II

(Незаконодателни актове)

РЕШЕНИЯ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2021/1772 НА КОМИСИЯТА

от 28 юни 2021 година

съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство

(нотифицирано под номер C(2021) 4800)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид 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) ([1]), и по-специално член 45, параграф 3 от него,

като има предвид, че:

1. ВЪВЕДЕНИЕ

(1) С Регламент (ЕС) 2016/679 се определят правилата за предаването на лични данни от администратори или обработващи лични данни в Европейския съюз на трети държави и международни организации, доколкото това предаване попада в неговото приложно поле. Правилата относно международното предаване на данни са установени в глава V от посочения регламент, по-специално в членове 44—50. Въпреки че движението на лични данни към и от държави извън Европейския съюз е от съществено значение за разширяването на международното сътрудничество и презграничната търговия, нивото на защита, което се предоставя на личните данни в Европейския съюз, не трябва да се излага на риск при предаване на трети държави ([2]).

(2) Съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 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, както е предвидено в член 45, параграф 1 и в съображение 103 от посочения регламент.

(3) Както е посочено в член 45, параграф 2 от Регламент (ЕС) 2016/679, приемането на решение относно адекватността трябва да се основава на цялостен анализ на правния ред на третата държава, който обхваща както правилата, приложими към вносителите на данни, така и ограниченията и гаранциите по отношение на достъпа до лични данни от страна на публичните органи. 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 104 от Регламент (ЕС) 2016/679). Стандартът, спрямо който се оценява „равностойността по същество“, е определеният от законодателството на ЕС, по-специално от Регламент (ЕС) 2016/679, както и от съдебната практика на Съда на Европейския съюз ([3]). Референтният документ на Европейския комитет по защита на данните (ЕКЗД) за адекватното ниво на защита също е от значение в това отношение ([4]).

([1]) ОВ L 119, 4.5.2016 г., стр. 1.

([2]) Вж. съображение 101 от Регламент (ЕС) 2016/679.

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

([4]) Референтният документ на Европейския комитет по защита на данните за адекватното ниво на защита WP 254 rev. 01. е достъпен на следния адрес: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(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 защита на личния живот и неговото ефективно прилагане, надзор и изпълнение чуждестранната система като цяло осигурява необходимото ниво на защита ([7]).

(5) Комисията анализира внимателно законодателство и практиката на Обединеното кралство. Въз основа на своите констатации, изложени в съображения 8—270, Комисията стига до заключението, че Обединеното кралство осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз към Обединеното кралство в рамките на приложното поле на Регламент (ЕС) 2016/679.

(6) Това заключение не се отнася до личните данни, предавани за целите на имиграционния контрол на Обединеното кралство, или до данните, които по друг начин попадат в обхвата на изключението по отношение на определени права на субекта на данни за целите на поддържането на ефективен имиграционен контрол („изключението във връзка с имиграционния контрол“) съгласно точка 4, подточка 1 от приложение 2 към Закона за защита на данните на Обединеното кралство. Валидността и тълкуването на изключението във връзка с имиграционния контрол съгласно правото на Обединеното кралство не са уредени вследствие на решение на Апелативния съд на Англия и Уелс от 26 май 2021 г. Макар да признава, че правата на субектите на данни принципно могат да бъдат ограничавани за целите на имиграционния контрол като „важен аспект на обществения интерес“, Апелативният съд установи, че в настоящата си форма изключението във връзка с имиграционния контрол е несъвместимо с правото на Обединеното кралство, тъй като за тази законодателна мярка липсват конкретни разпоредби, определящи гаранциите, изброени в член 23, параграф 2 от Общия регламент относно защитата на данните на Обединеното кралство (ОРЗД на Обединеното кралство) ([8]). При тези условия предаването на лични данни от Съюза към Обединеното кралство, за което може да се приложи изключението във връзка с имиграционния контрол, следва да бъде изключено от обхвата на настоящото решение ([9]). След като несъвместимостта с правото на Обединеното кралство бъде отстранена, изключението във връзка с имиграционния контрол следва да бъде преразгледано, както и необходимостта да се запази ограничението на обхвата на настоящото решение.

