура (Crown Prosecution Service) (вж. https://www.legislation.gov.uk/ukpga/1985/23/contents); Закона за данъчните и митническите служители (Commissioners for Revenue and Customs Act) от 2005 г., с който се установява Кралската данъчна и митническа служба (Her Majesty's Revenue and Customs) (вж. https://www.legislation.gov.uk/ukpga/2005/11/contents); Наказателно-процесуалния закон (Шотландия) (Criminal Procedure (Scotland) Act) от 1995 г., с който се създава Шотландската комисия за преразглеждане на наказателни дела (Scottish Criminal Cases Review Commission) (вж. https://www.legislation.gov.uk/ukpga/1995/46/contents); Закона за правосъдието (Северна Ирландия) (Justice (Northern Ireland) Act) от 2002 г., с който се създава прокуратурата на Северна Ирландия (Public Prosecution Service in Northern Ireland) (вж. https://www.legislation.gov.uk/ukpga/2002/26/contents) и Службата за борба с тежките измами (Serious Fraud Office), която е създадена и черпи правомощията си от Закона за наказателното правораздаване (Criminal Justice Act) от 1987 г. (вж. https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Например според информацията, предоставена от органите на Обединеното кралство, в рамките на прокуратурата (Crown Office and Procurator Fiscal Service), отговаряща за наказателното преследване в Шотландия, главният прокурор (Lord Advocate), който е ръководител на системата на наказателното преследване в Шотландия, черпи правомощията си да разследва смъртни случаи и да преследва престъпления от общото право, докато някои от функциите му са установени в нормативни актове. Освен това Короната, а оттам и различни държавни ведомства и министри също черпят своите правомощия от комбинация от законодателни актове, общо право и кралски изключителни права (това са правомощия по общото право, които са предоставени на Короната, но се упражняват от министрите).

([48]) Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел F: Правоприлагане, стр. 8 (вж. бележка под линия 9).

имат както правомощия, произтичащи от общото право, така и законоустановени правомощия ([49]) да изпълняват това задължение. Когато полицията разполага със законоустановени правомощия, те се ползват с приоритет спрямо всички правомощия по общото право ([50]).

(31) Обхватът на правомощията и задълженията на полицейския служител по общото право е признат от съдилищата като обхващащ „всички дейности, които според него са необходими за поддържането на мира, предотвратяването на престъпления или защитата на имуществото от престъпления“ ([51]). Правомощията по общото право не са безусловни. Те подлежат на редица ограничения, включително такива, установени от съдилищата ([52]) и от законодателството, по-специално Закона за правата на човека от 1998 г. и Закона за равенството от 2010 г. ([53]). Освен това за компетентните органи, обработващи данни съгласно част 3 от ЗЗД от 2018 г., това включва упражняване на правомощията по общото право в съответствие с изискванията на ЗЗД от 2018 г. ([54]). Също така при решението за извършване на какъвто и да било вид обработване на данни трябва да се вземат предвид изискванията съгласно приложимите насоки, като например Кодекса за поведение относно управлението на полицейска информация, както и насоките, специфични за някоя от държавите от Обединеното кралство ([55]). Правителството и оперативните полицейски служби издават редица ръководства, за да се гарантира, че полицейските служители упражняват своите правомощия във връзка с обработването на данни в границите, определени от общото право или съответния нормативен акт ([56]).

(32) Кралските изключителни права представляват друг компонент на „правото“ и се отнасят до определени правомощия, предоставени на Короната и упражнявани от изпълнителната власт, които не се основават на нормативен акт, а произтичат от суверенитета на монарха ([57]). Много малко са примерите за изключителни правомощия в контекста на правоприлагането. Те включват например рамката за правна взаимопомощ, с която се дава възможност за споделяне на данни от министър с трети държави за целите на правоприлагането, а правомощието за споделяне на данни по

([49]) Основните законодателни актове, с които се урежда режимът на главните полицейски правомощия (задържане, претърсване, разрешение за продължаване на задържане, снемане на пръстови отпечатъци, вземане на интимни проби, заповед за подслушване, достъп до комуникационни данни) са: i) за Англия и Уелс — Законът за полицията и доказателствата в наказателния процес от 1984 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1984/60/contents (изменен със Закона за защитата на свободите (Protection of Freedoms Act) от 2012 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2012/9/contents) и Законът за правомощията за разследване (Investigatory Powers Act) от 2016 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) за Шотландия — Законът за наказателното правораздаване (Шотландия) (Criminal Justice (Scotland) Act) от 2016 г., достъпен на следния адрес: https://www.legislation.gov.uk/asp/2016/1/contents, и Наказателно-процесуалният закон (Шотландия) от 1995 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1995/46/contents), iii) за Северна Ирландия — Наредба за полицията и доказателствата в наказателния процес (Северна Ирландия) (Police and Criminal Evidence (Northern Ireland) Order) от 1989 г., достъпна на следния адрес: https://www.legislation.gov.uk/nisi/1989/1341/contents

([50]) Органите на Обединеното кралство обясняват, че върховенството на законодателството отдавна е установено в Обединеното кралство, още от Решението по дело *Entick/Carrington* [1765] EWHC KB J98, в което се признава, че съществуват ограничения за упражняването на правомощия от страна на изпълнителната власт и се установява принципът, че правомощията по общото право и изключителните права на монарха и правителството са подчинени на местния закон.

([51]) Вж. дело *Rice/Connolly* [1966] 2 QB 414.

([52]) Вж. дело *R(Catt)/Association of Chief police Officers* [2015] AC 1065, по което във връзка с правомощията на полицията да получава и съхранява информация за лице (извършило престъпление) съдия Sumption счита, че съгласно общото право полицията има правомощието да получава и съхранява информация за полицейски цели, т.е. по-общо казано — за поддържането на обществения ред и предотвратяването и разкриването на престъпления. Тези правомощия не включват разрешение за използване на методи за получаване на информация, свързани с намеса, като например влизане в частна собственост или действия (различни от задържането съгласно правомощията по обичайното право), които биха представлявали нападение. Съдията намира, че в този случай правомощията по общото право са достатъчни, за да се разреши получаването и съхраняването на въпросния вид публична информация по тези жалби.

([53]) Закон за равенството (Equality Act) от 2010 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) Като пример за дело, при което правомощията на полицията по общото право се оценяват в рамките на ЗЗД от 1998 г., вж. решението на Висшия съд по дело *Bridges/the Chief Constable of South Wales Police* (вж. бележка под линия 33). Вж. също дела *Vidal-Hall/Google Inc* [2015] EWCA Civ 311 и *Richard/BBC* [2018] EWHC 1837 (Ch).

([55]) Вж. например насоките на полицейската служба на Северна Ирландия относно инструкцията за управлението на регистри, достъпни на следния адрес: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf

([56]) Камарата на общините публикува кратък информационен документ, в който се определят основните правомощия по общото право и основните законоустановени правомощия на полицията в Англия и Уелс (вж. https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf) Според този документ например, макар правомощията по поддържане на „мира в Кралството“ и „използването на сила“ да произтичат от общото право, „правомощията по спиране и претърсване“ винаги произтичат от нормативен акт. Освен това шотландското правителство предоставя на своя уебсайт информация относно полицейските правомощия по задържане и спиране и претърсване (вж. https://www.gov.scot/policies/police/police-powers/)

([57]) Според информацията, предоставена от органите на Обединеното кралство, изключителните правомощия, упражнявани от правителството, включват например изготвянето и ратифицирането на договори, провеждането на дипломация и използването на въоръжените сили в рамките на Обединеното кралство за поддържане на мира в подкрепа на полицията.

този начин невинаги е предвидено в нормативен акт ([58]). Кралските изключителни права са подчинени на принципите на общото право ([59]), а нормативните актове имат приоритет над тях, поради което за тях се прилагат ограниченията, предвидени в Закона за правата на човека от 1998 г. и ЗЗД от 2018 г. ([60]).

(33) Съгласно режима на Обединеното кралство, подобно на член 8 от Директива (ЕС) 2016/680, за да бъде спазен принципът на законосъобразност, от компетентните органи се изисква да осигурят, че обработването се основава на правото и че е „необходимо“ за изпълнението на задачата, осъществявана за целите на правоприлагането. ICO дава насоки в това отношение, като пояснява, че „това трябва да бъде целенасочен и пропорционален начин за постигане на целта. Обработването няма да бъде законосъобразно, ако целта може разумно да бъде постигната с други средства, които се характеризират с по-ниска степен на намеса. Не е достатъчно да се твърди, че обработването е необходимо, тъй като сте избрали да извършвате дейността си по определен начин. Въпросът е дали обработването е необходимо за посочената цел“ ([61]).

2.4.1.2. Обработване въз основа на „съгласието“ на субекта на данни

(34) Както е посочено в съображение 28, в член 35, параграф 2 от ЗЗД от 2018 г. се предвижда възможността да се обработват лични данни въз основа на „съгласието“ на физическото лице.

(35) Съгласието обаче не изглежда да е правно основание от значение за операциите по обработване, попадащи в обхвата на настоящото решение. Всъщност операциите по обработване, обхванати от настоящото решение, винаги ще се отнасят до данни, които са били предадени съгласно Директива (ЕС) 2016/680 от компетентен орган на държава членка на компетентен орган на Обединеното кралство. Поради това те обикновено няма да включват вида пряко взаимодействие (събиране) между публичен орган и субекти на данни, което може да се основава на съгласие съгласно член 35, параграф 2, буква а) от ЗЗД от 2018 г.

(36) Макар поради тази причина да се счита, че използването на съгласие не е от значение за оценката, извършвана съгласно настоящото решение, от съображения за изчерпателност следва да се отбележи, че в контекста на правоприлагането обработването никога не се основава единствено на съгласие, тъй като компетентният орган трябва винаги да има основно правомощие, което му позволява да обработва данните ([62]). По-конкретно, и подобно на това, което е разрешено съгласно Директива (ЕС) 2016/680 ([63]), това означава, че съгласието служи като допълнително условие за някои ограничени и специфични операции по обработване, които в противен случай не би било възможно да се извършат, например събирането и обработването на проба ДНК от физическо лице, което не е заподозряно. В този случай обработването няма да се извърши, ако не е дадено съгласие или ако то е било оттеглено ([64]).

([58]) В тази връзка вж. оценката на режима на Обединеното кралство за последващо предаване в съображения 74—87.

([59]) Вж. дело *Bancoult/Secretary of State for Foreign and Commonwealth Affairs* [2008] UKHL 61, по което съдът приема, че изключителното правомощие за издаване на укази в Съвета също подлежи на обичайните основания за съдебен контрол.

([60]) Вж. дело *Attorney-General/De Keyser's Royal Hotel Ltd* [1920] [1920] AC 508, по което съдът постановява, че изключителните правомощия не могат да се използват, когато ги заместват законоустановени правомощия; дело *Laker Airways Ltd/Department of Trade* [1977] QB 643, по което съдът решава, че изключителните правомощия не могат да се използват за осуетяване на законодателството; дело *R/Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3, по което съдът постановява, че не могат да се използват изключителни правомощия, когато те противоречат на приетото законодателство, дори когато това прието законодателство все още не е влязло в сила; дело *R (Miller)/Secretary of State for Exiting the European Union* [2017] UKSC 5, по което съдът потвърждава възможността да се коригират и отменят изключителни правомощия с нормативен акт. За общ преглед на връзката между кралските изключителни правомощия и нормативите актове или правомощията по общото право вж. краткия информационния документ на Камарата на общините, достъпен на следния адрес: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) Насоки за обработване на данни в областта на правоприлагането, „За какво се отнася първият принцип“ (Guide to Law Enforcement Processing, „What is the first principle about?“), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Това следва от формулировката на съответната разпоредба от ЗЗД от 2018 г., според която обработването на лични данни за всяка от целите на правоприлагането е законосъобразно само ако и до степен в която то е „въз основа на правото“ и ако или а) субектът на данни е дал съгласие за обработването за тази цел, или б) обработването е необходимо за изпълнението на задача, осъществявана за тази цел от компетентен орган.

([63]) Вж. съображения 35—37 от Директива (ЕС) 2016/680.

([64]) Органите на Обединеното кралство посочват като пример за случай, в който съгласието може да бъде подходящо основание за обработване, получаването на проба ДНК от полицията във връзка с изчезнало лице, за да се установи съвпадение с тяло, ако такова бъде открито. При такива обстоятелства би било неуместно полицията да принуди субекта на данни да представи проба; вместо това полицията ще поиска от лицето съгласие, което се дава свободно и може да бъде оттеглено по всяко време. Ако съгласието бъде оттеглено, данните не могат повече да бъдат обработвани, освен ако не бъде установено ново правно основание за продължаване на обработването на пробата (напр. ако субектът на данни се е превърнал в заподозряно лице). Друг пример би могъл да възникне, когато полицейска служба разследва престъпление, при което жертвата (може да става въпрос за жертва на грабеж, престъпление против половата неприкосновеност, домашно насилие, роднини в случай на убийство или друга жертва на престъпление) може да се възползва от насочване към службата за подкрепа за жертвите (независима благотворителна организация, посветена на подкрепата на хора, засегнати от престъпления и травматични инциденти). При такива обстоятелства полицията ще сподели със службата за подкрепа за жертвите само личните данни, като например името и координатите за връзка, ако жертвата е дала съгласие.

(37) В случаите, когато се изисква съгласието на физическото лице, това съгласие трябва да бъде недвусмислено и да включва ясно потвърждаващо действие ([65]). От полицейските служби се изисква да разполагат с декларация за поверителност, включваща, наред с другото, необходимата информация, свързана с валидното използване на съгласието. Освен това някои от тях публикуват допълнителни материали за това как спазват законодателството за защита на данните, включително как и кога биха използвали съгласието като правно основание ([66]).

2.4.1.3. Обработване на чувствителни данни

(38) Когато се обработват „специални категории данни“, следва да има специфични гаранции. В това отношение, подобно на предвиденото в член 10 от Директива (ЕС) 2016/680, в част 3 от ЗЗД от 2018 г. се предвиждат по-строги гаранции за така нареченото „обработване на чувствителни данни“ ([67]).

(39) Съгласно член 35, параграф 3 от ЗЗД от 1998 г. чувствителни данни може да бъдат обработвани от компетентните органи за целите на правоприлагането само в два случая: 1) субектът на данни е дал съгласието си за обработването за целите на правоприлагането и към момента на извършване на обработването администраторът има подходящ документ за политиката ([68]); или 2) обработването е строго необходимо за целите на правоприлагането, отговаря на поне едно от условията в приложение 8 към ЗЗД от 2018 г. и към момента на извършване на обработването администраторът има подходящ документ за политиката ([69]).

(40) Що се отнася до първия случай и както е обяснено в съображение 38, използването на съгласие не се счита за относимо с оглед на вида на прехвърлянето, което е предмет на настоящото решение ([70]).

(41) Когато обработването на чувствителни данни не се основава на съгласие, то може да се извърши при спазване на едно от условията, изброени в приложение 8 към ЗЗД от 2018 г. Тези условия са свързани с обработване, необходимо за законоустановени цели; правораздаване; защита на жизненоважните интереси на субекта на данни или на друго физическо лице, защита на деца и на лица, изложени на риск; правни претенции; съдебни актове; предотвратяване на измами; архивиране; когато личните данни явно са направени обществено достояние от субекта на данни. Освен случая, когато данните явно са направени обществено достояние, всички условия, предвидени в приложение 8, подлежат на проверка за изпълнение на критерия „строга необходимост“. Както е пояснено от ICO, „строго необходимо в този контекст означава, че обработването трябва да е свързано с належаща обществена нужда, която не

([65]) Няма отделно определение на понятието „съгласие“ за целите на обработването на лични данни съгласно част 3 от ЗЗД от 2018 г. ICO предостави насоки относно понятието „съгласие“ за целите на част 3 от ЗЗД от 2018 г., като поясни, че то има същото значение и следва да бъде приведено в съответствие с определението, предвидено в ОРЗД, а именно, че „съгласието трябва да бъде свободно изразено, конкретно и информирано и трябва да има реален избор за даване на съгласие за обработване на данните“ (Насоки за обработване на данни в областта на правоприлагането, „За какво се отнася първият принцип?“ (вж. бележка под линия 64) и Насоки за защита на данните относно съгласието (Guide to Data Protection on consent), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Вж. например информацията на уебстраницата на полицията в Линкълншир (https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) или на уебстраницата на полицията в Западен Йоркшир (вж. https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Член 35, параграф 8 от ЗЗД от 2018 г.

([68]) Член 35, параграф 4 от ЗЗД от 2018 г.

([69]) Член 35, параграф 5 от ЗЗД от 2018 г.

([70]) От съображения за изчерпателност следва да се отбележи, че когато обработването се основава на съгласие, съгласието трябва да бъде свободно изразено, конкретно и информирано и трябва да има конкретен избор за даване на съгласие за обработване на данните. Освен това при обработване въз основа на съгласието на субекта на данни от администратора се изисква да разполага с „подходящ документ за политиката“ (ПДП). В член 42 от ЗЗД от 2018 г. са посочени изискванията, на които трябва да отговаря ПДП. В него се пояснява, че документът трябва най-малкото да разяснява процедурите на администратора за гарантиране на спазването на принципите за защита на данните и да разяснява политиките на администратора по отношение на съхранението и изтриването на лични данни. Съгласно член 42 от ЗЗД от 2018 г. това означава, че администраторът трябва да представи документ, който а) обяснява процедурите на администратора за гарантиране на спазването на принципите за защита на данните; и б) разяснява политиката на администратора по отношение на съхранението и изтриването на лични данни, обработвани въз основа на съгласието на субекта на данни, или дава указания за вероятния срок на съхранение на тези лични данни. По-специално в документа за политиката се изисква от администратора, при спазване на задължението за документиране на дейностите по обработване, винаги да включва елементите, посочени в букви а) и б). ICO публикува образец (Насоки за обработване на данни в областта на правоприлагането, „Условия за обработване на чувствителни данни“) (Guide to Law Enforcement Processing, „Conditions for sensitive processing“), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) и може да предприеме действия по правоприлагане, ако администраторите не изпълняват тези изисквания. ПДП се разглежда и от съдилищата във връзка с евентуални нарушения на ЗЗД от 2018 г. Например по неотдавнашното дело *R (Bridges)/Chief Constable of South Wales Police* съдилищата са разгледали ПДП на администратора и са установили, че той е подходящ, но би било добре да съдържа допълнителни подробности. В резултат на това полицията в Южен Уелс преразгледа ПДП и го актуализира в съответствие с новите насоки на ICO (вж. бележка под линия 33). Освен това съгласно член 42, параграф 3 от ЗЗД от 2018 г. администраторът следва да извършва периодичен преглед на ПДП. Накрая, като допълнителна гаранция, съгласно член 42, параграф 4 от ЗЗД от 2018 г. от администратора се изисква да води разширен регистър на дейностите по обработване, който включва допълнителни елементи в сравнение с общото задължение на администратора да води документация за дейностите по обработване съгласно член 61 от ЗЗД от 2018 г.

можете разумно да постигнете със средства, които се характеризират с по-ниска степен на намеса“ ([71]). Освен това някои от условията са предмет на допълнителни ограничения. Например, за да се използват условията за „законоустановени цели“ и за „защита на деца и на лица, изложени на риск“ (приложение 8, точки 1 и 4), трябва да се приложи допълнителен критерий за наличие на важен обществен интерес. Освен това, що се отнася до условието за защита на деца (приложение 8, точка 4), субектът на данни също така трябва да е на определена възраст и да се счита за изложен на риск. Освен това администраторът може да приложи условието, предвидено в приложение 8, точка 4, само при специфични обстоятелства ([72]). Аналогично съществуват ограничения за условията „съдебни актове“ и „предотвратяване на измами“ (приложение 8, съответно точки 7 и 8). И двете са приложими само за определени администратори. Само съд или друг съдебен орган може да използва условието „съдебни актове“ и само администратори, които са организации за борба с измамите, могат да използват условието „предотвратяване на измами“.

(42) И накрая, когато обработването се основава на едно от условията, изброени в приложение 8 и съответно в член 42 от ЗЗД от 2018 г., трябва да има „подходящ документ за политиката“, в който се обясняват процедурите на администратора за гарантиране на спазването на принципите за защита на данните и политиките на администратора по отношение на съхранението и изтриването на лични данни, и се прилагат задълженията за водене на разширен регистър.

2.4.2. *Ограничаване в рамките на целта*

(43) Личните данни следва да се обработват с конкретна цел и впоследствие да се използват само дотолкова, доколкото употребата им не е несъвместима с целта на обработването. Този принцип на защита на данните е гарантиран от член 36 от ЗЗД от 2018 г. Съгласно тази разпоредба, подобно на член 4, параграф 1, буква б) от Директива (ЕС) 2016/680, се изисква а) целта, свързана с правоприлагането, за която се събират лични данни, във всеки един случай да бъде конкретна, изрично указана и легитимна, и б) така събраните лични данни да не се обработват по начин, който е несъвместим с целта, за която са били събрани.

(44) Когато компетентните органи обработват данни за целите на правоприлагането, това може да включва архивиране, научни или исторически изследвания и статистически цели ([73]). В тези случаи ЗЗД от 2018 г. пояснява също, че архивирането (или обработването за научни или исторически изследвания и статистически цели) не е разрешено, когато се извършва по отношение на решения, взети във връзка с конкретен субект на данни, или ако има вероятност да му причини значителни имуществени или неимуществени вреди ([74]).

2.4.3. *Точност и свеждане на данните до минимум*

(45) Данните трябва да бъдат точни и при необходимост да бъдат поддържани в актуален вид. Те трябва също така да са подходящи, относими и да не надхвърлят необходимото във връзка с целите, за които се обработват. Подобно на член 4, параграф 1, букви в), г) и д) от Директива (ЕС) 2016/680, тези принципи са гарантирани в членове 37 и 38 от ЗЗД от 2018 г. Трябва да се предприемат всички разумни стъпки, за да се гарантира, че неточните ([75])

([71]) Насоки за обработване на данни в областта на правоприлагането, „Условия за обработване на чувствителни данни“ (вж. бележка под линия 70).

([72]) Обработването се извършва без съгласието на субекта на данни, когато: а) субектът на данни не може да даде съгласие за обработването; б) от администратора не може разумно да се очаква да получи съгласието на субекта на данни за обработването; в) обработването трябва да се извършва без съгласието на субекта на данни, тъй като получаването на съгласието на субекта на данни би засегнало предоставянето на защитата, посочена в алинея 1, буква а).

([73]) Вж. член 41, параграф 1 от ЗЗД от 2018 г.

([74]) Вж. член 41, параграф 2 от ЗЗД от 2018 г.

([75]) Съгласно член 205 от ЗЗД от 2018 г. понятието „неточни“ означава „неточни или подвеждащи“ лични данни. Органите на Обединеното кралство обясняват, че по принцип данните, свързани с наказателни разследвания, често са непълни, но въпреки това те могат да бъдат точни.

лични данни се изтриват или коригират незабавно ([76]), като се взема предвид целта, свързана с правоприлагането, за която се обработват ([77]), и за да се гарантира, че лични данни, които са неточни, непълни или вече не са актуални, не се предават или предоставят за някоя от целите на правоприлагането ([78]).

(46) Освен това, подобно на член 7 от Директива (ЕС) 2016/680, режимът за защита на данните на Обединеното кралство предвижда, че доколкото е възможно, личните данни, основани на факти, трябва да се разграничават от личните данни, основани на лични оценки ([79]). Когато е уместно и доколкото е възможно, трябва да се прави ясно разграничение между личните данни, отнасящи се до различни категории субекти на данни, като заподозрени, осъдени за престъпление, пострадали от престъпление и свидетели ([80]).

2.4.4. *Ограничение на съхранението*

(47) Съгласно член 5 от Директива (ЕС) 2016/680 като общо правило данните следва да се съхраняват за период, не по-дълъг от необходимото за целите, за които личните данни се обработват. Съгласно член 39 от ЗЗД от 2018 г. и подобно на член 5 от посочената директива се забранява да се съхраняват лични данни, обработвани за която и да е от целите на правоприлагането, за период, по-дълъг от необходимото във връзка с целта, за която се обработват. Правният режим на Обединеното кралство изисква да бъдат определени подходящи срокове за периодичния преглед на необходимостта от продължаване на съхраняването на лични данни за всяка от целите на правоприлагането. Допълнителни правила относно практиките, свързани със съхранението на лични данни, и приложимите срокове са определени в съответното законодателство и насоките, уреждащи правомощията и функционирането на полицията. Например в Англия и Уелс Кодексът за поведение относно управлението на полицейска информация на Полицейския колеж и Ръководството за разрешена професионална практика относно управлението на полицейска информация осигуряват рамка за гарантиране на последователен процес на съхранение, преглед и унищожаване, основан на риска, за управлението на оперативната полицейска информация ([81]). Тази рамка определя ясни очаквания в рамките на службата относно начина, по който информацията следва да бъде създавана, споделяна, използвана и управлявана в отделните полицейски служби и други агенции и между тях ([82]). От полицията се очаква да спазва Кодекса за поведение, а съответствието се проверява от Кралския инспекторат на полицейските, противопожарните и спасителните служби ([83]).

(48) Полицейската служба на Северна Ирландия не е задължена по закон да спазва Кодекса за поведение относно управлението на полицейска информация. Рамката относно управлението на полицейска информация, приета през 2011 г., обаче е допълнена от Наръчник на полицейската служба на Северна Ирландия ([84]), в който се определят политики и процедури за начина, по който Кодексът за поведение относно управлението на полицейска информация се прилага в Северна Ирландия.

([76]) Член 38, параграф 1, буква b) от ЗЗД от 2018 г.

([77]) Съгласно Обяснителната рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита „това гарантира признаването както на правата на субектите на данни, така и на оперативните нужди на правоприлагащите органи. Този въпрос беше внимателно разгледан по време на етапите на изготвяне на законопроекта за защита на данните, тъй като може да има конкретни и ограничени оперативни причини, поради които данните не могат да бъдат коригирани. Най-често срещаният случай за това е при необходимост неточните лични данни да бъдат запазени в първоначалния им вид за доказателствени цели“ (вж. Обяснителната рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел F: Правоприлагане, стр. 21, вж. бележка под линия 9).

([78]) Член 38, параграф 4 от ЗЗД от 2018 г. Освен това съгласно член 38, параграф 5 от ЗЗД от 2018 г. качеството на личните данни трябва да бъде проверено, преди те да бъдат предадени или предоставени, при всяко предаване на лични данни се включва необходимата информация, позволяваща на получателя да оцени степента на точност, пълнота, надеждност и актуалност на данните, и ако след предаването на личните данни се окаже, че данните са били неточни или че предаването им е било незаконно, получателят трябва да бъде уведомен незабавно.

([79]) Член 38, параграф 2 от ЗЗД от 2018 г.

([80]) Член 38, параграф 3 от ЗЗД от 2018 г.

([81]) Тази рамка гарантира последователност при съхранението на получените лични данни. Периодът на преразглеждане зависи от престъпленията, които са разделени на четири групи: 1) някои въпроси, свързани с обществената защита; 2) други свързани с насилие и тежки престъпления против половата неприкосновеност; 3) всички други престъпления; 4) разни. Повече подробности могат да бъдат намерени в Ръководството за разрешена професионална практика относно управлението на полицейска информация (вж. бележка под линия 26).

([82]) Според информацията, предоставена от органите на Обединеното кралство, други организации могат да спазват принципите на Кодекса за поведение относно управлението на полицейска информация, ако желаят. Например Кралската данъчна и митническа служба и Националната агенция по престъпността доброволно приемат много от принципите на Кодекса за поведение относно управлението на полицейска информация, за да гарантират последователност в правоприлагането. Като цяло повечето организации ще предоставят на своите служители специфични политики и насоки за всички служители относно начина, по който да обработват лични данни като част от своите задължения, съобразени с конкретната организация. Това обикновено включва и задължително обучение.

([83]) Кодексът за поведение относно управлението на полицейска информация е издаден въз основа на правомощията, предвидени в Закона за полицията от 1996 г., който дава възможност на Полицейския колеж да издава кодекси за поведение, свързани с ефективното функциониране на полицията. Всеки кодекс за поведение, издаден съгласно посочения закон, трябва да бъде одобрен от министъра, като преди внасянето му в Парламента е необходимо да се проведе консултация с Националната агенция по престъпността. С член 39a, параграф 7 от Закона за полицията от 1996 г. се въвежда изискване полицията да отдава дължимото внимание на кодексите, издадени съгласно Закона за полицията от 1996 г.

([84]) Наръчник на полицейската служба на Северна Ирландия относно управлението на полицейска информация (PSNI MoPI Handbook), глави 1—6.

(49) В Шотландия полицейските служби използват стандартна оперативна процедура (СОП) за съхраняване на информация ([85]), която подпомага политиката за управление на информацията на полицейската служба на Шотландия ([86]). СОП определя специфични правила за съхранение на информацията, съхранявана от полицията на Шотландия.

(50) В допълнение към общото изискване за преглед на съхраняваната информация, което се прилага в цялото Обединено кралство, допълнителни подробности са предоставени в местни правила. Например в Англия и Уелс Законът за полицията и доказателствата в наказателния процес, изменен със Закона за защита на свободите от 2012 г., урежда съхранението на пръстови отпечатъци и ДНК профили, както и специален режим за лица, които не са осъдени ([87]). В Закона за защита на свободите беше създадена и длъжността комисар по въпросите на съхранението и използването на биометричен материал („комисарят по биометричните въпроси“) ([88]). Специфични правила относно фотографирането при задържане са изложени в Прегледа на фотографирането при задържане (Custody Image Review) от 2017 г. ([89]). В Шотландия Наказателно-процесуалният закон (Шотландия) от 1995 г. предвижда правила за получаване и съхранение на дактилоскопични и биологични проби ([90]). Подобно на Англия и Уелс, законодателството урежда съхранението на биометрични данни в различни случаи ([91]).

2.4.5. *Сигурност на данните*

(51) Личните данни трябва да се обработват по начин, който гарантира тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане. За тази цел публичните органи трябва да предприемат подходящи технически или организационни мерки за защита на личните данни от възможни заплахи. Тези мерки трябва да се оценяват, като се вземат предвид достиженията на техническия прогрес и съответните разходи.

(52) Тези принципи са отразени в член 40 от ЗЗД от 2018 г., съгласно който, подобно на член 4, параграф 1, буква е) от Директива (ЕС) 2016/680, личните данни, обработвани за целите на правоприлагането, трябва да се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, като се прилагат подходящи технически или организационни мерки. Това включва защита на данните срещу неразрешено или незаконосъобразно

([85]) Стандартна оперативна процедура (СОП) за съхраняване на информация (Record Retention Standard Operating Procedure), достъпна на следния адрес: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) За повече подробности относно управлението на информацията вж. информацията за Националните регистри на Шотландия, достъпна на следния адрес: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Сроковете за съхранение варират в зависимост от това дали дадено лице е било осъдено или не (членове 63I — 63KI от Закона за полицията и доказателствата в наказателния процес от 1984 г.). Например в случай на пълнолетно лице, осъдено за престъпление, подлежащо на вписване в регистрите за съдимост, неговите дактилоскопични отпечатъци и ДНК профил могат да бъдат съхранявани за неопределен срок (член 63I, параграф 2 от Закона за полицията и доказателствата в наказателния процес от 1984 г.). Съхранението на тези данни обаче ще бъде ограничено във времето, ако лицето е на възраст под 18 години, не е било осъждано преди и е осъдено за „леко“ престъпление, подлежащо на вписване в регистрите за съдимост (член 63K от Закона за полицията и доказателствата в наказателния процес от 1984 г.). В случай на задържано или обвинено лице, което не е било осъдено, данните се съхраняват за период до три години (член 63F от Закона за полицията и доказателствата в наказателния процес от 1984 г.). Удължаването на този срок за съхранение трябва да бъде одобрено от съдебен орган (член 63F, параграф 7 от Закона за полицията и доказателствата в наказателния процес от 1984 г.). Съхранението на данните не е възможно в случай на лица, които са задържани или обвинени в леко престъпление, но не са осъдени (член 63D и член 63H от Закона за полицията и доказателствата в наказателния процес от 1984 г.).

([88]) С член 20 от Закона за защита на свободите от 2012 г. се създава длъжността на комисаря по биометричните въпроси. Наред с други функции комисарят по биометричните въпроси решава дали полицията може да съхранява ДНК профили и пръстови отпечатъци, снети от задържани лица, които не са обвинени в квалифицирано престъпление (член 63G от Закона за полицията и доказателствата в наказателния процес от 1984 г.). Освен това комисарят по биометричните въпроси носи обща отговорност да контролира съхранението и използването на ДНК и пръстови отпечатъци, както и за съхранението им на основания, свързани с националната сигурност (член 20, параграф 2 от Закона за защита на свободите от 2012 г.). Комисарят по биометричните въпроси се назначава съгласно Кодекса за управление на публичните назначения (Кодексът е достъпен на следния адрес: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) и условията за назначаването му ясно показват, че той може да бъде отстранен от длъжност от министъра на вътрешните работи само при строго определен набор от обстоятелства; сред тях са неизпълнение на задълженията му в продължение на три месеца, осъждане за престъпление или неизпълнение на условията за неговото назначаване.

([89]) Преглед на използването и съхранението на изображения, снети при задържане (Review of the Use and Retention of Custody Images), достъпен на следния адрес: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) Член 18 и следващи от Наказателно-процесуалния закон (Шотландия) от 1995 г.

([91]) Сроковете за съхранение варират в зависимост от това дали лицето е осъдено (член 18, параграф 3 от Наказателно-процесуалния закон (Шотландия) от 1995 г.) или е непълнолетно. В последния случай срокът за съхранение е 3 години от присъдата на съда за непълнолетни (член 18E, параграф 8 от Наказателно-процесуалния закон (Шотландия) от 1995 г.). Данните на арестувани, но неосъдени лица не могат да бъдат съхранявани (член 18, параграф 3 от Наказателно-процесуалния закон (Шотландия) от 1995 г.), освен в конкретни случаи и в зависимост от тежестта на престъплението (член 18A от Наказателно-процесуалния закон (Шотландия) от 1995 г.). Със Закона за комисаря по биометричните въпроси на Шотландия (Scottish Biometrics Commissioner Act) от 2020 г. (вж. https://www.legislation.gov.uk/asp/2020/8/contents) се създава длъжността на комисаря по биометричните въпроси на Шотландия, който трябва да изготви и преразгледа кодекси за поведение (одобрени от парламента на Шотландия) относно получаването, съхранението, използването и унищожаването на биометрични данни за целите на наказателното правораздаване и дейността на полицията (член 7 от Закона за комисаря по биометричните въпроси на Шотландия от 2020 г.).

обработване и срещу случайна загуба, унищожаване или повреждане ([92]). В член 66 от ЗЗД от 2018 г. допълнително се уточнява, че всеки администратор и всеки обработващ лични данни трябва да прилагат подходящи технически и организационни мерки, за да гарантират ниво на сигурност, съответстващо на рисковете, произтичащи от обработването на лични данни. Съгласно обяснителните бележки администраторът трябва да оцени рисковете и да приложи подходящи мерки за сигурност въз основа на тази оценка, например криптиране или специфични нива на разрешение за достъп за персонала, обработващ данните ([93]). При оценката трябва също така да се вземат предвид, например, естеството на обработваните данни и всички други значими фактори или обстоятелства, които биха могли да засегнат сигурността на обработването.

(53) Режимът, уреждащ спазването на принципите за сигурност на данните, е много подобен на режима, установен в членове 29—31 от Директива (ЕС) 2016/680. По-специално, в случай на нарушение на сигурността на личните данни във връзка с лични данни, за които администраторът носи отговорност, съгласно член 67, параграф 1 от ЗЗД от 2018 г. администраторът трябва, без излишно забавяне и когато това е осъществимо, в рамките на 72 часа, след като е узнал за нарушението, да уведоми комисаря по информацията за нарушението на сигурността на личните данни ([94]). Задължението за уведомяване не се прилага, ако няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица ([95]). Администраторът трябва да документира фактите, свързани с всяко нарушение на сигурността на личните данни, последиците от него и предприетите действия за справяне с него по начин, който дава възможност на комисаря по информацията да провери съответствието със ЗЗД ([96]). Ако обработващият лични данни узнае за нарушение на сигурността, той трябва да уведоми администратора без излишно забавяне ([97]).

(54) Съгласно член 68, параграф 1 от ЗЗД от 2018 г., когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическите лица, администраторът трябва да съобщи на субекта на данни за нарушението без излишно забавяне ([98]). Съобщението трябва да съдържа същата информация като уведомлението до комисаря по информацията, описано в съображение 53. Това задължение не се прилага, ако администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението. То също така не се прилага, ако администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се материализира високият риск за правата и свободите на субектите на данни. И накрая, администраторът не е длъжен да уведомява субекта на данни, ако това то би довело до непропорционални усилия ([99]). В този случай информацията трябва да бъде предоставена на разположение на субекта на данни по друг също толкова ефективен начин, например чрез публично съобщение ([100]). Ако администраторът не е информирал субекта на данни за нарушението, комисарят по информацията, след като е бил уведомен съгласно раздел 67 от ЗЗД и след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, може да изиска от администратора да съобщи на субекта на данни за нарушението ([101]).

([92]) В съответствие с обяснителните бележки към ЗЗД от 2018 г. (вж. бележка под линия 45) администраторът трябва по-специално: да проектира и организира сигурността на личните данни с оглед на естеството им и на вредите, които може да настъпят вследствие на нарушение на сигурността; да определи ясно кой отговаря за гарантирането на сигурността на информацията в рамките на неговата организация; да гарантира, че разполага с необходимата физическа и техническа сигурност, подкрепена от надеждни политики и процедури и надежден и добре обучен персонал; и да бъде готов да реагира бързо и ефективно на всяко нарушение на сигурността.

([93]) Параграф 221 от обяснителните бележки към ЗЗД от 2018 г. (вж. бележка под линия 45).

([94]) В член 67, параграф 4 от ЗЗД от 2018 г. се предвижда, че уведомлението трябва да включва описание на естеството на нарушението на сигурността на личните данни (включително, когато е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни), името и координатите за връзка на точка за контакт, описание на евентуалните последици от нарушението на сигурността на личните данни и описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни (включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици от него).

([95]) Член 67, параграф 2 от ЗЗД от 2018 г.

([96]) Член 67, параграф 6 от ЗЗД от 2018 г.

([97]) Член 67, параграф 9 от ЗЗД от 2018 г.

([98]) Съгласно член 68, параграф 7 от ЗЗД от 2018 г. администраторът може да ограничи изцяло или частично предоставянето на информация на субекта на данни, до такава степен и за толкова време, за колкото тази мярка е необходима и пропорционална, като се вземат предвид основните права и легитимните интереси на субекта на данни, за да а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури; б) не се допусне неблагоприятно влияние върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания; в) се защити обществената сигурност; г) се защити националната сигурност; д) се защитят правата и свободите на други лица.

([99]) Член 68, параграф 3 от ЗЗД от 2018 г.

([100]) Член 68, параграф 5 от ЗЗД от 2018 г.

([101]) Член 68, параграф 6 от ЗЗД от 2018 г., предмет на ограничението, предвидено в член 68, параграф 8 от ЗЗД от 2018 г.