(7) Настоящото решение не следва да засяга прякото приложение на Регламент (ЕС) 2016/679 спрямо организации, установени в Обединеното кралство, когато условията относно териториалното приложение на посочения регламент, изложени в член 3 от него, са изпълнени.

2. ПРАВИЛА, ПРИЛОЖИМИ КЪМ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

2.1. Конституционна уредба

(8) Обединеното кралство е парламентарна демокрация с държавен глава конституционен суверен. 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, които отговарят за контрола върху правителството и за обсъждането и приемането на закони.

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

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

([7]) Вж. 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.

([8]) Апелативен съд (Гражданско отделение), *Open Rights Group/Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport*, [2021] EWCA Civ 800, точки 53—56. Апелативният съд отмени решението на Висшия съд (*High Court of Justice*), с което по-рано бе направена оценка на изключението с оглед на Регламент (ЕС) 2016/679 (по-специално член 23 от него) и Хартата на основните права на Европейския съюз и беше установено, че изключението е законосъобразно (*Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

([9]) Ако бъдат изпълнени приложимите условия, предаването за целите на имиграционния контрол на Обединеното кралство може да се извършва въз основа на механизмите за предаване, предвидени в членове 46—49 от Регламент (ЕС) 2016/679.

(9) Парламентът на Обединеното кралство е делегирал законодателни правомощия на парламента на Шотландия, парламента на Уелс (*Senedd Cymru*) и Събранието на Северна Ирландия по вътрешни въпроси в Шотландия, Уелс и Северна Ирландия, които Обединеното кралство не е резервирало за себе си. Макар защитата на данните да е въпрос, резервиран за компетентността 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 наказателноправните системи на Шотландия и Северна Ирландия, включително полицейската дейност, са делегирани съответно на парламента на Шотландия и на Събранието на Северна Ирландия. Обединеното кралство не разполага с кодифицирана конституция в смисъла на утвърден учредителен документ. Конституционните принципи са се оформили с течение на времето и произтичат по-специално от съдебната практика и правните обичаи. 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 от съдилищата. 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, 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]).

(10) Със Закона за правата на човека от 1998 г. правата, съдържащи се в ЕКПЧ, се въвеждат в правото на Обединеното кралство. По силата на Закона за правата на човека на всяко физическо лице се предоставят основните права и свободи, предвидени в членове 2—12 и в член 14 от Европейската конвенция за правата на човека, както и в членове 1, 2 и 3 от Първия протокол към нея и в член 1 от Тринадесетия протокол към нея, във връзка с членове 16, 17 и 18 от посочената конвенция. Това включва правото на зачитане на личния и семейния живот (и правото на защита на личните данни като част от него) 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.

(11) 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]).

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

(12) На 31 януари 2020 г. Обединеното кралство се оттегли от Европейския съюз. 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 се състоеше от съответното законодателство на ЕС (по-специално Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета ([15])) и национално законодателство, по-специално Закона за защита на данните от 2018 г. (ЗЗД от 2018 г.) ([16]), с който са установени национални норми в областите, в които това е допустимо съгласно Регламент (ЕС) 2016/679, уточнено е и е ограничено прилагането на нормите на Регламент (ЕС) 2016/679 и е транспонирана Директива (ЕС) 2016/680.

([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 е подписало Протокола за изменение на Конвенцията за защита на лицата при автоматизираната обработване на лични данни (известна като „Конвенция 108+“) през 2018 г. и понастоящем работи по ратифицирането ѝ.

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

([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), достъпно на следния адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=BG

([15]) 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 (ОВ L 119, 4.5.2016 г., стр. 89), достъпна на следния адрес: https://eur-lex.europa.eu/legal-content/bg/TXT/PDF/?uri=CELEX:32016L0680 .

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

(13) С цел подготвяне за оттеглянето от Европейския съюз правителството на Обединеното кралство прие Закона от 2018 г. за оттеглянето от Европейския съюз ([17]), с който пряко приложимите законодателни актове на Съюза бяха включени в правото на Обединеното кралство ([18]). Това така наречено „запазено право на ЕС“ включва Регламент (ЕС) 2016/679 в неговата цялост (заедно със съображенията към него) ([19]). По силата на горепосочения закон „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 и общите принципи на правото на Съюза във вида, в който 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“) ([20]).

(14) Съгласно Закона за оттеглянето от Европейския съюз от 2018 г. 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. Те упражниха това правомощие с приемането на Наредбите от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС) ([21]). С тях се изменя Регламент (ЕС) 2016/679, както той е въведен в правото на Обединеното кралство посредством Закона от 2018 г. за оттеглянето от Европейския съюз, ЗЗД от 2018 г. и други законодателни актове в областта на защитата на данните, с цел привеждане в съответствие с националния контекст ([22]).

(15) Вследствие на това правната уредба за защита на личните данни в Обединеното кралство след края на преходния период се състои от:

— ОРЗД на Обединеното кралство, включен в правото на Обединеното кралство съгласно Закона от 2018 г. за оттеглянето от Европейския съюз и изменен с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС) ([23]), и

— ЗЗД от 2018 г. ([24]), изменен с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС).

(16) Тъй като ОРЗД на Обединеното кралство се основава на законодателството на ЕС, правилата за защита на личните данни в Обединеното кралство в много отношения следват тясно съответните правила, приложими в Европейския съюз.

(17) Наред с правомощията, предоставени на министъра съгласно Закона от 2018 г. за оттеглянето от Европейския съюз, няколко разпоредби на ЗЗД от 2018 г. дават правомощия на министъра да приема вторично законодателство за изменение на определени разпоредби на закона или да определя допълващи и допълнителни правила ([25]). Досега

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

([18]) Замисълът и правното действие на Закона от 2018 г. за оттеглянето от Европейския съюз е, че всички преки законодателни актове на Съюза, които са били включени в правото на Обединеното кралство в края на преходния период, са част от правото на Обединеното кралство така, както са били в сила непосредствено преди края на преходния период, вж. член 3 от Закона от 2018 г. за оттеглянето от Европейския съюз.

([19]) В Обяснителните бележки към Закона от 2018 г. за оттеглянето от Европейския съюз се уточнява, че: „когато законодателството се преобразува съгласно този член, самият текст на законодателния акт ще представлява част от вътрешното законодателство. Това ще включва пълния текст на законодателния акт на ЕС (заедно със съображенията към него)“. (Обяснителни бележки към Закона от 2018 г. за оттеглянето от Европейския съюз, точка 83, достъпни на следния адрес: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). Според информацията, предоставена от органите на Обединеното кралство, тъй като съображенията нямат статут на обвързващи правни норми, не е било необходимо те да бъдат изменяни по начина, по който членовете на Регламент (ЕС) 2016/679 са изменени с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения.

([20]) Член 6 от Закона от 2018 г. за оттеглянето от Европейския съюз.

([21]) 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.

([22]) Тези изменения на ОРЗД и на ЗЗД от 2018 г. на Обединеното кралство имат предимно технически характер, като например заличаване на препратки към „пържави членки“ или адаптиране на терминологията, напр. замяна на позоваванията на Регламент (ЕС) 2016/679 с позовавания на ОРЗД на Обединеното кралство. В някои случаи са били необходими промени, за да се отрази чисто националният контекст на разпоредбите, например по отношение на това „кой“ приема „наредби относно адекватното ниво на защита“ за целите на правната уредба на Обединеното кралство за защита на данните (вж. член 17A от ЗЗД от 2018 г.), т.е. министърът, а не Европейската комисия.

([23]) Общ регламент относно защитата на данните с отразени направените в него промени, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([24]) Закон за защита на данните от 2018 г., с отразени направените в него промени, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf.