2.4.6. *Прозрачност*

(55) Субектите на данни трябва да бъдат информирани за основните характеристики на обработването на техните лични данни. Този принцип на защита на данните е отразен в член 44 от ЗЗД от 2018 г., в който, подобно на член 13 от Директива (ЕС) 2016/680, се предвижда, че администраторът има общо задължение да предоставя на субектите на данни информация относно обработването на техните лични данни (чрез предоставяне на свободно достъпна за обществеността информация или по друг начин) ([102]). Информацията, която се изисква да бъде предоставена, включва а) данни за идентифициране и координатите за връзка на администратора; б) координатите за връзка на длъжностното лице по защита на данните, когато е приложимо; в) целите, за които администраторът обработва лични данни; г) съществуването на права на субектите на данни да изискват от администратора достъп до, коригиране или изтриване на лични данни и ограничаване на обработването им; и д) съществуването на право да бъде подадена жалба до комисаря по информацията и координатите за връзка с комисаря ([103]).

(56) Администраторът трябва също така да предостави на субекта на данни, в конкретни случаи и с цел да му се даде възможност да упражни правата си по ЗЗД от 2018 г. (например когато обработваните лични данни са били събрани без знанието на субекта на данни), информация относно а) правното основание на обработването; б) срока, за който ще се съхраняват личните данни, а ако това е невъзможно — критериите, използвани за определяне на този срок; в) когато е приложимо, категориите получатели на личните данни (включително получатели в трети държави или международни организации); г) допълнителна информация, необходима за упражняването на правата на субекта на данни съгласно част 3 от ЗЗД от 2018 г. ([104]).

2.4.7. *Индивидуални права*

(57) На субектите на данни трябва да бъдат предоставени редица приложими права. Глава 3, част 3 от ЗЗД от 2018 г. предоставя на физическите лица права на достъп, коригиране, изтриване и ограничаване ([105]), които са сравними с предвидените в глава 3 от Директива (ЕС) 2016/680.

(58) Правото на достъп е уредено в член 45 от ЗЗД от 2018 г. Първо, дадено физическо лице има право да получи потвърждение от администратора дали неговите лични данни се обработват или не ([106]). Второ, когато се обработват лични данни, субектът на данни има право да получи достъп до тези данни и следната информация относно обработването: а) целите и правното основание за обработването; б) обработваните категории данни; в) получателя, пред когото са разкрити данните; г) срока, за който ще се съхраняват личните данни; д) съществуването на право на субекта на данни да изиска коригиране и изтриване на лични данни; е) правото да се подаде жалба; и ж) всякаква налична информация относно произхода на съответните лични данни ([107]).

(59) Съгласно член 46 от ЗЗД от 2018 г. субектът на данни има право да изиска от администратора да коригира неточни лични данни, отнасящи се до него. Администраторът трябва да коригира данните (или когато данните са неточни, защото са непълни, да ги допълни) без излишно забавяне. Ако личните данни трябва да се съхраняват за доказателствени цели, администраторът трябва (вместо да коригира личните данни) да ограничи обработването им ([108]).

([102]) В Насоките за обработване на данни в областта на правоприлагането е даден следният пример: „На Вашия уебсайт има обща декларация за поверителност, която съдържа основна информация за организацията, целта, за която обработвате лични данни, правата на субекта на данни и правото му да подаде жалба до комисаря по информацията. Вие сте получили сведения, че дадено лице е присъствало при извършването на престъпление. При първия разговор с това лице трябва да му предоставите общата информация, както и допълнителна подкрепяща информация, за да му дадете възможност да упражни правата си. Можете да ограничите информацията за добросъвестно обработване, която предоставяте, само ако тя ще се отрази неблагоприятно върху разследването, което предприемате“ (Насоки за обработване на данни в областта на правоприлагането, „Каква информация трябва да предоставим на дадено лице?“ (Guide to Law Enforcement Processing, „What information should we supply to an individual?“), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) В Насоките за обработване на данни в областта на правоприлагането се посочва, че предоставената информация относно обработването на лични данни трябва да бъде сбита, разбираема и леснодостъпна; написана на ясен и разбираем език, адаптиран към нуждите на уязвимите лица, като например децата; и безплатна (Насоки за обработване на данни в областта на правоприлагането, „Как да предоставим тази информация?“ (Guide to Law Enforcement Processing, „How should we provide this information?“), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Член 44, параграф 2 от ЗЗД от 2018 г.

([105]) За подробен анализ на правата на субектите вж. Насоки за обработване на данни в областта на правоприлагането във връзка с индивидуалните права, достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) Член 45, параграф 1 от ЗЗД от 2018 г.

([107]) Член 45, параграф 2 от ЗЗД от 2018 г.

([108]) Член 46, параграф 4 от ЗЗД от 2018 г.

(60) Член 47 от ЗЗД от 2018 г. предоставя на физическите лица право на изтриване и ограничаване на обработването. Администраторът трябва ([109]) да изтрие личните данни без излишно забавяне, когато обработването на личните данни би нарушило някой от принципите за защита на данните, правните основания за обработването или гаранциите, свързани с архивирането и обработването на чувствителни данни. Администраторът трябва също така да изтрие данните, ако има правно задължение да направи това. Ако личните данни трябва да се съхраняват за доказателствени цели, администраторът трябва (вместо да изтрие личните данни) да ограничи обработването им ([110]). Администраторът трябва да ограничи обработването на лични данни, ако субектът на данни оспорва точността на личните данни, но не е възможно да се установи дали те са точни или не ([111]).

(61) Когато субект на данни поиска коригиране или изтриване на лични данни или ограничаване на обработването им, администраторът трябва писмено да уведоми субекта на данни дали искането е удовлетворено, а при отказ — да информира субекта на данни за причините за отказа и за наличните възможности за правна защита (правото на субекта на данни да отправи искане до комисаря по информацията да разследва дали ограничението е било приложено законно, правото да подаде жалба до комисаря по информацията и правото да поиска от съда заповед за изпълнение) ([112]).

(62) Когато администраторът коригира лични данни, получени от друг компетентен орган, той трябва да уведоми другия орган ([113]). Когато администраторът коригира, изтрие или ограничи обработването на лични данни, които са били разкрити от администратора, администраторът трябва да уведоми получателите, а получателите трябва също така да коригират, изтрият или ограничат обработването на личните данни (доколкото те запазват отговорността си за тях) ([114]).

(63) Освен това субектът на данни има право да бъде информиран без излишно забавяне от администратора за нарушение на сигурността на личните данни, когато има вероятност то да породи висок риск за правата и свободите на физическите лица ([115]).

(64) По отношение на всички тези права на субекта на данни и подобно на предвиденото в член 12 от Директива (ЕС) 2016/680 администраторът е длъжен да гарантира, че всяка информация, която се предоставя на субекта на данни, е в сбита, разбираема и леснодостъпна форма ([116]) и при възможност се предоставя в същата форма като тази на искането ([117]). Администраторът трябва да изпълни искането на субекта на данни без излишно забавяне или във всички случаи, като общо правило, в срок от един месец от искането ([118]). Когато администраторът има основателни опасения във връзка със самоличността на дадено лице, той може да поиска допълнителна информация и да отложи разглеждането на искането до установяването на самоличността. Администраторът може да начисли такса в разумен размер или да откаже да предприеме действия, когато счете искането за очевидно неоснователно ([119]). ICO предостави насоки за това кога дадено искане се счита за очевидно неоснователно или прекомерно и кога може да бъде начислена такса ([120]).

(65) Освен това съгласно член 53, параграф 4 от ЗЗД от 2018 г. министърът може с наредба да определи максималния размер на таксата.

([109]) Субектът на данни може да поиска от администратора да изтрие лични данни или да ограничи обработването им (но задълженията на администратора за изтриване на данните или ограничаване на обработването им се прилагат независимо от това дали е направено такова искане).

([110]) Член 46, параграф 4 и член 47, параграф 2 от ЗЗД от 2018 г.

([111]) Член 47, параграф 3 от ЗЗД от 2018 г.

([112]) Член 48, параграф 1 от ЗЗД от 2018 г.

([113]) Член 48, параграф 7 от ЗЗД от 2018 г.

([114]) Член 48, параграф 9 от ЗЗД от 2018 г.

([115]) Член 68 от ЗЗД от 2018 г.

([116]) Член 52, параграф 1 от ЗЗД от 2018 г.

([117]) Член 52, параграф 3 от ЗЗД от 2018 г.

([118]) Член 54 от ЗЗД от 2018 г. съдържа определение на понятието „приложим срок“, което означава срок от един месец или по-дълъг срок, който може да бъде посочен в наредби, считано от съответния момент (когато администраторът получи въпросното искане; когато администраторът получи информацията (ако има такава), поискана във връзка с искане по член 52, параграф 4 от ЗЗД; или когато се плати таксата (ако има такава), начислена във връзка с искането по член 53 от ЗЗД.

([119]) Член 53, параграф 1 от ЗЗД от 2018 г.

([120]) Съгласно насоките на ICO администраторът може да реши да начисли такса на субекта на данни, ако искането на последния е очевидно неоснователно или прекомерно, но все пак избере да отговори на него. Таксата трябва да бъде в разумен размер и да съответства на направените разходи. Насоки за обработване на данни в областта на правоприлагането, „Очевидно неоснователни и прекомерни искания“ (Guide to Law Enforcement Processing „Manifestly unfounded and excessive requests“), достъпни на следния адрес: 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. Ограничения на правата на субекта на данни и задължения за прозрачност

(66) При определени обстоятелства компетентен орган може да ограничи някои права на субекта на данни: правото на достъп ([121]), на информация ([122]), да бъде уведомен за нарушение на сигурността на личните данни ([123]) и да бъде информиран за причината за отказ на искане за коригиране или изтриване на данни ([124]). Подобно на режима, който се съдържа в глава III от Директива (ЕС) 2016/680, компетентният орган може да прилага ограничението само когато то е необходимо и пропорционално, като се вземат предвид основните права и легитимните интереси на субекта на данни, за да: а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури; б) не се допусне неблагоприятно влияние върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания; в) се защити обществената сигурност; г) се защити националната сигурност; д) се защитят правата и свободите на други лица.

(67) ICO предостави насоки за прилагането на тези ограничения. Съгласно тези насоки администраторите трябва да извършат анализ на всеки отделен случай, за да постигнат баланс между правата на лицето и вредата, която би настъпила в резултат на разкриването. По-специално те трябва да обосноват необходимостта и пропорционалността на всяко прилагано ограничение и могат да ограничат предоставяната информация само ако това би засегнало горепосочените цели ([125]).

(68) Съществуват и редица други насоки, издадени от компетентните органи, които предоставят подробна информация относно всички аспекти на законодателството за защита на данните, включително относно прилагането на ограниченията на правата на субектите на данни ([126]). Например в Наръчника за защита на данните на Националния съвет на началниците на полицията се посочва следното по отношение на член 45, параграф 4: „Важно е да се отбележи, че ограниченията могат да се прилагат само доколкото и докато е необходимо. Следователно не се допуска общо прилагане на ограничението по отношение на всички лични данни на заявителя или постоянно прилагане на ограничението. По последния въпрос често е необходимо личните данни, събрани без знанието на субект на данни, който е заподозрян в рамките на разследване, първоначално да бъдат защитени от разкриване пред него, за да се избегне неблагоприятно влияние върху разследването, докато то е в ход, но на по-късен етап не биха настъпили вреди от разкриването им, ако те са били разкрити пред лицето по време на разпит. Полицейските служби трябва да приемат процедури, които гарантират, че прилагането на тези ограничения е само в необходимата степен и само за необходимия срок“ ([127]). В споменатите насоки се дават и примери за това в кои случаи е вероятно да се приложи всяко едно от ограниченията ([128]).

(69) Освен това във връзка с възможността за ограничаване на което и да е от горепосочените права за защита на „националната сигурност“ администраторът може да подаде заявление за удостоверение, подписано от министър или от главния прокурор (или генералния адвокат на Шотландия), удостоверяващо, че ограничаването на тези права представлява необходима и пропорционална мярка за защита на националната сигурност ([129]). Правителството на Обединеното кралство издаде насоки относно удостоверенията за национална сигурност съгласно ЗЗД от 2018 г., в които по-специално се подчертава, че всяко ограничаване на правата на субектите на данни с цел опазване на националната сигурност трябва да бъде пропорционално и необходимо ([130]) (за повече информация относно удостоверенията за национална сигурност вж. съображения 131—134).

([121]) Член 45, параграф 4 от ЗЗД от 2018 г.

([122]) Член 44, параграф 4 от ЗЗД от 2018 г.

([123]) Член 68, параграф 7 от ЗЗД от 2018 г.

([124]) Член 48, параграф 3 от ЗЗД от 2018 г.

([125]) Вж. например Насоки за обработване на данни в областта на правоприлагането във връзка с правото на достъп, достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8

([126]) Вж. например Наръчник за защита на данните за полицейски специалисти в областта на защитата на данните, издаден от Националния съвет на началниците на полицията (вж. бележка под линия 27), или насоките, предоставени от Службата за борба с тежките измами, достъпни на следния адрес: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/

([127]) Наръчник за защита на данните на Националния съвет на началниците на полицията (Data protection Manual of the National Police Chief Counsel), стр. 140 (вж. бележка под линия 27).

([128]) В Наръчника за защита на данните на Националния съвет на началниците на полицията се посочва, че целта „да се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури“ е вероятно да е от значение за личните данни, обработвани във връзка с искания за информация, съдебни производства по семейни дела, дисциплинарни проверки, които нямат наказателноправен характер, и разследвания, като например независимото разследване във връзка със сексуалното насилие над деца; докато „защитата на правата и свободите на други лица“ е от значение за личните данни, които биха се отнасяли както за заявителя, така и за други лица“ (Наръчник за защита на данните на Националния съвет на началниците на полицията, стр. 140, вж. бележка под линия 27).

([129]) Член 79 от ЗЗД от 2018 г.

([130]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност (UK Government Guidance on National Security Certificates), достъпни на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Освен това, когато се прилага ограничение на правото на субект на данни, компетентният орган трябва без излишно забавяне да информира субекта на данни, че правата му са били ограничени, за причините за ограничението и за наличните възможности за правна защита, освен ако предоставянето на тази информация би подкопало причината за прилагане на ограничението ([131]). Като допълнителна гаранция срещу злоупотребата с ограничения администраторът трябва да документира причините за ограничаване на информацията и при поискване да предостави записа на комисаря по информацията ([132]).

(71) Ако администраторът откаже да предостави допълнителна информация, свързана с прозрачността, или откаже да предостави достъп или да изпълни искане за коригиране или изтриване на данни, или за ограничаване на обработването, лицето може да поиска от комисаря по информацията да разследва дали администраторът е приложил ограничението в съответствие със закона ([133]). Засегнатото лице може също така да подаде жалба до комисаря по информацията или да поиска от съда да разпореди на администратора да изпълни искането ([134]).

2.4.7.2. Автоматизирано вземане на решения

(72) Членове 49 и 50 от ЗЗД от 2018 г. обхващат съответно правата, свързани с автоматизираното вземане на решения, и гаранциите, които трябва да се прилагат ([135]). Подобно на член 11 от Директива (ЕС) 2016/680, администраторът може да вземе важно решение, основаващо се единствено на автоматизирано обработване на лични данни, само ако това се изисква или разрешава от закона ([136]). Решението е важно, ако би породило неблагоприятни правни последици за субекта на данни или би засегнало значително субекта на данни ([137]).

(73) Когато администраторът е задължен или оправомощен по закон да вземе важно решение, член 50 от ЗЗД от 2018 г. определя гаранциите, които ще се прилагат по отношение на такова решение (което е определено като „отговарящо на условията важно решение“). Администраторът трябва, веднага щом това е разумно осъществимо, да уведоми субекта на данни, че е взето такова решение. След това в рамките на един месец субектът на данни може да поиска от администратора да преразгледа решението или да вземе ново решение, което не се основава единствено на автоматизирано обработване. Администраторът трябва да разгледа искането и да информира субекта на данни за резултата от това разглеждане. ЗЗД от 2018 г. предоставя на министъра правомощието да приема наредби за допълнителни гаранции ([138]). Такива наредби все още не са приети.

2.4.8. *Последващо предаване*

(74) Нивото на защита на личните данни, предавани от правоприлагащ орган на държава членка на правоприлагащ орган на Обединеното кралство, не трябва да бъде подкопавано от по-нататъшно предаване на такива данни на получатели в трета държава. Подобно „последващо предаване“, което от гледна точка на правоприлагащ орган на Обединеното кралство представлява международно предаване на данни от Обединеното кралство, следва да бъде разрешено само когато новият получател извън Обединеното кралство също е обвързан от правила, гарантиращи ниво на защита, сходно с това в правния ред на Обединеното кралство.

([131]) Член 44, параграфи 5 и 6: Член 45, параграфи 5 и 6; Член 48, параграф 4 от ЗЗД от 2018 г.

([132]) Член 44, параграф 7; Член 45, параграф 7; член 48, параграф 6 от ЗЗД от 2018 г.

([133]) Член 51 от ЗЗД от 2018 г.

([134]) Член 167 от ЗЗД от 2018 г.

([135]) Що се отнася до обхвата на автоматизираното обработване, в обяснителните бележки към ЗЗД от 2018 г. се посочва, че: „тези разпоредби се отнасят до напълно автоматизираното вземане на решения, а не до автоматизираното обработване. Автоматизирано обработване (включително профилиране) е налице, когато дадена операция се извършва върху данни, без да е необходима човешка намеса. То се използва редовно в правоприлагането за филтриране на големи набори от данни до управляеми количества, които да се използват от човек оператор. Автоматизираното вземане на решения е форма на автоматизирано обработване и изисква окончателното решение да се взема без човешка намеса“. (Обяснителни бележки към ЗЗД, параграф 204, вж. бележка под линия 45).

([136]) В допълнение към защитата, предвидена в ЗЗД, съществуват и други законодателни ограничения в правната рамка на Обединеното кралство, които се прилагат за правоприлагащите агенции и биха предотвратили автоматизираното обработване (включително профилирането), което води до незаконна дискриминация. Със Закона за правата на човека от 1998 г. правата, съдържащи се в ЕКПЧ, се въвеждат в правото на Обединеното кралство, включително забраната за дискриминация съгласно член 14 от Конвенцията. По същия начин Законът за равенството от 2010 г. забранява дискриминацията на хора въз основа на защитени признаци (които включват пол, раса, увреждане и т.н.).

([137]) Член 49, параграф 2 от ЗЗД от 2018 г.

([138]) Член 50, параграф 4 от ЗЗД от 2018 г.

(75) Режимът на Обединеното кралство по отношение на международното предаване на данни се урежда от глава 5, част 3 от ЗЗД от 2018 г. ([139]) и отразява подхода, възприет в глава V от Директива (ЕС) 2016/680. По-специално, за да предаде лични данни на трета държава, компетентният орган трябва да отговаря на три условия: а) предаването трябва да е необходимо за целите на правоприлагането; б) предаването трябва да се основава на: i) наредба относно адекватното ниво на защита по отношение на третата държава, ii) ако не се основава на наредба относно адекватното ниво на защита, то трябва да се основава на наличието на подходящи гаранции, или iii) ако не се основава на решение относно адекватното ниво на защита или подходящи гаранции, то трябва да се основава на специални обстоятелства; и в) получателят на предаването трябва да бъде: i) съответен орган (т.е. еквивалентен на компетентния орган) в третата държава; ii) „съответна международна организация“, например международен орган, който изпълнява функции, съответстващи на някоя от целите на правоприлагането; или iii) лице, различно от съответния орган, но само когато предаването е строго необходимо за изпълнението на една от целите на правоприлагането; не е налице предимство на основни права и свободи на съответния субект на данни пред обществения интерес, изискващ предаването; предаването на личните данни на съответния орган в третата държава би било неефективно или неподходящо; и получателят е информиран за целите, за които данните могат да бъдат обработвани ([140]).

(76) Разпоредбите относно адекватното ниво на защита по отношение на трета държава, територия или сектор в трета държава, международна организация или описание ([141]) на такава държава, територия, сектор или организация се приемат от министъра. Що се отнася до стандарта, който трябва да бъде спазен, министърът трябва да прецени дали такава територия/сектор/организация осигурява адекватно ниво на защита на личните данни. В член 74а, параграф 4 от ЗЗД от 2018 г. се уточнява, че за тази цел министърът трябва да вземе предвид редица елементи, които са отражение на елементите, изброени в член 36 от Директива (ЕС) 2016/680 ([142]). В това отношение, след края на преходния период, част 3 от ЗЗД от 2018 г. представлява „произтичащото от правото на ЕС национално законодателство“, което, както беше обяснено, ще бъде тълкувано от съдилищата на Обединеното кралство в съответствие с приложимата съдебна практика на Съда, датираща отпреди излизането на Обединеното кралство от Съюза, и общите принципи на правото на Съюза, тъй като те са били в сила непосредствено преди края на преходния период. Това включва стандарта за „равностойност по същество“, който съответно ще се прилага за оценките на адекватното ниво на защита, извършвани от органите на Обединеното кралство.

(77) Що се отнася до процедурата, спрямо наредбите се прилагат „общите“ процесуални изисквания, предвидени в член 182 от ЗЗД от 2018 г. В рамките на тази процедура, когато предлага да се приемат бъдещи наредби на

([139]) Тази нова рамка се прилага след края на преходния период, включително правомощието на министъра да приема наредби относно адекватното ниво на защита. Въпреки това в наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения (по-специално точки 10—12 от приложение 21, вмъкнато в ЗЗД от 2018 г. с тези наредби) се предвижда, че определени предавания на лични данни в края на преходния период и след него се третират така, сякаш се основават на наредби относно адекватното ниво на защита. Тези предавания включват предавания към трети държави, които са обект на решение на ЕС относно адекватното ниво на защита в края на преходния период, и към държави — членки на ЕС, държави от ЕАСТ и територията на Гибралтар на основание на прилагането от тяхна страна на Директивата относно правоприлагането в областта на защитата на данните при обработването на данни в областта на правоприлагането (държавите от ЕАСТ прилагат Директива (ЕС) 2016/680 в резултат на задълженията си съгласно достиженията на правото от Шенген). Това означава, че в края на преходния период предаването на данни към тези държави може да продължи както преди напускането на ЕС. След края на преходния период министърът трябва да извърши преглед на констатациите за адекватно ниво на защита в срок от четири години.

([140]) Членове 73 и 77 от ЗЗД от 2018 г.

([141]) Органите на Обединеното кралство обясниха, че описанието на дадена държава или международна организация се отнася до ситуация, при която би било необходимо да се направи специфично и частично определяне на адекватността с целенасочени ограничения (напр. наредба относно адекватното ниво на защита по отношение само на определен вид предаване на данни).

([142]) Вж. член 74а, параграф 4 от ЗЗД от 2018 г., в който се предвижда, че при оценяване на адекватността на нивото на защита „министърът трябва по-специално да вземе предвид а) върховенството на закона, спазването на правата на човека и основните свободи, съответното законодателство — както общо, така и секторно, включително в областта на обществената сигурност, отбраната, националната сигурност и наказателното право и достъпа на публичните органи до лични данни, а също и прилагането на това законодателство, правилата за защита на данните, професионалните правила и мерките за сигурност, включително правилата за последващо предаване на лични данни на друга трета държава или международна организация, които са в сила във въпросната държава или международна организация, съдебната практика, както и наличието на ефективни и приложими права на субектите на данни и ефективни административни и съдебни средства за защита за субектите на данни, чиито лични данни се предават, б) наличието и ефективното функциониране на един или повече независими надзорни органи във въпросната трета държава, или органи, на чийто надзор подлежи дадена международна организация, отговорни за осигуряване и привеждане в изпълнение на правилата за защита на данните, включително адекватни изпълнителни правомощия, за подпомагане и консултиране на субектите на данни при упражняването на техните права и за сътрудничество с комисаря, и в) международните ангажименти, които съответната трета държава или международна организация е поела, или други задължения, произтичащи от правно обвързващи конвенции или инструменти, както и от участието ѝ в многостранни или регионални системи, по-конкретно по отношение на защитата на личните данни.“

Обединеното кралство относно адекватното ниво на защита ([143]), министърът трябва да се консултира с комисаря по информацията. След като бъдат приети от министъра, тези наредби се представят пред Парламента и спрямо тях се прилага процедурата за „отрицателна резолюция“, съгласно която и двете камари на Парламента могат да осъществят контрол на наредбата и имат правомощието да приемат предложение за отмяна на наредбата в срок от 40 дни ([144]).

(78) Съгласно член 74B, параграф 1 от ЗЗД от 2018 г. наредбите относно адекватното ниво на защита трябва да бъдат преразглеждани на интервали, не по-дълги от четири години, а министърът трябва постоянно да следи за събития в трети държави и международни организации, които биха могли да засегнат решенията за приемане на наредби относно адекватното ниво на защита или за изменение или отмяна на такива наредби. Когато министърът узнае, че дадена държава или организация вече не осигурява адекватно ниво на защита на личните данни, той трябва, доколкото е необходимо, да измени или отмени наредбите и да започне консултации със съответната трета държава или международна организация с цел да се отстрани липсата на адекватно ниво на защита.

(79) Подобно на предвиденото в член 37 от Директива (ЕС) 2016/680, при липсата на наредба относно адекватното ниво на защита предаването на лични данни в контекста на сектора на правоприлагането би било възможно, когато са налице подходящи гаранции. Такива гаранции се осигуряват чрез а) правнообвързващ инструмент, в който са предвидени подходящи гаранции за защитата на личните данни; или б) оценка, извършена от администратора, който, след оценка на всички обстоятелства около предаването, е стигнал до заключението, че по отношение на защитата на личните данни съществуват подходящи гаранции ([145]). Освен това, когато предаването се основава на подходящи гаранции, в ЗЗД от 2018 г. се предвижда, че в допълнение към обичайната надзорна роля на ICO компетентните органи трябва да предоставят на ICO конкретна информация за предаването на данни ([146]).

(80) Ако предаването не се основава на решение относно адекватното ниво на защита или на подходящи гаранции, то може да се осъществи само при определени специфични обстоятелства, наричани „особени обстоятелства“ ([147]). Такъв е случаят, когато предаването е необходимо: а) за да бъдат защитени жизненоважни интереси на субекта на данни или на друго лице; б) за да бъдат защитени легитимни интереси на субекта на данни; в) за предотвратяване на непосредствена и сериозна заплаха за обществената сигурност на трета държава; г) в отделни случаи — за някоя от целите на правоприлагането; или д) в отделни случаи — с правна цел (напр. във връзка със съдебни производства или с цел получаване на правни съвети) ([148]). Може да се отбележи, че букви г) и д) не се прилагат, ако правата и свободите на субекта на данни надделяват над обществения интерес от предаването ([149]). Този набор от обстоятелства съответства на специфичните ситуации и условия, които се определят като „дерогации“ съгласно член 38 от Директива (ЕС) 2016/680.

(81) При тези обстоятелства датата, часът и обосновката на предаването, името и всяка друга относима информация за получателя и описанието на предадените лични данни трябва да бъдат документирани и при поискване предоставени на комисаря по информацията ([150]).

(82) В член 78 от ЗЗД от 2018 г. се урежда случаят на „последващо предаване“, а именно когато лични данни, които са били предадени от Обединеното кралство на трета държава, впоследствие се предават на друга трета държава или на международна организация. В съответствие с член 78, параграф 1 предаващият администратор от Обединеното кралство трябва да постави като условие за предаването данните да не бъдат допълнително предавани на трета държава без разрешението на предаващия администратор. Освен това съгласно член 78, параграф 3 и подобно на предвиденото в член 35, параграф 1, буква д) от Директива (ЕС) 2016/680, в случай че се изисква такова разрешение, се прилагат редица материалноправни изисквания. По-конкретно, когато решава дали да разреши

([143]) Вж. Меморандума за разбирателство между министъра на цифровите технологии, културата, медиите и спорта и Службата на комисаря по информацията във връзка с новата оценка на адекватното ниво на защита в Обединеното кралство, който може да бъде намерен на следния адрес: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) През този 40-дневен срок двете камари на Парламента имат възможност, ако желаят, да гласуват против наредбите. Ако бъде направено такова гласуване, в крайна сметка наредбите ще престанат да пораждат правно действие за в бъдеще.

([145]) Член 75 от ЗЗД от 2018 г.

([146]) Съгласно член 75, параграф 3 от ЗЗД от 2018 г., когато предаването на данни се извършва при използването на подходящи гаранции: а) предаването трябва да бъде документирано, б) при поискване документацията трябва да бъде предоставена на комисаря и в) документацията трябва да включва по-специално i) датата и часа на предаването, ii) името и всяка друга относима информация за получателя, iii) обосновката за предаването и iv) описание на предадените лични данни.

([147]) Насоки за обработване на данни в областта на правоприлагането, „Съществуват ли особени обстоятелства?“ (Guide to Law Enforcement Processing, „Are there any special circumstances?“), достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

([148]) Член 76 от ЗЗД от 2018 г.

([149]) Член 76 от ЗЗД от 2018 г.

([150]) Член 76, параграф 3 от ЗЗД от 2018 г.

предаването или не, компетентният орган трябва да се увери, че по-нататъшното предаване е необходимо за целите на правоприлагането, и следва да вземе предвид, наред с други фактори, а) сериозността на обстоятелствата, довели до искането за разрешение, б) целта, за която личните данни са били първоначално предадени, и в) стандартите за защита на личните данни, които се прилагат в третата държава или международната организация, на която ще бъдат предадени личните данни.

(83) Освен това се прилагат допълнителни гаранции, когато данните, обект на последващо предаване от Обединеното кралство, първоначално са били прехвърлени от Европейския съюз.

(84) Първо, подобно на член 35, параграф 1, буква в) от Директива (ЕС) 2016/680, в член 73, параграф 1, буква b) от ЗЗД от 2018 г. се предвижда, че в случаите, когато личните данни първоначално са били предадени или предоставени по друг начин на администратора или на друг компетентен орган от държава членка, тази държава членка или който и да било субект, установен в тази държава членка, който е компетентен орган за целите на Директива (ЕС) 2016/680, трябва да са дали разрешение за предаването в съответствие с правото на държавата членка.

(85) Подобно на член 35, параграф 2 от Директива (ЕС) 2016/680 обаче такова разрешение не се изисква, когато: а) предаването е необходимо за предотвратяването на непосредствена и сериозна заплаха за обществената сигурност на държава членка или на трета държава, или за основните интереси на държава членка, и б) разрешението не може да бъде получено своевременно. В този случай органът в държавата членка, който би бил отговорен за вземането на решение дали да разреши прехвърлянето, трябва да бъде информиран незабавно ([151]).

(86) Второ, същият подход се прилага и в случай на данни, първоначално предадени от Европейския съюз на Обединеното кралство, след това предадени от Обединеното кралство на трета държава, която впоследствие ще ги предаде на трета държава. В този случай съгласно член 78, параграф 4 компетентният орган на Обединеното кралство не може да даде разрешение за последното предаване съгласно член 78, параграф 1, освен ако „държавата членка [която първоначално е предала въпросните данни] или който и да било субект, установен в тази държава членка, който е компетентен орган за целите на Директивата относно правоприлагането, са разрешили предаването в съответствие с правото на държавата членка“. Тези гаранции са важни, тъй като дават възможност на органите на държавите членки да гарантират непрекъснатост на защитата в съответствие със законодателството на ЕС за защита на данните по цялата „верига на предаване“.

(87) Тази нова рамка за международно предаване на данни започна да се прилага в края на преходния период ([152]). В точки 10—12 от приложение 21 (въведено с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения) обаче се предвижда, че след края на преходния период определени предавания на лични данни се третират така, все едно се основават на наредби относно адекватното ниво на защита. Тези предавания включват предавания към държава членка, държава от ЕАСТ, трета държава, спрямо която в края на преходния период се прилага решение на ЕС относно адекватното ниво на защита, и територията на Гибралтар. Следователно предаванията към тези държави може да продължат както преди оттеглянето на Обединеното кралство от Съюза. След края на преходния период министърът трябва да извърши преглед на тези констатации за адекватно ниво на защита в срок от четири години, т.е. до края на декември 2024 г. Според обяснението, предоставено от органите на Обединеното кралство, въпреки че министърът трябва да предприеме такъв преглед до края на декември 2024 г., сред преходните разпоредби няма разпоредба за изтичане на срока на действие и съответните преходни разпоредби няма автоматично да престанат да пораждат правно действие, ако прегледът не приключи до края на декември 2024 г.

2.4.9. *Отчетност*

(88) Съгласно принципа на отчетност публичните органи, които обработват данни, са длъжни да въведат подходящи технически и организационни мерки за ефективно спазване на своите задължения за защита на данните и да могат да докажат това спазване, по-специално пред компетентния надзорен орган.

(89) Този принцип е отразен в член 56 от ЗЗД от 2018 г., с който се въвежда общо задължение за отчетност за администратора, т.е. задължение за прилагане на подходящи технически и организационни мерки, за да се гарантира и да може да се докаже, че обработването на лични данни е в съответствие с изискванията на част 3 от ЗЗД от 2018 г. Прилаганите мерки трябва да бъдат преразглеждани и, когато е необходимо, актуализирани и когато това е пропорционално по отношение на обработването, да включват подходящи политики за защита на данните.

([151]) Член 73, параграф 5 от ЗЗД от 2018 г.

([152]) Приложимостта на тази нова уредба трябва да се разглежда в светлината на член 782 от Споразумението за търговия и сътрудничество между Европейския съюз и Европейската общност за атомна енергия, от една страна, и Обединеното кралство Великобритания и Северна Ирландия, от друга страна (ОВ L 444, 31.12.2020 г., стр. 14) („СТС ЕС—Обединено кралство“), достъпно на следния адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

(90) В съответствие с глава IV от Директива (ЕС) 2016/680 в членове 55—71 от ЗЗД от 2018 г. се предвиждат различни механизми, чрез които се гарантира отчетност, а администраторите и обработващите лични данни могат да докажат, че спазват изискванията. По-специално администраторите са длъжни да прилагат мерки за защита на данните още на етапа на проектирането и по подразбиране, т.е. да гарантират, че принципите за защита на данните се прилагат ефективно, и са длъжни да поддържат регистри за всички категории дейности по обработване, за които отговаря администраторът (вкл. информация за самоличността на администратора, координатите за връзка на длъжностното лице по защита на данните, целите на обработването, категориите получатели на разкривания и описание на категориите субекти на данни и лични данни), и да съхраняват тези регистри на разположение на комисаря по информацията при поискване. Администраторът и обработващият лични данни трябва също така да водят записи за определени операции по обработване и да ги предоставят на комисаря по информацията ([153]). От администраторите също така се изисква по-специално да си сътрудничат с комисаря по информацията при изпълнението на задачите на комисаря.

(91) В ЗЗД от 2018 г. се предвиждат и допълнителни изисквания за обработване, което може да породи висок риск за правата и свободите на физическите лица. Те включват задължение за извършване на оценка на въздействието върху защитата на данните и за консултиране с комисаря по информацията преди обработването, ако оценката показва, че обработването може да породи висок риск за правата и свободите на физическите лица (ако няма мерки за ограничаване на риска).

(92) Освен това администраторите трябва да назначат длъжностно лице по защита на данните, освен ако администраторът не е съд или друг съдебен орган, който действа в изпълнение на съдебните си функции ([154]). Администраторът трябва да гарантира, че длъжностното лице по защита на данните участва във всички въпроси, свързани със защитата на личните данни, разполага с необходимите ресурси и достъп до личните данни и операциите по обработване и може да изпълнява задачите си независимо. Задачите на длъжностното лице по защита на данните са посочени в член 71 от ЗЗД от 2018 г. и включват предоставяне на информация и съвети, наблюдение на спазването на изискванията, както и сътрудничество с комисаря по информацията и изпълнение на ролята на точка за контакт за комисаря по информацията. При изпълнението на своите задачи длъжностното лице по защита на данните трябва да отчита рисковете, свързани с операциите по обработване, като взема предвид естеството, обхвата, контекста и целите на обработването.

2.5. **Надзор и привеждане в изпълнение**

2.5.1. *Независим надзор*

(93) С цел да се гарантира, че адекватното ниво на защита на данните се осигурява и на практика, трябва да съществува независим надзорен орган с правомощия за наблюдение и привеждане в изпълнение на правилата за защита на данните. Този орган трябва да действа с пълна независимост и безпристрастност при изпълнението на своите задължения и при упражняването на правомощията си.

(94) В Обединеното кралство надзорът и привеждането в изпълнение на ОРЗД на Обединеното кралство и на ЗЗД от 2018 г. се осъществяват от комисаря по информацията ([155]). Комисарят по информацията надзирава и обработването на лични данни от компетентните органи, които попадат в обхвата на част 3 от ЗЗД от 2018 г. ([156]). Комисарят по информацията е еднолична корпоративна структура (*corporation sole*): отделен правен субект, учреден като едноличен орган. Комисарят по информацията се подпомага в работата си от служба. Към 31 март 2020 г. Службата на комисаря по информацията разполагаше със 768 постоянни служители ([157]). Комисарят по информацията е на бюджетна издръжка на Министерството на цифровите технологии, културата, медиите и спорта (DCMS) ([158]).

([153]) Член 62 от ЗЗД от 2018 г.

([154]) Член 69 от ЗЗД от 2018 г.

([155]) Член 36, параграф 2, буква б) от Директива (ЕС) 2016/680.

([156]) Член 116 от ЗЗД от 2018 г.

([157]) Годишен доклад и годишни финансови отчети на комисаря по информацията за 2019—2020 г., достъпни на следния адрес: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([158]) Отношенията им се уреждат със споразумение за управление. По-специално основните отговорности на DCMS като финансиращо ведомство включват: да гарантира, че ICO е обезпечена с адекватно финансиране и ресурси; да представлява на интересите на ICO пред Парламента и други държавни ведомства; да осигури наличието на солидна национална уредба за защита на данните; и да предоставя насоки и подкрепа на ICO по корпоративни въпроси, като например въпроси, свързани с недвижимо имущество, наеми и обществени поръчки (Споразумението за управление за периода 2018—2021 г. е достъпно на следния адрес: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Независимостта на комисаря е изрично уредена в член 52 от ОРЗД на Обединеното кралство, който отразява изискванията, предвидени в член 52, параграфи 1—3 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([159]). Комисарят трябва да действа напълно независимо при изпълнението на своите задачи и упражняването на своите правомощия в съответствие с ОРЗД на Обединеното кралство, да остане независим от външно влияние, било то пряко, или непряко, във връзка с тези задачи и правомощия, и нито да търси, нито да приема инструкции от когото и да било. Комисарят трябва също така да се въздържа от всякакви несъвместими със служебните му задължения действия и по време на своя мандат не трябва да се ангажира с никакви несъвместими функции, независимо дали срещу възнаграждение, или безвъзмездно.

(96) Условията за назначаване и отстраняване на комисаря по информацията са посочени в приложение 12 към ЗЗД от 2018 г. Комисарят по информацията се назначава от кралицата по препоръка на правителството след провеждане на безпристрастен конкурс на общо основание. Кандидатът трябва да притежава подходящите квалификации, умения и компетентност. В съответствие с Кодекса за управление на публичните назначения ([160]) консултативна комисия за оценка изготвя списък на кандидатите, които могат да бъдат назначени. Преди министърът на цифровите технологии, културата, медиите и спорта да финализира решението си, съответната специална комисия на Парламента трябва да осъществи контрол преди назначаването. Становището на комисията се оповестява публично ([161]).

(97) Комисарят по информацията има мандат до седем години. Комисарят по информацията може да бъде отстранен от длъжност от Нейно величество след обръщение от страна на двете камари на Парламента ([162]). Искане за освобождаване от длъжност на комисаря по информацията не може да бъде представено пред никоя камара на Парламента, освен ако министър не е подал до Парламента доклад, в който посочва, че е убеден, че комисарят по информацията е извършил тежко нарушение и/или че комисарят вече не отговаря на условията, необходими за изпълнението на функциите на комисар ([163]).