([25]) Такива правомощия се съдържат например в член 16 (правомощие да се правят допълнителни изключения от специфични разпоредби на ОРЗД на Обединеното кралство в конкретни, тясно определени случаи), в член 17A (правомощие да се приемат наредби относно адекватното ниво на защита), в членове 212 и 213 (правомощие да се предприема законодателна инициатива и да се въвеждат преходни разпоредби) и в член 211 (правомощие да се извършват незначителни и последващи изменения) от ЗЗД от 2018 г.

министърът е упражнил само правомощието по член 137 от ЗЗД от 2018 г. с цел приемането на Наредбите за защита на данните (Такси и информация) (изменения) от 2019 г., в които се определят обстоятелствата, при които администраторите на данни трябва да плащат годишна такса на независимия орган на Обединеното кралство за защита на данните — комисаря по информацията.

(18) И накрая, допълнителни насоки относно законодателството на Обединеното кралство за защита на данните са предвидени в кодексите за поведение и в други насоки, приети от комисаря по информацията. Въпреки че официално насоките не са правнообвързващи, те имат тълкувателна тежест и показват как законодателството за защита на данните се прилага и привежда в изпълнение на практика от комисаря. По-специално съгласно членове 121—125 от ЗЗД от 2018 г. комисарят трябва да изготви кодекси за поведение относно споделянето на данни, директния маркетинг, съобразените с възрастта дизайн и защита на данните и журналистиката.

(19) Следователно по своята структура и основни компоненти правната уредба на Обединеното кралство, която се прилага по отношение на данните, предавани съгласно настоящото решение, 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**

(20) Както Регламент (ЕС) 2016/679, така и ОРЗД на Обединеното кралство се прилагат за обработването на лични данни изцяло или частично с автоматични средства или за обработването с други средства, ако личните данни са част от регистър с лични данни ([26]). Определенията на понятията „лични данни“, „субект на данни“ и „обработване“ в ОРЗД на Обединеното кралство са идентични с тези в Регламент (ЕС) 2016/679 ([27]). Освен това ОРЗД на Обединеното кралство се прилага за ръчното неструктурирано обработване на лични данни ([28]), съхранявани от определени публични органи на Обединеното кралство ([29]), въпреки че принципите и правата, залегнали в ОРЗД на Обединеното кралство, които нямат отношение към такива лични данни, са отменени с членове 24 и 25 от ЗЗД от 2018 г. Подобно на Регламент (ЕС) 2016/679, ОРЗД на Обединеното кралство не се прилага за обработването на лични данни от физическо лице в хода на чисто лични или домашни занимания ([30]).

(21) Приложното поле на ОРЗД на Обединеното кралство се простира и върху обработването на лични данни в хода на дейност, която непосредствено преди края на преходния период е попадала извън приложното поле на правото на Европейския съюз (напр. националната сигурност) ([31]) или е била в приложното поле на дял 5, глава 2 от Договора за Европейския съюз (дейности по общата външна политика и политика на сигурност) ([32]). Както е в системата на

([26]) Член 2, параграфи 1 и 5 от ОРЗД на Обединеното кралство.

([27]) Член 4, параграфи 1 и 2 от ОРЗД на Обединеното кралство.

([28]) Ръчното неструктурирано обработване на лични данни е определено в член 2, параграф 5, буква б) като обработване на лични данни, което не е автоматизирано или структурирано.

([29]) В член 2, параграф 1A от ОРЗД на Обединеното кралство е предвидено, че регламентът се прилага и за ръчното неструктурирано обработване на лични данни, съхранявани от публичен орган, отговарящ за свободата на информацията. Публични органи, отговарящи за свободата на информацията, са всички публични органи, определени в Закона за свобода на информацията от 2000 г. или всички шотландски публични органи, определени в Закона за свобода на информацията (Шотландия) от 2002 г. (Акт на парламента на Шотландия № 13). Член 21, параграф 5 от ЗЗД от 2018 г.

([30]) Член 2, параграф 2, буква а) от ОРЗД на Обединеното кралство.