(98) Източниците на финансиране на комисаря по информацията са три: i) таксите за защита на данните, плащани от администраторите, които се определят с наредба на министъра ([164]) и възлизат на 85—90 % от годишния бюджет на Службата ([165]); ii) безвъзмездна помощ, която може да бъде изплатена от правителството на комисаря по информацията и се използва главно за финансиране на неговите оперативни разходи във връзка със задачи, които не са свързани със защитата на данните ([166]); iii) таксите, събирани за услуги ([167]). Понастоящем не се събират такива такси.

(99) Общите функции на комисаря по информацията във връзка с обработването на лични данни, които попадат в обхвата на част 3 от ЗЗД от 2018 г., са определени в приложение 13 към ЗЗД от 2018 г. Задачите му включват наблюдение и привеждане в изпълнение на част 3 от ЗЗД от 2018 г., повишаване на обществената осведоменост, предоставяне на консултации на Парламента, правителството и други институции относно законодателните и административните мерки, повишаване на осведомеността на администраторите и обработващите лични данни за техните задължения,

([159]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

([160]) Кодекс за управление на публичните назначения, достъпен на следния адрес: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Втори доклад от сесия 2015—2016 г. на комисията по култура, медии и спорт на Камарата на общините, достъпен на следния адрес: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) „Обръщение“ е предложение, внесено в Парламента, което има за цел да запознае монарха със становищата на Парламента по даден въпрос.

([163]) Точка 3 от приложение 12 към ЗЗД от 2018 г.

([164]) Член 137 от ЗЗД от 2018 г.

([165]) В членове 137 и 138 от ЗЗД от 2018 г. се съдържат редица гаранции, за да се осигури определянето на таксите на подходящо равнище. По-специално в член 137, параграф 4 от ЗЗД от 2018 г. се изброяват обстоятелствата, които министърът трябва да вземе предвид при приемането на наредби за определяне на сумите, дължими от различните организации. В член 138, параграф 1 и член 182 от ЗЗД от 2018 г. също се съдържа правно изискване, преди наредбите да бъдат приети, министърът да се консултира с комисаря по информацията и с представители на други лица, които може да бъдат засегнати от наредбите, така че техните становища да могат да бъдат взети предвид. Освен това съгласно член 138, параграф 2 от ЗЗД от 2018 г. комисарят по информацията е длъжен да извършва преглед на действието на Наредбите за таксите и може да представя на министъра предложения за изменение на Наредбите. Накрая, с изключение на случаите, когато се приемат наредби само за да се вземе предвид увеличението на индекса на цените на дребно (в който случай спрямо тях ще се приложи процедурата за отрицателна резолюция), спрямо наредбите се прилага процедурата за потвърдителна резолюция и те не може да бъдат приети, докато не бъдат одобрени с резолюция на всяка камара на Парламента.

([166]) В Споразумението за управление се пояснява, че „министърът може да извършва плащания на комисаря по информацията със средства, предоставени от Парламента съгласно точка 9 от приложение 12 към ЗЗД от 2018 г. След консултация с комисаря по информацията DCMS ще му изплати съответните суми (безвъзмездна помощ) за административните разходи на ICO и за изпълнението на неговите функции във връзка с редица специфични функции, включително свобода на информацията“ (Споразумение за управление за периода 2018—2021 г., точка 1.12, вж. бележка под линия 158).

([167]) Член 134 от ЗЗД от 2018 г.

предоставяне на информация на субекта на данни при упражняването на неговите права и провеждане на разследвания. С цел запазване на независимостта на съдебната власт комисарят по информацията няма право да изпълнява функциите си във връзка с обработването на лични данни чрез лице, действащо в изпълнение на съдебните си функции, или от съд или правораздавателен орган, действащ в изпълнение на съдебните си функции. Надзорът на съдебната власт обаче се осигурява от специализираните органи, разгледани по-нататък.

2.5.1.1. Привеждане в изпълнение, включително санкции

(100) Комисарят има общи правомощия за разследване, корективни правомощия, правомощия за даване на разрешения и становища във връзка с обработването на лични данни, за които се прилага част 3 от ЗЗД от 2018 г. Комисарят има правомощия да уведомява администратора или обработващия лични данни за предполагаемо нарушение на част 3, да отправя предупреждения до администратора или обработващия лични данни, когато има вероятност операции по обработване на данни, които те възнамеряват да извършат, да нарушат разпоредбите на част 3, и да отправя официално предупреждение до администратора или обработващия лични данни, когато операции по обработване на данни са нарушили разпоредбите на част 3. Освен това комисарят може да издава по собствена инициатива или при поискване становища до Парламента на Обединеното кралство, правителството или до други институции и органи, както и до обществеността по всякакви въпроси, свързани със защитата на лични данни ([168]).

(101) Освен това комисарят има правомощия:

— да разпорежда на администратора и на обработващия лични данни (и при определени обстоятелства на всяко друго лице) да предоставят необходимата информация, като издава информационно постановление („информационно постановление“) ([169]);

— да провежда разследвания и одити, като издава ревизионно постановление, чрез който администраторът или обработващият лични данни бива задължен да допусне комисаря да влезе в определени помещения, да проверява или преглежда документи или оборудване, да изслушва лица, обработващи лични данни от името на администратора („ревизионно постановление“) ([170]);

— да получава по друг начин достъп до документите на администраторите и обработващите лични данни и достъп до техните помещения в съответствие с член 154 от ЗЗД от 2018 г. („правомощия за влизане и проверка“);

— да упражнява корективни правомощия, включително чрез предупреждения и официални предупреждения, или да дава разпореждания чрез изпълнително постановление, чрез което администраторите/обработващите лични данни биват задължени да предприемат или да се въздържат от предприемането на конкретни действия („изпълнително постановление“) ([171]); и

— да налага административни наказания „глоба“ или „имуществена санкция“ под формата на наказателно постановление („наказателно постановление“) ([172]).

(102) В Политиката на ICO за регулаторните действия се определят обстоятелствата, при които комисарят издава съответно информационно, ревизионно, изпълнително и наказателно постановление ([173]). С изпълнително постановление може да бъдат наложени изисквания, които комисарят смята за подходящи с цел отстраняване на неизпълнението. С наказателно постановление лицето се задължава да плати на комисаря по информацията посочена в постановлението сума. Наказателно постановление може да бъде издадено, когато е налице неизпълнение на определени разпоредби на ЗЗД от 2018 г. ([174]), или може да бъде връчено на администратор или обработващ лични данни, който не е изпълнил информационно постановление, ревизионно постановление или изпълнително постановление.

(103) По-конкретно, когато се решава дали на администратор или обработващ лични данни да бъде връчено наказателно постановление и се определя размерът на санкцията, комисарят по информацията трябва да вземе предвид изброените в член 155, параграф 3 от ЗЗД от 2018 г. обстоятелства, включително естеството и тежестта на неизпълнението, дали неизпълнението е извършено умишлено или по небрежност, действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни, степента на отговорност на администратора или обработващия лични данни (като се вземат предвид

([168]) Точка 2 от приложение 13 към ЗЗД от 2018 г.
([169]) Член 142 от ЗЗД от 2018 г. (при спазване на ограниченията по член 143 от ЗЗД от 2018 г.).
([170]) Член 146 от ЗЗД от 2018 г. (при спазване на ограниченията по член 147 от ЗЗД от 2018 г.).
([171]) Членове 149—151 от ЗЗД от 2018 г. (при спазване на ограниченията по член 152 от ЗЗД от 2018 г.).
([172]) Член 155 от ЗЗД от 2018 г. (при спазване на ограниченията по член 156 от ЗЗД от 2018 г.).
([173]) Политика за регулаторните действия, достъпна на следния адрес: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) По-специално ICO може да издаде наказателно постановление за неизпълнение на разпоредбите на член 149, параграфи 2, 3, 4 или 5 от ЗЗД от 2018 г.

техническите и организационните мерки, въведени от администратора или обработващия лични данни), евентуалните свързани предишни неизпълнения на администратора или обработващия лични данни; категориите лични данни, засегнати от неизпълнението, и дали санкцията би била ефективна, пропорционална и възпираща.

(104) Максималният размер на санкцията, която може да бъде наложена с наказателно постановление, е а) 17 500 000 британски лири във връзка с неизпълнение на принципите за защита на данните (членове 35, 36, 37, член 38, параграф 1, член 39, параграф 1 и член 40 от ЗЗД от 2018 г.), задълженията за прозрачност и индивидуалните права (членове 44, 45, 46, 47, 48, 49, 52 и 53 от ЗЗД за 2018 г.) и принципите за международно предаване на лични данни (членове 73, 75, 76, 77 или 78 от ЗЗД от 2018 г.); и б) 8 700 000 британски лири в останалите случаи ([175]). При неизпълнение на информационно постановление, ревизионно постановление или изпълнително постановление максималният размер на санкцията, която може да бъде наложена с наказателно постановление, е 17 500 000 британски лири.

(105) Според последните си годишни доклади (2018—2019 г. ([176]), 2019—2020 г. ([177])) комисарят по информацията проведе редица разследвания във връзка с обработването на лични данни от правоприлагащи органи в областта на наказателното право. Например комисарят проведе разследване и през октомври 2019 г. публикува Становище относно използването от правоприлагащите органи на технологии за разпознаване на лица на обществени места. Разследването е съсредоточено по-специално върху използването на функции за разпознаване на лица на живо от полицията на Южен Уелс и Столичната полицейска служба (MPS). Освен това комисарят разследва матрицата за бандите (Gangs matrix) ([178]) на MPS и установи редица сериозни нарушения на законодателството за защита на данните, които има вероятност да подкопаят общественото доверие в матрицата и използването на данните.

(106) През ноември 2018 г. комисарят по информацията издаде изпълнително постановление и впоследствие MPS предприе необходимите действия за повишаване на сигурността и отчетността и за гарантиране на пропорционалното използване на данните.

(107) Друг пример за скорошно изпълнително действие е глобата в размер на 325 000 британски лири, наложена от комисаря през май 2018 г. на Кралската прокуратура за загубата на некриптирани DVD дискове, съдържащи записи на полицейски разпити. Освен това комисарят по информацията проведе разследвания по по-широки теми, например през първата половина на 2020 г., относно използването на извличането на данни от мобилни телефони за целите на полицията и обработването на данните на жертвите от полицията.

(108) В допълнение към тези правомощия за привеждане в изпълнение на комисаря по информацията, някои нарушения на законодателството за защита на данните представляват престъпления и поради това за тях може да се налагат наказания (член 196 от ЗЗД от 2018 г.). Това се отнася например за получаването или разкриването на лични данни без съгласието на администратора и за предоставянето на друго лице на разкритите лични данни без съгласието на администратора ([179]); реидентифицирането на информация, която представлява деидентифицирани лични данни, без съгласието на администратора, отговарящ за деидентифицирането на личните данни ([180]); умишленото възпрепятстване на комисаря да упражнява правомощията си за проверката на лични данни в съответствие с международни задължения ([181]), представянето на неверни данни в отговор на информационно постановление или унищожаването на информация във връзка с информационни и ревизионни постановления ([182]).

(109) Комисарят по информацията също така има задължение по член 139 от ЗЗД от 2018 г. да представя пред всяка камара на Парламента общ доклад относно упражняването на функциите си съгласно Закона ([183]).

([175]) Член 157 от ЗЗД от 2018 г.

([176]) Годишен доклад и годишни финансови отчети на комисаря по информацията за 2018—2019 г., достъпни на следния адрес: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Годишен доклад на комисаря по информацията за 2019—2020 г. (вж. бележка под линия 157).

([178]) База данни, в която са записани разузнавателни данни, свързани с предполагаеми членове на банди и жертви на престъпления, свързани с банди.

([179]) Член 170 от ЗЗД от 2018 г.

([180]) Член 171 от ЗЗД от 2018 г.

([181]) Член 119 от ЗЗД от 2018 г.

([182]) Членове 144 и 148 от ЗЗД от 2018 г.

([183]) Както е посочено в Споразумението за управление, годишният доклад трябва: i) да обхваща всички предприятия, дъщерни предприятия и съвместни предприятия под контрола на ICO; ii) да спазва Наръчника за финансово отчитане на Министерството на финансите (FReM); iii) да съдържа декларация за управлението, в която се посочва как счетоводителят е управлявал и контролирал ресурсите, използвани в организацията през годината, като онагледява в каква степен организацията се справя с рисковете за постигането на своите цели и задачи; и iv) да очертава основните дейности и резултати през предходната финансова година и да представя в обобщен вид прогнозното планиране (Споразумение за управление за периода 2018—2021 г., точка 3.26, вж. бележка под линия 158).

2.5.2. *Надзор на съдебната власт*

(110) Надзорът на обработването на лични данни от съдилищата и съдебната власт е двояк. Когато лице, заемащо съдебна длъжност, или съд не действа в изпълнение на съдебните си функции, надзорът се осъществява от комисаря по информацията. Когато администраторът действа в изпълнение на съдебните си функции, ICO не може да упражнява надзорните си функции ([184]) и надзорът се осъществява от специални органи. Това отразява подхода, възприет в член 32 от Директива (ЕС) 2016/680.

(111) По-специално във втория случай, за съдилищата в Англия и Уелс и трибунала от първа инстанция (First-tier Tribunal) и трибунала от по-горна инстанция (Upper Tribunal) на Англия и Уелс, такъв надзор се осъществява от Съдебния състав за защита на данните ([185]). Освен това главният съдия (Lord Chief Justice) и първият председател (Senior President) на трибуналите са издали декларация за поверителност ([186]), в която се посочва как съдилищата в Англия и Уелс обработват лични данни при изпълнение на съдебни функции. Подобна декларация е издадена от северноирландската ([187]) и шотландската ([188]) съдебни власти.

(112) Освен това в Северна Ирландия главният съдия на Северна Ирландия назначи съдия от Висшия съд като съдия по надзора на данните (DSJ) ([189]). Те също са издали насоки за съдебната власт на Северна Ирландия относно действията, които трябва да се предприемат в случай на загуба или възможна загуба на данни, и относно процедурата за решаване на всички въпроси, свързани с това ([190]).

(113) В Шотландия председателят на Върховния съд (*Lord President*) е назначил съдия по надзора на данните, който да разглежда всички жалби на основание защита на данните. Това е уредено в правилата за жалбите във връзка със съдебната система, които съответстват на правилата, установени за Англия и Уелс ([191]).

(114) Накрая, един от върховните съдии във Върховния съд се определя да упражнява надзор на защитата на данните.

([184]) Член 117 от ЗЗД от 2018 г.

([185]) Съдебният състав за защита на данните отговаря за предоставянето на насоки и обучение на съдебната власт. Той също така разглежда жалби от субекти на данни във връзка с обработването на лични данни от съдилища, трибунали и физически лица, действащи в изпълнение на съдебните си функции. Съставът има за цел да осигури средствата, чрез които може да бъде решена всяка жалба. Ако жалбоподател не е удовлетворен от решение на Състава и е предоставил допълнителни доказателства, Съставът може да преразгледа решението си. Въпреки че самият Състав не налага финансови санкции, ако Съставът смята, че има достатъчно тежко нарушение на ЗЗД от 2018 г., той може да го отнесе до Службата за разглеждане на поведението в съдебната система (JCIO), която ще разгледа жалбата. Ако жалбата бъде уважена, лорд-канцлерът (*Lord Chancellor*) и главният съдия (или първият съдия, на когото е делегирано правомощието да действа от негово име) решават какви действия да бъдат предприети срещу заемащия длъжността. Това може да включва, по ред на тежестта: официално становище, предупреждение и официално предупреждение и, като крайна мярка, отстраняване от длъжност. Ако дадено лице не е удовлетворено от начина, по който JCIO е разгледала жалбата, то може да подаде друга жалба до омбудсмана по назначенията и поведението в съдебната система (вж. https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Омбудсманът има правомощието да поиска от JCIO да преразгледа жалбата и може да предложи на жалбоподателя да получи обезщетение, когато смята, че е претърпял вреди в резултат на лошо администриране.

([186]) Декларацията за поверителност на главния съдия и първия председател на трибуналите е достъпна на следния адрес: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Декларацията за поверителност на главния съдия на Северна Ирландия е достъпна на следния адрес: https://judiciaryni.uk/data-privacy.

([188]) Декларацията за поверителност на шотландските съдилища и трибунали е достъпна на следния адрес: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) DSJ предоставя насоки на съдебната власт и разглежда нарушения и/или жалби във връзка с обработването на лични данни от съдилища или физически лица, действащи в изпълнение на съдебните си функции.

([190]) Когато жалбата се смята за сериозна или нарушението за тежко, те се предават на служителя по жалбите във връзка със съдебната система за по-нататъшно разглеждане в съответствие с Кодекса за поведение във връзка с жалбите, издаден от главния съдия на Северна Ирландия. Такава жалба може да приключи: без по-нататъшни действия, със становище, с обучение или с наставничество, с неофициално предупреждение, с официално предупреждение, с последно предупреждение, с ограничаване на правото да се упражняват съдебни функции или с предаване на законоустановен трибунал. Кодексът за поведение във връзка с жалбите, издаден от главния съдия на Северна Ирландия, е достъпен на следния адрес: 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]) Всяка основателна жалба се разглежда от съдията по надзора на данните и се предава на председателя на Върховния съд, който има правомощието да издаде становище, предупреждение или официално предупреждение, ако сметне това за необходимо (сходни правила съществуват за членовете на трибунала и са достъпни на следния адрес: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Средства за правна защита*

(115) С цел да се осигури адекватна защита, и по-специално упражняване на индивидуалните права, на субекта на данни следва да се предоставят ефективни административни и съдебни средства за правна защита, включително и обезщетение за вреди.

(116) Първо, субектът на данни има право да подаде жалба до комисаря по информацията, ако смята, че във връзка с личните му данни е извършено нарушение на част 3 от ЗЗД от 2018 г. ([192]). Както е описано в съображения 100 и 109, комисарят по информацията има правомощието да преценява спазването от администратора и обработващия лични данни на ЗЗД от 2018 г., да ги задължава да предприемат или да се въздържат от предприемането на необходимите действия в случай на неспазване и да налага глоби.

(117) Второ, в ЗЗД от 2018 г. се предвижда право на средства за правна защита срещу комисаря по информацията. Ако комисарят не постигне „напредък“ ([193]) по жалба, подадена от субекта на данни, жалбоподателят има достъп до съдебни средства за правна защита, тъй като може да поиска от трибунала от първа инстанция ([194]) да разпореди на комисаря да предприеме подходящи действия, за да отговори на жалбата, или да информира жалбоподателя за напредъка по жалбата ([195]). Освен това всяко лице, на което комисарят е издал някое от посочените по-горе постановления (информационно, ревизионно, изпълнително или наказателно постановление), може да го обжалва пред трибунала от първа инстанция. Ако трибуналът сметне, че решението на комисаря е незаконосъобразно или че комисарят по информацията е трябвало да упражни правото си на преценка по различен начин, трибуналът трябва да уважи жалбата или да замени постановлението с друго такова или с решение, което комисарят по информацията е можел да издаде или да постанови ([196]).

(118) Трето, физическите лица могат да получат съдебна защита срещу администраторите и обработващите лични данни пряко пред съдилищата съгласно член 167 от ЗЗД от 2018 г. Ако по искане на субект на данни съдът е убеден, че е налице нарушение на правата на субекта на данни съгласно законодателството за защита на данните, съдът може да разпореди на администратора по отношение на обработването или на обработващ лични данни, действащ от името на този администратор, да предприеме посочените в заповедта действия или да се въздържи от предприемането на посочените в заповедта действия. Освен това съгласно член 169 от ЗЗД от 2018 г. всяко лице, което е претърпяло вреда поради нарушение на изискване на законодателството за защита на данните (включително на част 3 от ЗЗД от 2018 г.), различно от ОРЗД на Обединеното кралство, има право на обезщетение за тази вреда от администратора или обработващия лични данни, освен ако администраторът или обработващият лични данни докаже, че администраторът или обработващият лични данни по никакъв начин не е отговорен за събитието, причинило вредата. Вредите включват както финансови загуби, така и вреди, които не са свързани с финансови загуби, като например емоционално страдание.

(119) Четвърто, доколкото дадено лице смята, че неговите права, включително правото на неприкосновеност на личния живот и на защита на данните, са били нарушени от публичните органи, то може да получи правна защита пред съдилищата на Обединеното кралство съгласно Закона за правата на човека от 1998 г. Съгласно част 3 от ЗЗД от 2018 г. администраторите, т.е. компетентните органи, винаги са публични органи по смисъла на Закона за правата на човека от 1998 г. Физическо лице, което твърди, че публичен орган е действал (или възнамерява да действа) по начин, който е несъвместим с право, прогласено по Конвенцията, и следователно е незаконосъобразен съгласно член 6, параграф 1 от Закона за правата на човека от 1998 г., може да заведе дело срещу органа в съответния съд или трибунал или да се позове на съответните права във всяко съдебно производство, когато лицето е (или би било) жертва на незаконосъобразното действие ([197]).

([192]) Член 165 от ЗЗД от 2018 г.

([193]) Член 166 от ЗЗД от 2018 г. се отнася конкретно до следните случаи: а) комисарят не е предприел подходящи действия, за да отговори на жалбата, б) комисарят не е предоставил на жалбоподателя информация за напредъка по жалбата или за резултата от нея преди изтичането на 3-месечния срок, считано от датата на получаване на жалбата от него, или в) ако разглеждането на жалбата от страна на комисаря не е приключило в този срок, не е предоставил тази информация на жалбоподателя в следващите 3 месеца.

([194]) Трибуналът от първа инстанция е компетентният съд за разглеждане на жалби срещу решения, взети от държавни регулаторни органи. В случай на решение на комисаря по информацията компетентно е отделението „Общи правни въпроси“ (*General Regulatory Chamber*), което има юрисдикция за цялото Обединено кралство.

([195]) Член 166 от ЗЗД от 2018 г.

([196]) Членове 161 и 162 от ЗЗД от 2018 г.

([197]) Вж. дело *Brown/Commissioner of the Met* от 2016 г., в което съдът предоставя правна защита на ищеца в контекста на защитата на данните по дело, заведено срещу полицията. Съдът се произнася в полза на ищеца, като уважава исковете му за нарушение на задълженията по ЗЗД от 1998 г., нарушение на ЗПЧ от 1998 г. (и свързаното с него право по член 8 от ЕКПЧ) и непозволено увреждане, изразяващо се в злоупотреба с лична информация (ответникът в крайна сметка признава, че е нарушил ЗЗД и ЕКПЧ, така че решението се съсредоточава върху подходящото обезщетение). В резултат на тези нарушения съдът присъжда парично обезщетение на ищеца.

(120) Ако съдът установи, че акт на публичен орган е незаконосъобразен, в рамките на своите правомощия той може да предостави такова поправяне на вредите или обезщетение или да постанови такова разпореждане, каквото счита за справедливо и подходящо ([198]). Съдът може също така да обяви разпоредба от първичното право за несъвместима с право, гарантирано от ЕКПЧ.

(121) Накрая, след изчерпване на националните средства за правна защита дадено лице може да получи правна защита от Европейския съд по правата на човека за нарушения на правата, гарантирани от ЕКПЧ.

2.6. **Последващо споделяне**

(122) Правото на Обединеното кралство допуска, при определени условия, споделянето на данни от правоприлагащ орган с други органи на Обединеното кралство за цели, различни от тези, за които те са били първоначално събрани (т.нар. „последващо споделяне“).

(123) Подобно на предвиденото в член 4, параграф 2 от Директива (ЕС) 2016/680, член 36, параграф 3 от ЗЗД от 2018 г. позволява личните данни, събрани от компетентен орган за целите на правоприлагането, да бъдат обработвани по-нататък (независимо дали от първоначалния администратор или от друг администратор) за всяка друга цел на правоприлагането, при условие че администраторът е оправомощен по закон да обработва данни за другата цел и че обработването е необходимо и пропорционално ([199]). В този случай всички гаранции, предвидени в част 3 от ЗЗД от 2018 г. и анализирани по-горе, се прилагат за обработването, извършвано от получаващия орган.

(124) В правния ред на Обединеното кралство различни закони изрично позволяват последващо споделяне. По-специално i) Законът за цифровата икономика от 2017 г. позволява споделянето между публичните органи за няколко цели, например в случай на измама срещу публичния сектор, която би довела до загуба или риск от загуба за публичен орган ([200]) или в случай на дълг към публичен орган или към Короната ([201]); ii) Законът за престъпленията и съдилищата от 2013 г. позволява споделянето на информация с Националната агенция по престъпността (NCA) ([202]) с цел борба, разследване и наказателно преследване на тежката и организираната престъпност; iii) Законът за тежките престъпления от 2007 г. позволява на публичните органи да разкриват информация на организации за борба с измамите с цел предотвратяване на измами ([203]).

(125) В тези закони изрично се предвижда, че споделянето на информация следва да става в съответствие с правилата, предвидени в ЗЗД от 2018 г. Освен това Полицейският колеж издаде Разрешена професионална практика относно споделянето на информация ([204]), за да помогне на полицията да изпълнява задълженията си за защита на данните съгласно ОРЗД на Обединеното кралство, ЗЗД и Закона за правата на човека от 1998 г. Дали споделянето е съобразено с приложимата правна уредба за защита на данните, разбира се, подлежи на съдебен контрол ([205]).

(126) Освен това, подобно на предвиденото в член 9 от Директива (ЕС) 2016/680, в ЗЗД от 2018 г. се предвижда, че лични данни, събрани за целите на правоприлагането, могат да бъдат обработвани за цел, различна от правоприлагането, когато обработването е разрешено от закона ([206]). Този вид споделяне обхваща два случая: 1) когато правоприлагащ орган в областта на наказателното право споделя данни с правоприлагащ орган в друга правна област, различен от разузнавателна агенция (като например финансов или данъчен орган, орган за защита на конкуренцията, служба за

([198]) Член 8, параграф 1 от Закона за правата на човека от 1998 г.

([199]) Член 36, параграф 3 от ЗЗД от 2018 г.

([200]) Член 56 от Закона за цифровата икономика от 2017 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) Член 48 от Закона за цифровата икономика от 2017 г.

([202]) Член 7 от Закона за престъпленията и съдилищата от 2013 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2013/22/contents.

([203]) Член 68 от Закона за тежките престъпления от 2007 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([204]) Разрешената професионална практика относно споделянето на информация е достъпна на следния адрес: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

([205]) Вж. напр. дело *M/the Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), по което от Висшия съд е поискано да разгледа възможността за споделяне на данни между полицията и Партньорството за намаляване на икономическата престъпност (BCRP) — организация, оправомощена да управлява схема за уведомяване за отстраняване, с която на лица се забранява да влизат в търговските помещения на нейните членове. Съдът разглежда споделянето на данни, което се осъществява въз основа на споразумение, имащо за цел защита на обществеността и предотвратяване на престъпления, и в крайна сметка стига до заключението, че повечето аспекти на споделянето на данни са законосъобразни, с изключение на определена чувствителна информация, споделяна между полицията и BCRP. Друг пример е дело *Cooper/NCA* [2019] EWCA Civ 16, в което Апелативният съд потвърждава споделянето на данни между полицията и Агенцията по тежката организирана престъпност (SOCA), която понастоящем е част от NCA.

([206]) Член 36, параграф 4 от ЗЗД от 2018 г.

закрила на младежта); 2) когато правоприлагащ орган в областта на наказателното право споделя данни с разузнавателна агенция. В първия случай обработването на лични данни ще попадне в приложното поле на ОРЗД на Обединеното кралство, както и в това на част 2 от ЗЗД от 2018 г. Както е посочено в решението, прието съгласно Регламент (ЕС) 2016/679, гаранциите, предвидени в ОРЗД на Обединеното кралство и в част 2 от ЗЗД от 2018 г., осигуряват ниво на защита, което по същество е равностойно на предоставяното в Съюза ([207]).

(127) Във втория случай, по отношение на споделянето на данни, събрани от правоприлагащ орган в областта на наказателното право, с разузнавателна агенция за целите на националната сигурност, правното основание, което разрешава такова споделяне, е Законът за борба с тероризма от 2008 г. (ЗБТ от 2008 г.) ([208]). Съгласно ЗБТ от 2008 г. всяко лице може да предоставя информация на всяка от разузнавателните служби с цел изпълнение на някоя от функциите на тази служба, включително „националната сигурност“.

(128) Що се отнася до условията, при които данните могат да бъдат споделяни за целите на националната сигурност, Законът за разузнавателните служби и Законът за службите за сигурност ограничават възможността на разузнавателните служби да получават данни до това, което е необходимо за изпълнение на техните законоустановени функции. Компетентните органи, които попадат в обхвата на част 3 от ЗЗД от 2018 г. и които желаят да споделят данни с разузнавателните служби, ще трябва да вземат предвид редица фактори/ограничения в допълнение към законоустановените функции на агенциите, определени в Закона за разузнавателните служби и Закона за службите за сигурност ([209]). В член 20 от ЗБТ от 2008 г. се пояснява, че всяко споделяне на данни съгласно член 19 от ЗБТ от 2008 г. трябва да продължава да е в съответствие със законодателството за защита на данните. Това означава, че се прилагат всички ограничения и изисквания на ЗЗД от 2018 г. Освен това правоприлагащите органи и разузнавателните служби са публични органи за целите на Закона за правата на човека от 1998 г. и следователно трябва да гарантират, че действат в съответствие с правата, гарантирани от ЕКПЧ, включително член 8 от нея. С други думи, тези изисквания означават, че всяко споделяне на данни между правоприлагащите органи и разузнавателните служби е в съответствие със законодателството за защита на данните и ЕКПЧ.

(129) Спрямо обработването от страна на разузнавателните служби на лични данни, получени от правоприлагащите органи за целите на националната сигурност, се прилагат редица условия и гаранции ([210]). Част 4 от ЗЗД от 2018 г. се прилага за всяко обработване от разузнавателните служби или от тяхно име. В нея се определят основните

([207]) Решение за изпълнение на Комисията съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство (C(2021) 4800).

([208]) Член 19 от Закона за борба с тероризма от 2008 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) В член 2, параграф 2 от Закона за разузнавателните служби от 1994 г. (вж. https://www.legislation.gov.uk/ukpga/1994/13/contents) се предвижда, че „Началникът на Разузнавателната служба отговаря за ефикасността на тази служба и е длъжен да гарантира, че: а) са налице мерки за гарантиране, че Разузнавателната служба не получава информация, освен доколкото това е необходимо за правилното изпълнение на функциите ѝ, и че тя не разкрива информация, освен доколкото това е необходимо i) за тази цел; ii) в интерес на националната сигурност; iii) за целите на предотвратяването или разкриването на тежки престъпления; или iv) за целите на наказателно производство; и б) че Разузнавателната служба не предприема никакви действия за прокарване на интересите на някоя политическа партия в Обединеното кралство“, докато в член 2, параграф 2 от Закона за службите за сигурност от 1989 г. (вж. https://www.legislation.gov.uk/ukpga/1989/5/contents) се предвижда, че „Генералният директор отговаря за ефикасността на Службата и е длъжен да гарантира, че: а) са налице мерки за гарантиране, че Службата не получава информация, освен доколкото това е необходимо за правилното изпълнение на функциите ѝ, нито разкрива информация, освен доколкото това е необходимо за тази цел или за целите на предотвратяването или разкриването на тежки престъпления, или за целите на наказателно производство; и б) че Службата не предприема никакви действия за прокарване на интересите на някоя политическа партия; и в) че са налице мерки, договорени с генералния директор на Националната агенция по престъпността, за координиране на дейностите на Службата съгласно член 1, параграф 4 от този закон с дейностите на полицейските сили, Националната агенция по престъпността и други правоприлагащи органи“.

([210]) Гаранциите и ограниченията на правомощията на разузнавателните служби се уреждат и от Закона за правомощията за разследване от 2016 г., в който, наред със Закона за уреждане на правомощията за разследване от 2000 г. за Англия, Уелс и Северна Ирландия и Закона за уреждане на правомощията за разследване (Шотландия) от 2000 г. за Шотландия, е предвидено правното основание за използването на тези правомощия. Тези правомощия обаче не са от значение в контекста на „последващото споделяне“, тъй като обхващат прякото събиране на лични данни от разузнавателните агенции. За оценка на правомощията, предоставени на разузнавателните агенции съгласно Закона за уреждане на правомощията за разследване, вж. Решение за изпълнение на Комисията съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство (C(2021) 4800).

принципи за защита на данните (законосъобразност, справедливост и прозрачност ([211]); ограничаване в рамките на целта ([212]); свеждане на данните до минимум ([213]); точност ([214]); ограничение на съхранението ([215]) и сигурност ([216])), поставят се условия за обработването на специални категории данни ([217]), предоставят се права на субектите на данни ([218]), изисква се защита на данните на етапа на проектирането ([219]) и се урежда международното предаване на лични данни ([220]).

(130) В същото време член 110 от ЗЗД от 2018 г. предвижда освобождаване от действието на определени разпоредби от част 4 на ЗЗД от 2018 г., когато такова освобождаване е необходимо за гарантиране на националната сигурност. В член 110, параграф 2 от ЗЗД от 2018 г. са изброени разпоредбите, от които се допуска освобождаване. То включва принципите за защита на данните (с изключение на принципа на законосъобразност), правата на субекта на данни, задължението за информиране на комисаря по информацията относно нарушение на сигурността на данните, правомощията на комисаря по информацията да извършва проверки в съответствие с международните задължения, някои от правомощията на комисаря по информацията за привеждане в изпълнение, разпоредбите, които криминализират определени нарушения на защитата на данните, и разпоредбите, свързани с обработване поради специални цели, като например журналистически, академични или художествени. Това освобождаване може да се използва въз основа на анализа на всеки отделен случай ([221]). Както е обяснено от органите на Обединеното кралство и потвърдено от съдебната практика на съдилищата на Обединеното кралство, „а) администраторът трябва да вземе предвид действителните последици за националната сигурност или отбрана, ако трябва да спазва конкретната разпоредба за защита на данните и ако би могъл разумно да спази обичайното правило, без да се засяга националната сигурност или отбрана“ ([222]). Дали освобождаването е било използвано по подходящ начин, подлежи на надзор от страна на ICO ([223]).

([211]) Съгласно член 86, параграф 6 от ЗЗД от 2018 г., за да се определят справедливостта и прозрачността на обработването, следва да се вземе предвид методът, по който са получени данните. В този смисъл изискването за справедливост и прозрачност е изпълнено, ако данните са получени от лице, което е законно оправомощено или е длъжно да ги предостави.

([212]) Съгласно член 87 от ЗЗД от 2018 г. целите на обработването трябва да бъдат конкретни, изрично указани и легитимни. Данните не трябва да се обработват по начин, който е несъвместим с целите, за които се събират. Съгласно член 87, параграф 3 по-нататъшно съвместимо обработване на лични данни може да бъде разрешено само ако администраторът е оправомощен по закон да обработва данните за тази цел и обработването е необходимо и пропорционално на тази друга цел. Обработването следва да се счита за съвместимо, ако се състои в обработване за целите на архивиране в обществен интерес, за целите на научни или исторически изследвания или за статистически цели и при прилагането на подходящи гаранции (член 87, параграф 4 от ЗЗД от 2018 г.).

([213]) Личните данни трябва да бъдат подходящи, относими и не надхвърлят необходимото (член 88 от ЗЗД от 2018 г.).

([214]) Личните данни трябва да бъдат точни и актуални (член 89 от ЗЗД от 2018 г.).

([215]) Личните данни не трябва да се съхраняват по-дълго от необходимото (член 90 от ЗЗД от 2018 г.).

([216]) Шестият принцип на защитата на данните е, че личните данни трябва да се обработват по начин, който включва вземането на подходящи мерки за сигурност по отношение на рисковете, произтичащи от обработването на лични данни. Рисковете включват (но не се ограничават до) случаен или неразрешен достъп до лични данни или унищожаване, загуба, използване, промяна или разкриване на лични данни (член 91 от ЗЗД от 2018 г.). В член 107 също така се изисква 1) всеки администратор да прилага съответни мерки за сигурност, подходящи за рисковете, произтичащи от обработването на лични данни, и 2) в случай на автоматизирано обработване всеки администратор и всеки обработващ лични данни да прилага, въз основа на оценка на риска, предотвратяващи или ограничаващи риска мерки.

([217]) Член 86, параграф 2, буква b) и приложение 10 от ЗЗД от 2018 г.

([218]) Част 4, глава 3 от ЗЗД от 2018 г., по-специално правата: на достъп, коригиране и заличаване, на възражение срещу обработването и спрямо тях да не се прилага автоматизирано вземане на решения, на намеса в автоматизирано вземане на решения и да бъдат информирани относно процеса на вземане на решения. Освен това администраторът трябва да предостави на субекта на данни информация относно обработването на неговите лични данни.

([219]) Член 103 от ЗЗД от 2018 г.

([220]) Член 109 от ЗЗД от 2018 г. Предаването на лични данни на международни организации или държави извън Обединеното кралство е възможно, ако предаването е необходима и пропорционална мярка, която се извършва за целите на законоустановените функции на администратора или за други цели, предвидени в конкретни разпоредби на Закона за службите за сигурност от 1989 г. и Закона за разузнавателните служби от 1994 г.

([221]) Вж. дело *Baker/Secretary of State for the Home Department* [2001] UKIT NSA2 („*Baker/Secretary of State*“).

([222]) Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална рамка за защита на данните и разследващите правомощия, стр. 15—16, достъпна на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Вж. също решение по дело *Baker/Secretary of State* (вж. по-горе бележка под линия 220), в което Трибуналът отменя удостоверение за национална сигурност, издадено от министъра на вътрешните работи, и потвърждава прилагането на изключението, свързано с националната сигурност, като счита, че няма причина да се предвиди общо изключение от задължението за отговор на искания за достъп и че допускането на такова изключение при всички обстоятелства без анализ на всеки отделен случай надхвърля необходимото и пропорционалното за защитата на националната сигурност.

([223]) Вж. Меморандум за разбирателство между ICO и UKIC, съгласно който „При получаване на жалба от субект на данни ICO ще иска да се увери, че въпросът е бил разгледан правилно и, когато е приложимо, че прилагането на всяко освобождаване е било използвано по подходящ начин“ (Меморандум за разбирателство между Службата на комисаря по информацията (ICO) и разузнавателната общност на Обединеното кралство (UKIC), точка 16, достъпен на следния линк: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Освен това във връзка с възможността за ограничаване на някое от горепосочените права с цел защита на „националната сигурност“ член 79 от ЗЗД от 2018 г. дава възможност на администратора да подаде заявление за удостоверение, подписано от министър или от главния прокурор, удостоверяващо, че ограничаването на тези права представлява или в определен момент е представлявало необходима и пропорционална мярка за защита на националната сигурност ([224]). Правителството на Обединеното кралство издаде насоки относно удостоверенията за национална сигурност съгласно ЗЗД от 2018 г., в които по-специално се подчертава, че всяко ограничаване на правата на субектите на данни с цел опазване на националната сигурност трябва да бъде пропорционално и необходимо ([225]). Всички удостоверения за национална сигурност трябва да бъдат публикувани на уебсайта на ICO ([226]).

(132) Удостоверението следва да бъде за определен срок, не по-дълъг от пет години, така че да бъде редовно преразглеждано от орган на изпълнителната власт ([227]). В удостоверението се посочват личните данни или категориите лични данни, предмет на освобождаването, както и разпоредбите на ЗЗД от 2018 г., за които се прилага освобождаването ([228]).

(133) Важно е да се отбележи, че удостоверенията за национална сигурност не предвиждат допълнително основание за ограничаване на правата за защита на данните поради съображения, свързани с националната сигурност. С други думи, администраторът или обработващият лични данни може да използва удостоверение само когато е стигнал до заключението, че е необходимо да се използва освобождаването, свързано с националната сигурност, като то трябва да се прилага въз основа на анализа на всеки отделен случай. Дори ако по отношение на въпросния случай се прилага удостоверение за национална сигурност, ICO може да проучи дали в конкретен случай е оправдано да се използва освобождаването, свързано с националната сигурност ([229]).