([31]) Дейностите, свързани с националната сигурност, попадат в приложното поле на ОРЗД на Обединеното кралство, ако не се извършват от компетентен орган за целите на правоприлагането, в какъвто случай се прилага част 3 от ЗЗД от 2018 г., или от или от името на разузнавателна служба, чиито дейности са изключени от обхвата на ОРЗД на Обединеното кралство и са предмет на част 4 от ЗЗД от 2018 г. съгласно член 2, параграф 2, буква в) от ОРЗД на Обединеното кралство. Например полицейски орган може да извършва проверки за сигурност на служител с цел да се гарантира, че може да му се има доверие за достъп до материали, свързани с националната сигурност. Въпреки че полицията е компетентен орган за целите на правоприлагането, въпросното обработване на данни не е с цел правоприлагане и ОЗРД на Обединеното кралство би бил приложим. Вж. Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална рамка за защита на данните и правомощията за разследване, стр. 8, достъпна на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

([32]) Член 2, параграф 1, букви а) и б) от ОРЗД на Обединеното кралство.

Европейския съюз, ОРЗД на Обединеното кралство не се прилага за обработването на лични данни от компетентен орган 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 (така наречените „цели на правоприлагането“) — този вид обработване е уредено в част 3 от ЗЗД от 2018 г. и съответно в Директива (ЕС) 2016/680 съгласно правото на Европейския съюз — нито за обработването на лични данни от разузнавателните служби (Службата за сигурност, Службата за тайно разузнаване и Правителствената централа за комуникации), което е обхванато в част 4 от ЗЗД от 2018 г. ([33]).

(22) Териториалният обхват на ОРЗД на Обединеното кралство е описан в член 3 от ОРЗД на Обединеното кралство ([34]) и включва обработването на лични данни (независимо къде се извършва) в контекста на дейностите на дадено място на установяване на администратор или обработващ лични данни в Обединеното кралство, както и обработването на лични данни на субекти на данни, които се намират в Обединеното кралство, когато дейностите по обработване на данни са свързани с предлагането на стоки или услуги на такива субекти на данни или наблюдението на тяхното поведение ([35]). Това отразява подхода, възприет в член 3 от Регламент (ЕС) 2016/679.

2.4. **Определения за „лични данни“ и за понятията „администратор“ и „обработващ лични данни“**

(23) Определенията за „лични данни“, „обработване“, „администратор“, „обработващ лични данни“, както и определението за „псевдонимизация“, залегнали в Регламент (ЕС) 2016/679, са запазени без съществени изменения в ОРЗД на Обединеното кралство ([36]). Освен това специалните категории лични данни са определени в член 9, параграф 1 от ОРЗД на Обединеното кралство по същия начин, както и в Регламент (ЕС) 2016/679 („разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице“). В член 205 от ЗЗД от 2018 г. се съдържат определенията за „биометрични данни“ ([37]), „данни за здравословното състояние“ ([38]) и „генетични данни“ ([39]).

2.5. **Гаранции, права и задължения**

2.5.1. *Законосъобразност и добросъвестност на обработването*

(24) Личните данни следва да се обработват законосъобразно и добросъвестно.

(25) Принципите на законосъобразност, добросъвестност и прозрачност и основанията за законосъобразно обработване на лични данни са гарантирани в правото на Обединеното кралство чрез разпоредбите на член 5, параграф 1, буква а) и член 6, параграф 1 от ОРЗД на Обединеното кралство, които са идентични със съответните разпоредби на Регламент (ЕС) 2016/679 ([40]). Член 8 от ЗЗД от 2018 г. допълва член 6, параграф 1, буква д), като в него се предвижда, че обработването на лични данни съгласно член 6, параграф 1, буква д) от ОРЗД на Обединеното кралство (необходимо за изпълнението на задача, извършвана в обществен интерес, или при упражняването на

([33]) Член 2, параграф 2, букви б) и в) от ОРЗД на Обединеното кралство.