(134) Всяко лице, пряко засегнато от издаването на удостоверението, може да обжалва решението за издаване на удостоверението ([230]) пред трибунала от по-горна инстанция ([231]) или, когато удостоверението идентифицира данни чрез общо описание, да оспори прилагането на удостоверението по отношение на конкретни данни ([232]).

(135) Трибуналът ще преразгледа решението за издаване на удостоверение и ще реши дали са били налице основателни причини за издаването му ([233]). Той може да разгледа широк кръг от въпроси, включително да прецени необходимостта, пропорционалността и законосъобразността, като отчита въздействието върху правата на субектите на данни и претегли необходимостта от опазване на националната сигурност. В резултат на това трибуналът може да реши, че удостоверението не се прилага за конкретни лични данни, които са предмет на обжалването ([234]).

([224]) ЗЗД от 2018 г. отмени възможността за издаване на удостоверение съгласно член 28, параграф 2 от Закона за защита на данните от 1998 г. Въпреки това възможността за издаване на „стари удостоверения“ все още съществува, доколкото е налице възможност за оспорване съгласно Закона от 1998 г. (вж. част 5, точка 17 от приложение 20 към ЗЗД от 2018 г.). Тази възможност обаче изглежда много рядка и ще се прилага само в ограничени случаи, например когато субектът на данни оспорва използването на изключението, свързано с националната сигурност, във връзка с обработване от публичен орган, който е извършил обработването съгласно Закона от 1998 г. Следва да се отбележи, че в тези случаи член 28 от ЗЗД от 1998 г. ще се прилага изцяло, и следователно това включва възможността субектът на данни да оспори удостоверението. В момента няма удостоверения за национална сигурност, издадени съгласно ЗЗД от 1998 г.

([225]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност съгласно Закона за защита на данните от 2018 г., достъпни на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) Съгласно член 130 от ЗЗД от 2018 г. ICO може да реши да не публикува текста или част от текста на удостоверението, ако това би било в противоречие с интересите на националната сигурност или с обществения интерес, или би могло да застраши безопасността на което и да е лице. В тези случаи обаче ICO ще публикува факта, че удостоверението е било издадено.

([227]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност, точка 15, вж. бележка под линия 225.

([228]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност, точка 5, бележка под линия 225.

([229]) Член 102 от ЗЗД от 2018 г. изисква администраторът да може да докаже, че е спазил разпоредбите на ЗЗД от 2018 г. Това означава, че разузнавателната служба ще трябва да докаже на ICO, че когато използва освобождаването, тя е разгледала конкретните обстоятелства по случая. ICO публикува и регистър на удостоверенията за национална сигурност, който е достъпен на следния адрес: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Член 111, параграф 3 от ЗЗД от 2018 г.

([231]) Трибуналът от по-горна инстанция е съдът, компетентен да разглежда жалби срещу решения, постановени от административни трибунали от по-долна инстанция, и има специална компетентност за пряко обжалване на решения на определени държавни органи.

([232]) Член 111, параграф 5 от ЗЗД от 2018 г.

([233]) В дело *Baker/Secretary of State* (вж. по-горе бележка под линия 221), Трибуналът отмени удостоверение за национална сигурност, издадено от министъра на вътрешните работи, като счете, че няма причина да се предвиди общо изключение от задължението за отговаряне на искания за достъп и че допускането на такова изключение при всички обстоятелства, без анализ на всеки отделен случай, надхвърля необходимото и пропорционалното за защитата на националната сигурност.

([234]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност, точка 25, бележка под линия 225.

(136) Различен набор от възможни ограничения се отнася до тези, които се прилагат съгласно приложение 11 към ЗЗД от 2018 г. за някои разпоредби на част 4 от ЗЗД от 2018 г. ([235]) с цел защита на други важни цели от обществен интерес или защитени интереси, като например парламентарния имунитет, адвокатската тайна, провеждането на съдебни производства или бойната готовност на въоръжените сили. Тези разпоредби не се прилагат (освобождаване) за определени категории информация („на база категории“) или доколкото прилагането им би могло да накърни защитения интерес („на база накърняване“) ([236]). Позоваване на освобождаването на база накърняване може да се прави само дотолкова, доколкото прилагането на въпросната разпоредба за защита на данните би могло да накърни конкретния интерес. Следователно използването на освобождаване трябва винаги да бъде обосновано с позоваване на съответното накърняване на интерес, което би могло да настъпи в конкретния случай. Освобождаването на база категории може да се използва само по отношение на конкретната, тясно определена категория информация, за която е предоставено освобождаване. Този тип освобождаване е сходно по цел и последици с няколко от освобожданията от действието на ОРЗД на Обединеното кралство (съгласно приложение 2 към ЗЗД от 2018 г.), които на свой ред отразяват тези, предвидени в член 23 от ОРЗД.

(137) От гореизложеното следва, че са налице ограничения и условия съгласно приложимите правни разпоредби на Обединеното кралство, както се тълкуват също така от съдилищата и от комисаря по информацията, за да се гарантира, че тези освобождавания и ограничения остават в границите на това, което е необходимо и пропорционално за защита на националната сигурност.

(138) Обработването на лични данни, извършвано от разузнавателните служби съгласно част 4 от ЗЗД от 2018 г., се надзирава от комисаря по информацията ([237]).

(139) Общите функции на комисаря по информацията във връзка с обработването на лични данни от разузнавателните служби съгласно част 4 от ЗЗД от 2018 г. са определени в приложение 13 към ЗЗД от 2018 г. Задачите му включват, без това изброяване да е изчерпателно, наблюдение и привеждане в изпълнение на част 4 от ЗЗД от 2018 г., повишаване на обществената осведоменост, предоставяне на консултации на Парламента, правителството и други институции относно законодателните и административните мерки, повишаване на осведомеността на администраторите и обработващите лични данни за техните задължения, предоставяне на информация на субекта на данни относно упражняването на неговите права и провеждане на разследвания.

(140) Що се отнася до част 3 от ЗЗД от 2018 г., комисарят има правомощието да уведомява администраторите за твърдяно нарушение и да отправя предупреждения, че има вероятност дадено обработване да наруши правилата, както и да отправя официални предупреждения при потвърждаване на нарушението. Той може също така да издава изпълнителни и наказателни постановления за нарушения на определени разпоредби от закона ([238]). Въпреки това, за разлика от другите части на ЗЗД от 2018 г., комисарят не може да издаде ревизионно постановление на орган, свързан с националната сигурност ([239]).

(141) Освен това в член 110 от ЗЗД от 2018 г. се предвижда изключение от използването на определени правомощия на комисаря, когато това е необходимо за целите на опазването на националната сигурност. Това включва правомощието на комисаря да издава (всякакъв вид) постановления съгласно ЗЗД (информационни, ревизионни, изпълнителни и наказателни), правомощието да извършва проверки в съответствие с международните задължения,

([235]) Това включва: i) принципите за защита на данните от част 4, с изключение на изискването за законосъобразност на обработването съгласно първия принцип и факта, че обработването трябва да отговаря на едно от съответните условия, посочени в приложения 9 и 10; ii) правата на субектите на данни; и iii) задълженията, свързани с докладването на нарушения на ICO.

([236]) Съгласно Обяснителната рамка на Обединеното кралство освобожданията на база категории включват: i) информацията за присъждането на кралски почести и отличия; ii) адвокатската тайна; iii) поверителната информация, свързана с трудово правоотношение, обучение или образование; и iv) изпитните протоколи и оценки. Освобождаването на база накърняване на интерес обхваща следните въпроси: i) предотвратяването или разкриването на престъпления; задържането и наказателното преследване на извършители на престъпления; ii) парламентарния имунитет; iii) съдебните производства; iv) бойната готовност на въоръжените сили на Короната; v) икономическото благосъстояние на Обединеното кралство; vi) преговорите със субекта на данни; vii) научните или историческите изследвания или статистическите цели; viii) архивирането в обществен интерес. Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална сигурност, стр. 13, вж. бележка под линия 222.

([237]) Член 116 от ЗЗД от 2018 г.

([238]) Съгласно член 149, параграф 2 във връзка с член 155 от ЗЗД от 2018 г. на администратора или обработващия лични данни могат да бъдат издадени изпълнителни и наказателни постановления във връзка с нарушения по част 4, глава 2 от ЗЗД от 2018 г. (принципи на обработването), на разпоредба на част 4 от ЗЗД от 2018 г., предоставяща права на субект на данни, на изискване за съобщаване на комисаря за нарушение на сигурността на личните данни съгласно член 108 от ЗЗД от 2018 г. и на принципите за предаване на лични данни на трети държави, държави, които не са страни по Конвенцията, и международни организации, посочени в член 109 от ЗЗД от 2018 г. (За повече подробности относно изпълнителните и наказателните постановления вж. съображения 102—103).

([239]) Съгласно член 147, параграф 6 от ЗЗД от 2018 г. комисарят по информацията не може да издава ревизионно постановление на орган, посочен в член 23, параграф 3 от Закона за свободата на информацията от 2000 г. Това включва Службата за сигурност (*MI5*), Тайната разузнавателна служба (*MI6*) и Държавния комуникационен щаб (*Government Communications Headquarter*).

правомощията за влизане и проверка, както и правилата относно нарушенията ([240]). Както е обяснено в съображение 136, тези изключения ще се прилагат само ако е необходимо и пропорционално и въз основа на анализа на всеки отделен случай. Прилагането на тези изключения може да подлежи на съдебен контрол ([241]).

(142) ICO и разузнавателните служби на Обединеното кралство подписаха меморандум за разбирателство ([242]), с който се установява рамка за сътрудничество по редица въпроси, включително уведомленията за нарушения на сигурността на данните и разглеждането на жалбите на субектите на данни. По-специално в него се предвижда, че при получаване на жалба ICO преценява дали е направено законосъобразно позоваване на освобождаване, свързано с националната сигурност. Отговорите на запитвания, отправени от ICO в контекста на разглеждането на индивидуални жалби, трябва да бъдат дадени в срок от 20 работни дни в съответствие със съответните Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност съгласно Закона за защита на данните, като се използват подходящи сигурни канали, ако тези отговори включват класифицирана информация. От април 2018 г. до момента ICO е получила 21 жалби от физически лица относно разузнавателните служби. Всяка жалба беше оценена и резултатът беше съобщен на субекта на данни ([243]).

(143) Освен това Комисията по разузнаване и сигурност (ISC) упражнява парламентарен надзор върху обработването на данни от разузнавателните агенции. Тази комисия има своето правно основание в Закона за правосъдието и сигурността от 2013 г. (ЗПС от 2013 г.) ([244]). Със Закона ISC се създава като комисия на Парламента на Обединеното кралство. ISC се състои от членове, принадлежащи към двете камари на Парламента и назначени от министър-председателя след консултация с лидера на опозицията ([245]). От ISC се изисква да представя на Парламента годишен доклад относно изпълнението на своите функции и други доклади, които счита за подходящи ([246]).

(144) От 2013 г. на ISC бяха предоставени по-големи правомощия, включително надзор на оперативните дейности на службите за сигурност. Съгласно член 2 от ЗПС от 2013 г., ISC има за задача да надзирава разходите, администрирането, политиките и операциите на националните агенции за сигурност. В ЗПС от 2013 г. се уточнява,

([240]) Разпоредбите, от които може да бъде получено освобождаване, са: член 108 (съобщаване на комисаря за нарушение на сигурността на личните данни), член 119 (проверка в съответствие с международните задължения); членове 142—154 и приложение 15 (постановления на комисаря и правомощия за влизане и проверка); и членове 170—173 (нарушения, свързани с лични данни). Освен това във връзка с обработването от разузнавателните служби, предвидено в точка 1, букви a) и g) и точка 2 от приложение 13 (други общи функции на комисаря).

([241]) Виж например дело *Baker/Secretary of State for the Home Department* (вж. бележка под линия 221).

([242]) Меморандум за разбирателство между ICO и разузнавателната общност на Обединеното кралство, вж. бележка под линия 231.

([243]) В седем от тези случаи ICO е посъветвала жалбоподателя да повдигне въпроса пред администратора на лични данни (такъв е случаят, когато дадено лице е изпратило жалба до ICO, но първо е трябвало да изпрати запитване до администратора на данни), в един от тези случаи ICO е предоставила общи съвети на администратора на данни (това се използва, когато действията на администратора на лични данни не изглежда да са в нарушение на законодателството, но подобряване на практиките е можело да предотврати проблема, с който ICO е сезирана), а в останалите 13 случая не е било необходимо предприемането на действия от администратора на данни (това се използва, когато проблемът, повдигнат от лицето, попадат в обхвата на Закона за защита на данните от 2018 г., защото засяга обработването на лични данни, но въз основа на предоставената информация не изглежда администраторът да е нарушил законодателството).

([244]) Както беше обяснено от органите на Обединеното кралство, със ЗПС бяха разширени правомощията на ISC, за да ѝ отредят роля в надзора на разузнавателната общност отвъд трите агенции и да ѝ се даде възможност за ретроспективен надзор на оперативните дейности на агенциите по въпроси от значителен национален интерес.

([245]) Член 1 от ЗПС от 2013 г. Министрите не отговарят на условията за членство. Членовете на ISC заемат длъжността си за срока на мандата на Парламента, по време на който са били назначени. Те могат да бъдат отстранени с решение на камарата на Парламента, от чиято квота са били назначени, или ако престанат да бъдат членове на Парламента или станат министри. Всеки член може също така да подаде оставка.

([246]) Докладите и изявленията на Комисията са достъпни онлайн на следния адрес: http://isc.independent.gov.uk/committee-reports. През 2015 г. ISC публикува доклад относно „Неприкосновеност на личния живот и сигурността: модерна и прозрачна правна уредба“ (вж.: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf), в който се разглежда правната уредба на техниките за наблюдение, използвани от разузнавателните агенции, и в който бяха отправени редица препоръки, които след това бяха разгледани и включени в Законопроекта за правомощията за разследване, който бе приет и стана ЗПР от 2016 г. Отговорът на правителството на доклада относно неприкосновеността на личния живот и сигурността е достъпен на следния адрес: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

че ISC има право да провежда разследвания по оперативни въпроси, когато те не са свързани с текущи операции ([247]). Меморандумът за разбирателство, договорен между министър-председателя и ISC ([248]), уточнява подробно елементите, които трябва да се вземат предвид, когато се преценява дали дадена дейност не е част от текуща операция ([249]). Министър-председателят може да поиска от ISC да разследва текущи операции и ISC може да прави преглед на информацията, предоставена доброволно от агенциите.

(145) Съгласно приложение 1 към ЗПС от 2013 г. ISC може да поиска от ръководителите на всяка една от трите разузнавателни служби да разкрият всякаква информация. Агенцията трябва да предостави тази информация, освен ако министърът не наложи вето ([250]). Органите на Обединеното кралство обясниха, че на практика много малко информация не достига до ISC ([251]).

(146) По отношение на средствата за правна защита, на първо място, съгласно член 165, параграф 2 от ЗЗД от 2018 г. субектът на данни може да подаде жалба до ICO, ако счита, че във връзка с отнасящите се до него лични данни е налице нарушение на част 4 от ЗЗД от 2018 г., включително всяко неправомерно използване на дерогациите и ограниченията, свързани с националната сигурност.

(147) Освен това съгласно част 4 от ЗЗД от 2018 г. физическите лица имат право да поискат от Висшия съд (или Върховния съд по граждански дела (Court of Session) в Шотландия) да постанови мярка, с която на администратора се разпорежда да спазва правото на достъп до данните ([252]), да възразят срещу обработването ([253]) и на коригиране или изтриване.

(148) Физическите лица също така имат право да поискат обезщетение за вреди от администратора или обработващия лични данни, претърпени поради нарушение на изискване на част 4 от ЗЗД от 2018 г. ([254]). Вредите включват както финансови загуби, така и вреди, които не са свързани с финансови загуби, като например емоционално страдание ([255]).

(149) Накрая, дадено лице може да подаде жалба до Трибунала за правомощията за разследване (Investigatory Powers Tribunal) за всяко действие, извършено пряко от или от името на разузнавателните агенции на Обединеното кралство ([256]). Трибуналът за правомощията за разследване (IPT) е създаден със Закона за уреждане на правомощията за разследване от 2000 г. за Англия, Уелс и Северна Ирландия и Закона за уреждане на правомощията за разследване (Шотландия) от 2000 г. за Шотландия (ЗУПР от 2000 г.) и е независим от изпълнителната власт ([257]). В съответствие с член 65 от ЗУПР от 2000 г. членовете на IPT се назначават от Нейно Величество за срок от пет години.

(150) Член на Трибунала може да бъде отстранен от длъжност от Нейно величество след обръщение ([258]) от страна на двете камари на Парламента ([259]).

(151) За да предяви иск пред IPT („изискване за процесуална легитимация“), съгласно член 65 от ЗУПР от 2000 г. дадено лице трябва да е убедено, че i) спрямо него, спрямо негова собственост, спрямо съобщения, изпратени от него или до него, или предназначени за него, или спрямо използването от него на пощенска или далекосъобщителна услуга, или далекосъобщителна система ([260]) е било извършено действие от разузнавателна служба, и ii) че действието е

([247]) Член 2 от ЗПС от 2013 г.
([248]) Меморандум за разбирателство между министър-председателя и ISC, достъпен на следния адрес: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf.
([249]) Меморандум за разбирателство между министър-председателя и ISC, точка 14, вж. бележка под линия 248.
([250]) Министърът може да наложи вето върху разкриването на информация само на две основания: информацията е чувствителна и не следва да се разкрива на ISC в интерес на националната сигурност; или информацията е от такъв характер, че ако от министъра бъде изискано да я представи пред специална парламентарна комисия на Камарата на общините, министърът ще счете (не само на основания, засягащи националната сигурност) за неуместно да го направи (точка 4, подточка 2 от приложение 1 към ЗПС от 2013 г.)
([251]) Обяснителна рамка на Обединеното кралство, раздел H: Национална сигурност, стр. 43.
([252]) Член 94, параграф 11 от ЗЗД от 2018 г.
([253]) Член 99, параграф 4 от ЗЗД от 2018 г.
([254]) Член 169 от Закона за защита на данните от 2018 г., с който се допускат искове от „лице, което претърпява вреди поради нарушение на изискване на законодателството за защита на данните“.
([255]) Член 169, параграф 5 от ЗЗД от 2018 г.
([256]) Вж. член 65, параграф 2, буква b) от ЗУПР.
([257]) Съгласно приложение 3 към ЗУПР от 2000 г. членовете трябва да имат определен съдебен опит и имат право на преназначаване.
([258]) Относно понятието „обръщение“ вж. бележка под линия 183.
([259]) Точка 1, подточка 5 от приложение 3 към ЗУПР от 2000 г.
([260]) Член 65, параграф 4 от ЗУПР от 2000 г.

извършено при „подлежащи на обжалване обстоятелства“ ([261]) или „е извършено от или за сметка на разузнавателни служби“ ([262]). Тъй като по-специално понятието „убедено“ се тълкува доста широко ([263]), завеждането на дело пред Трибунала подлежи на сравнително ниски изисквания за процесуална легитимация.

(152) Когато Трибуналът разглежда жалба, подадена до него, той е длъжен да разследва дали лицата, за които в жалбата са направени определени твърдения, са имали контакт с жалбоподателя, както и да разследва органа, за който се твърди, че е участвал в нарушенията, и дали твърдяното действие е било извършено ([264]). Когато води дадено производство, Трибуналът трябва да прилага същите принципи за произнасяне в това производство, които биха били приложени от него във връзка с молба за съдебен контрол ([265]).

(153) Трибуналът трябва да уведоми жалбоподателя дали жалбата е решена в негова полза или не ([266]). Съгласно член 67, параграфи 6 и 7 от ЗУПР от 2000 г. Трибуналът има правомощието да налага временни мерки и да присъжда обезщетение или да постановява всяко друго решение, което счита за уместно ([267]). Съгласно член 67а от ЗУПР от 2000 г. решението на Трибунала може да бъде обжалвано, при условие че бъде допуснато от Трибунала или от съответния въззивен съд.

(154) По-специално, физическите лица могат да предявят иск и да получат правна защита от IPT, когато считат, че публичен орган е действал (или възнамерява да действа) по начин, който е несъвместим с правата на ЕКПЧ, включително правото на неприкосновеност на личния живот и на защита на данните, и който следователно е незаконосъобразен съгласно член 6, параграф 1 от Закона за правата на човека от 1998 г. На IPT е предоставена изключителна компетентност по отношение на всички искове по Закона за правата на човека във връзка с разузнавателните агенции. Това означава, както отбелязва Висшият съд (*High Court*), че „дали е налице нарушение на Закона за правата на човека по отношение на фактите по конкретно дело, е нещо, което по принцип може да бъде повдигнато пред и отсъдено от независим трибунал, който има достъп до всички релевантни материали, включително до секретни материали. […] В този контекст също така имаме предвид, че решенията на IPT вече могат да бъдат обжалвани пред подходящ въззивен съд (в Англия и Уелс, това ще бъде Апелативният съд); и че Върховният съд наскоро реши, че актовете на IPT по принцип подлежат на съдебен контрол: вж. *R (Privacy International)/Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219“ ([268]). Ако IPT установи, че акт на публичен орган е незаконосъобразен, той може да предостави такова поправяне на вредите или обезщетение или да постанови такава мярка, в рамките на своите правомощия, каквито счита за справедливи и подходящи ([269]).

([261]) Такива обстоятелства се отнасят до действия на публичните органи при упражняване на публична власт (напр. заповед, разрешение/постановление за получаване на съобщения и др.), или ако обстоятелствата са такива, че (независимо дали има упражняване на публична власт) не би било уместно действията да се извършат без упражняването ѝ или най-малкото без надлежно разглеждане на въпроса дали следва да се приложи такова упражняване на публична власт. Счита се, че действията, разрешени от съдебен комисар, са извършени при подлежащи на обжалване обстоятелства (член 65, параграф 7ZA от ЗУПР от 2000 г.), докато други действия, извършени с разрешението на лице, заемащо съдебна длъжност, не се считат за извършени при подлежащи на обжалване обстоятелства (член 65, параграфи 7 и 8 от ЗУПР от 2000 г.).

([262]) Според информацията, предоставена от органите на Обединеното кралство, ниският праг за подаване на жалба води до това, че не е необичайно разследването на Трибунала да установи, че жалбоподателят в действителност никога не е бил обект на разследване от публичен орган. В последния статистически доклад на IPT се посочва, че през 2016 г. Трибуналът е получил 209 жалби, 52 % от които са били счетени за недопустими, а 25 % са оставени „без разглеждане“. Органите на Обединеното кралство обясниха, че това означава, че по отношение на жалбоподателя не са били използвани специални разузнавателни средства/правомощия, или че са използвани специални разузнавателни техники и Трибуналът е установил, че действието е законосъобразно. Освен това 11 % от жалбите са били недопустими поради липса на компетентност, били са оттеглени или са били нередовни, 5 % са били недопустими, тъй като не са били подадени в срок, и 7 % са били отсъдени в полза на жалбоподателя. Статистически доклад на Трибунала за правомощията за разследване от 2016 г., достъпен на следния адрес: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf.

([263]) Вж. дело *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH. По това дело IPT, позовавайки се на съдебната практика на ЕСПЧ, приема, че подходящият критерий за проверка на убеждението, че действие, попадащо в обхвата на член 68, параграф 5 от ЗУПР от 2000 г., е извършено пряко от или от името на някоя разузнавателна служба, е дали има основание за такова убеждение, включително факта, че дадено лице може да твърди, че е жертва на нарушение, причинено от самото съществуване на специалните разузнавателни средства или на законодателство, позволяващо специални разузнавателни средства, само ако може да докаже, че поради личното си положение е изложено на риск от прилагането на такива средства спрямо него (вж. *Human Rights Watch/Secretary of State*, т. 41)..

([264]) Член 67, параграф 3 от ЗРРП от 2000 г.

([265]) Член 67, параграф 2 от ЗРРП от 2000 г.

([266]) Член 68, параграф 4 от ЗУПР от 2000 г.

([267]) Това може да включва разпореждане, изискващо унищожаването на цялата информация, съхранявана от някой публичен орган по отношение на лице.

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

([269]) Член 8, параграф 1 от Закона за правата на човека от 1998 г.

(155) След изчерпване на националните средства за правна защита дадено лице може да получи правна защита от Европейския съд по правата на човека за нарушения на правата, гарантирани от ЕКПЧ, включително на правото на неприкосновеност на личния живот и на защита на данните.

(156) От гореизложеното следва, че споделянето от страна на правоприлагащите органи в областта на наказателното право на Обединеното кралство, на данни, предавани съгласно настоящото решение, с други публични органи, включително разузнавателни агенции, е обхванато от ограничения и условия, които гарантират, че такова последващо споделяне ще бъде необходимо и пропорционално и ще подлежи на специални гаранции за защита на данните съгласно ЗЗД от 2018 г. Освен това обработването на данни от съответните публични органи се надзирава от независими органи и засегнатите лица имат достъп до ефективни средства за правна защита.

3. **ЗАКЛЮЧЕНИЕ**

(157) Комисията счита, че част 3 от ЗЗД от 2018 г. гарантира ниво на защита на личните данни, предавани за целите на наказателното правоприлагане от компетентните органи в Съюза на компетентните органи на Обединеното кралство, което по същество е равностойно на гарантираното от Директива (ЕС) 2016/680.

(158) Комисията смята освен това, че като цяло механизмите за упражняване на надзор и възможностите за правна защита, предвидени от правото на Обединеното кралство, позволяват нарушенията да бъдат установени и реално наказани и предоставят на субекта на данни правни средства за защита за получаване на достъп до отнасящите се до него лични данни и в крайна сметка за коригиране или изтриване на такива данни.

(159) Накрая, въз основа на наличната информация относно правния ред на Обединеното кралство Комисията счита, че всяка намеса, свързана с основните права на физическите лица, чиито лични данни се предават от Европейския съюз на Обединеното кралство, от страна на публични органи на Обединеното кралство за цели от обществен интерес, включително в контекста на споделяне на лични данни между правоприлагащите органи и други публични органи, като например националните органи за сигурност, ще бъде ограничена до строго необходимото за постигане на въпросната законна цел, и че съществува ефективна правна защита срещу подобна намеса.

(160) Поради това следва да се вземе решение, че Обединеното кралство осигурява адекватно ниво на защита по смисъла на член 36, параграф 2 от Директива (ЕС) 2016/680, тълкуван в светлината на Хартата на основните права.

(161) Това заключение се основава както на съответния вътрешен режим на Обединеното кралство, така и на международните му ангажименти, по-специално на спазването на Европейската конвенция за правата на човека и признаването на юрисдикцията на Европейския съд по правата на човека. Следователно спазването на такива международни задължения е особено важен елемент от оценката, на която се основава настоящото решение.

4. **ПОСЛЕДИЦИ ОТ НАСТОЯЩОТО РЕШЕНИЕ И ДЕЙСТВИЯ НА ОРГАНИТЕ ЗА ЗАЩИТА НА ДАННИТЕ**

(162) Държавите членки и техните органи са длъжни да предприемат необходимите мерки за спазване на актовете на институциите на Съюза, тъй като тези актове по презумпция са законосъобразни и съответно произвеждат правно действие, докато срокът им на действие не изтече, не бъдат оттеглени, отменени вследствие на жалба за отмяна или обявени за невалидни вследствие на преюдициално запитване или възражение за незаконосъобразност.

(163) Следователно решение на Комисията относно адекватното ниво на защита, прието съгласно член 36, параграф 3 от Директива (ЕС) 2016/680, е обвързващо за всички органи на държавите членки, адресати на решението, включително за независимите им надзорни органи. По-специално по време на периода на прилагане на настоящото решение предаването на данни от администратор или обработващ лични данни в Съюза на администратори или обработващи лични данни в Обединеното кралство може да се извършва без да е необходимо допълнително разрешение.

(164) Същевременно следва да се припомни, че съгласно член 47, параграф 5 от Директива (ЕС) 2016/680 и както е обяснено от Съда в решението по дело *Schrems*, когато национален орган за защита на данните поставя под въпрос, включително въз основа на получена жалба, съгласуваността на дадено решение на Комисията относно адекватното ниво на защита с основните права на неприкосновеност на личния живот и на защита на данните на лицето, националното законодателство трябва да предвижда правни способи, позволяващи на съответния орган да представи възраженията си пред национална юрисдикция, която може да бъде длъжна да отправи преюдициално запитване до Съда на ЕС ([270]).

([270]) Решение по дело *Schrems*, т. 65.

5. НАБЛЮДЕНИЕ, СПИРАНЕ НА ДЕЙСТВИЕТО, ОТМЯНА ИЛИ ИЗМЕНЕНИЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(165) Съгласно член 36, параграф 4 от Директива (ЕС) 2016/680 Комисията трябва да наблюдава постоянно съответните развития в Обединеното кралство след приемането на настоящото решение, за да прецени дали то все още осигурява равностойно по същество ниво на защита. Това наблюдение е особено важно в този случай, тъй като Обединеното кралство ще администрира, прилага и привежда в изпълнение нов режим за защита на данните, спрямо който вече не се прилага правото на Съюза и който може да претърпи промени. В това отношение ще се обърне специално внимание на практическото прилагане на правилата на Обединеното кралство относно предаването на лични данни на трети държави, включително чрез сключването на международни споразумения, и на въздействието, което това може да окаже върху нивото на защита на данните, предавани съгласно настоящото решение, както и на ефективността на упражняването на индивидуалните права в областите, обхванати от настоящото решение. Наред с други елементи, развитието на съдебната практика и надзорът от страна на ICO и други независими органи ще бъдат използвани за мониторинга от страна на Комисията.

(166) За да се улесни този мониторинг, органите на Обединеното кралство следва своевременно и редовно да информират Комисията за всяка съществена промяна в правния ред на Обединеното кралство, която има отражение върху правната уредба, предмет на настоящото решение, както и за всяко развитие на практиките, свързани с обработването на личните данни, оценени в настоящото решение, и по-специално за елементите, посочени в съображение 165.

(167) На следващо място, за да се даде възможност на Комисията да изпълнява ефективно функцията си по извършване на наблюдение, държавите членки следва да я информират за всички релевантни действия, предприети от националните органи по защита на данните, по-специално във връзка със запитвания или жалби на субекти на данни от ЕС във връзка с предаване на лични данни от Съюза към компетентни органи на Обединеното кралство. Комисията следва да бъде информирана и за всеки признак, че действията на публичните органи на Обединеното кралство, отговарящи за предотвратяването, разследването, разкриването или наказателното преследване на престъпления, включително тези на надзорните органи, не гарантират изискваното ниво на защита.

(168) Когато наличната информация, по-специално информацията, получена в резултат на наблюдението на настоящото решение или предоставена от органите на Обединеното кралство или на държавите членки, показва, че нивото на защита, предлагано от Обединеното кралство, може вече да не е адекватно, Комисията следва незабавно да информира компетентните органи на Обединеното кралство за това и да поиска предприемането на подходящи мерки в определен срок, който не може да надвишава три месеца. При необходимост този срок може да бъде удължен за определен период от време, като се вземе предвид естеството на разглеждания въпрос и/или мерките, които трябва да бъдат предприети.

(169) Ако при изтичането на посочения срок компетентните органи на Обединеното кралство не предприемат тези мерки или не докажат по друг задоволителен начин, че настоящото решение продължава да се основава на адекватно ниво на защита, Комисията ще започне процедурата, посочена в член 58, параграф 2 от Директива (ЕС) 2016/680, с оглед частично или пълно спиране на действието или отмяна на настоящото решение.

(170) Като алтернативна възможност Комисията ще започне тази процедура с оглед изменение на Решението, по-специално като обвърже предаването на данни с допълнителни условия или като ограничи обхвата на констатацията за адекватност само до предаването на данни, за което продължава да се осигурява адекватно ниво на защита.

(171) При надлежно обосновани наложителни причини за спешност Комисията ще използва възможността да приеме, в съответствие с процедурата, посочена в член 58, параграф 3 от Директива (ЕС) 2016/680, актове за изпълнение с незабавно приложение за спиране на действието, отмяна или изменение на решението.

6. СРОК НА ДЕЙСТВИЕ И ПОДНОВЯВАНЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(172) Следва да се вземе предвид, че в края на преходния период, предвиден в Споразумението за оттегляне, и веднага след като временната разпоредба по член 782 от Споразумението за търговия и сътрудничество между ЕС и Обединеното кралство престане да се прилага, Обединеното кралство ще администрира, прилага и привежда в изпълнение нов режим за защита на данните в сравнение с този, който е бил в сила, когато е било обвързано от правото на Европейския съюз. Това може по-специално да включва изменения или промени в уредбата за защита на данните, оценена в настоящото решение, както и други релевантни развития.

(173) Поради това е целесъобразно да се предвиди настоящото решение да се прилага за период от четири години, считано от влизането му в сила.

(174) Когато по-специално информацията, получена в резултат на наблюдението на настоящото решение, покаже, че констатациите относно адекватността на нивото на защита, осигурявано в Обединеното кралство, все още са фактически и правно обосновани, Комисията следва, най-късно шест месеца преди настоящото решение да престане да се прилага, да започне процедурата за изменение на настоящото решение чрез удължаване на неговия времеви обхват, по принцип, за допълнителен период от четири години. Всеки подобен акт за изпълнение, изменящ настоящото решение, трябва да бъде приет в съответствие с процедурата, посочена в член 58, параграф 2 от Директива (ЕС) 2016/680.

7. **ЗАКЛЮЧИТЕЛНИ СЪОБРАЖЕНИЯ**

(175) Европейският комитет по защита на данните публикува становището си ([271]), като то бе взето предвид при изготвянето на настоящото решение.

(176) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден по силата на член 58 от Директива (ЕС) 2016/680.

(177) В съответствие с член 6а от Протокол № 21 относно позицията на Обединеното кралство и Ирландия по отношение на пространството на свобода, сигурност и правосъдие, приложен към ДЕС и към ДФЕС, Ирландия не е обвързана от заложените в Директива (ЕС) 2016/680 правила и съответно от настоящото решение за изпълнение относно обработването на лични данни от държавите членки при осъществяване на дейности, попадащи в обхвата на трета част, дял V, глава 4 или глава 5 от ДФЕС, когато Ирландия не е обвързана от правилата, уреждащи формите на съдебно сътрудничество по наказателноправни въпроси или на полицейско сътрудничество, в рамките на които трябва да бъдат съблюдавани разпоредбите, установени въз основа на член 16 от ДФЕС. Освен това по силата на Решение за изпълнение (ЕС) 2020/1745 на Съвета ([272]) Директива (ЕС) 2016/680 трябва да бъде приведена в действие и да се прилага временно в Ирландия, считано от 1 януари 2021 г. Следователно Ирландия е обвързана от настоящото решение за изпълнение при същите условия, които се прилагат за прилагането на Директива (ЕС) 2016/680 в Ирландия, посочени в Решение за изпълнение (ЕС) 2020/1745 по отношение на достиженията на правото от Шенген, в които участва.

(178) В съответствие с членове 2 и 2а от Протокол № 22 относно позицията на Дания, приложен към Договора за Европейския съюз и към Договора за функционирането на Европейския съюз, Дания не е обвързана от правилата, установени в Директива (ЕС) 2016/680 и следователно от настоящото решение за изпълнение, нито от тяхното прилагане, свързано с обработването на лични данни от държавите членки при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС. Като се има предвид обаче, че Директива (ЕС) 2016/680 се основава на достиженията на правото от Шенген, в съответствие с член 4 от посочения протокол на 26 октомври 2016 г. Дания уведоми за решението си да прилага Директива (ЕС) 2016/680. Следователно по силата на международното право Дания е длъжна да прилага настоящото решение за изпълнение.

(179) По отношение на Исландия и Норвегия настоящото решение за изпълнение представлява развитие на разпоредбите на достиженията на правото от Шенген по смисъла на Споразумението, сключено от Съвета на Европейския съюз и Република Исландия и Кралство Норвегия за асоциирането на последните в процеса на изпълнение, прилагане и развитие на достиженията на правото от Шенген ([273]).

(180) По отношение на Швейцария настоящото решение за изпълнение представлява развитие на разпоредбите на достиженията на правото от Шенген по смисъла на Споразумението между Европейския съюз, Европейската общност и Конфедерация Швейцария относно асоциирането на Конфедерация Швейцария към изпълнението, прилагането и развитието на достиженията на правото от Шенген ([274]).

(181) По отношение на Лихтенщайн настоящото решение за изпълнение представлява развитие на разпоредбите на достиженията на правото от Шенген по смисъла на Протокола между Европейския съюз, Европейската общност, Конфедерация Швейцария и Княжество Лихтенщайн относно присъединяването на Княжество Лихтенщайн към Споразумението между Европейския съюз, Европейската общност и Конфедерация Швейцария относно асоциирането на Конфедерация Швейцария към изпълнението, прилагането и развитието на достиженията на правото от Шенген ([275]).

([271]) Становище 15/2021 относно проекта на решение за изпълнение на Европейската комисия съгласно Директива (ЕС) 2016/680 относно адекватната защита на личните данни в Обединеното кралство, достъпно на следния адрес: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_en

([272]) Решение за изпълнение (ЕС) 2020/1745 на Съвета от 18 ноември 2020 г. относно привеждането в действие на разпоредбите на достиженията на правото от Шенген в областта на защитата на личните данни и относно временното привеждане в действие на някои разпоредби на достиженията на правото от Шенген в Ирландия (ОВ L 393, 23.11.2020 г., стр. 3).

([273]) ОВ L 176, 10.7.1999 г., стр. 36.

([274]) ОВ L 53, 27.2.2008 г., стр. 52.

([275]) ОВ L 160, 18.6.2011 г., стр. 21.

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

За целите на член 36 от Директива (ЕС) 2016/680 Обединеното кралство осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз на публичните органи на Обединеното кралство, отговарящи за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания.

Член 2

Когато с цел защита на физическите лица във връзка с обработване на техни лични данни компетентните надзорни органи в държавите членки упражняват правомощията си по член 47 от Директива (ЕС) 2016/680 по отношение на предаването на данни на публични органи в Обединеното кралство в рамките на приложното поле, посочено в член 1, съответната държава членка незабавно уведомява Комисията.

Член 3

1. Комисията непрекъснато наблюдава прилагането на правната уредба, на която се основава настоящото решение, включително условията, при които се извършват последващите предавания и се упражняват индивидуалните права, с цел да прецени дали Обединеното кралство продължава да осигурява адекватно ниво на защита по смисъла на член 1.

2. Държавите членки и Комисията се информират взаимно за случаите, в които комисарят по информацията или всеки друг компетентен орган на Обединеното кралство не е гарантирал спазването на правната уредба, на която се основава настоящото решение.

3. Държавите членки и Комисията се информират взаимно за всеки признак, че намесата на публичните органи на Обединеното кралство в правото на физическите лица на защита на личните им данни надвишава строго необходимото или че няма ефективна правна защита срещу подобна намеса.

4. Когато Комисията разполага с данни, че вече не се осигурява адекватно ниво на защита, тя информира компетентните органи на Обединеното кралство и може да спре действието, да отмени или да измени настоящото решение.

5. Комисията може да спре действието, да отмени или да измени настоящото решение, ако липсата на съдействие от страна на правителството на Обединеното кралство не позволява Комисията да определи дали е засегната констатацията в член 1.

Член 4

Срокът на действие на настоящото решение изтича на 27 юни 2025 г., освен ако срокът му на действие не бъде удължен в съответствие с процедурата, посочена в член 58, параграф 2 от Директива (ЕС) 2016/680.

Член 5

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 28 юни 2021 година.

За Комисията
Didier REYNDERS
Член на Комисията