([34]) Същият териториален обхват се прилага и за обработването на лични данни съгласно част 2 от ЗЗД от 2018 г., която допълва ОРЗД на Обединеното кралство (член 207, параграф 1А).

([35]) Това по-специално означава, че ЗЗД от 2018 г., а следователно и настоящото решение не се прилагат за териториите, зависими от Британската корона (Джърси, Гърнзи и остров Ман), и за отвъдморските територии на Обединеното кралство, като например Фолкландските острови и територията на Гибралтар.

([36]) Член 4, параграфи 1, 2, 5, 7 и 8 от ОРЗД на Обединеното кралство.

([37]) „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.

([38]) „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.

([39]) „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.

([40]) Съгласно член 6, параграф 1 от ОРЗД на Обединеното кралство обработването е законосъобразно само ако и доколкото: а) субектът на данни е дал съгласие за обработване на личните му данни за една или повече конкретни цели; б) обработването е необходимо за изпълнението на договор, по който субектът на данни е страна, или за предприемане на стъпки по искане на субекта на данни преди сключването на договор; в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора; г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данни или на друго физическо лице; д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора; или е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данни, които изискват защита на личните данни, по-специално когато субектът на данни е дете.

официалните правомощия на администратора), включва обработването на лични данни, необходимо за правораздаването, за упражняването на функция на някоя от двете камари на Парламента, за упражняването на функция, възложена на лице с акт или правна норма, за упражняването на функция на Короната, на министър на Короната или на правителствен отдел, или на дейност, с която се подкрепя или насърчава демократичната ангажираност.

(26) По отношение на съгласието (едно от основанията за законосъобразно обработване), в ОРЗД на Обединеното кралство са запазени непроменени и условията, предвидени в член 7 от Регламент (ЕС) 2016/679, тоест администраторът трябва да е в състояние да докаже, че субектът на данни е дал съгласие, трябва да бъде представено писмено искане за съгласие, като се използва ясен и прост език, субектът на данни трябва да има правото да оттегли съгласието си по всяко време и, когато се прави оценка дали съгласието е било свободно изразено, следва да се отчита дали изпълнението на даден договор е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор. Освен това, съгласно член 8 от ОРЗД на Обединеното кралство, в контекста на предоставянето на услуги на информационното общество съгласието на дете е законосъобразно само когато детето е поне на 13 години. Тази възраст попада във възрастовите граници, определени в член 8 от Регламент (ЕС) 2016/679.

2.5.2. *Обработване на специални категории лични данни*

(27) Когато се обработват „специални категории данни“, следва да има специфични гаранции.

(28) В ОРЗД на Обединеното кралство и в ЗЗД от 2018 г. се съдържат специфични правила за обработването на специални категории лични данни, които са определени в член 9, параграф 1 от ОРЗД на Обединеното кралство по същия начин, както и в Регламент (ЕС) 2016/679 (вж. съображение 23 по-горе). В съответствие с член 9 от ОРЗД обработването на специални категории лични данни по принцип е забранено, освен ако се прилага конкретно изключение.

(29) В изключенията (изброени в член 9, параграфи 2 и 3 от ОРЗД на Обединеното кралство) не са въведени промени по същество в сравнение с тези, посочени в член 9, параграфи 2 и 3 от Регламент (ЕС) 2016/679. Освен ако субектът на данни е дал изричното си съгласие за обработването на този вид лични данни, обработването на специални категории лични данни е разрешено само при специфични и ограничени обстоятелства. В повечето случаи обработването на чувствителни данни трябва да е необходимо за конкретна цел, определена в съответната разпоредба (вж. член 9, параграф 2, букви б), в), е), ж), з), и) и й).

(30) Освен това, когато за изключение съгласно член 9, параграф 2 от ОРЗД на Обединеното кралство се изисква разрешение по закон или изключението е свързано с обществения интерес, в член 10 от ЗЗД от 2018 г. и в приложение 1 към него допълнително са уточнени условията, които трябва да бъдат изпълнени за прилагането на тези изключения. Например при обработване на чувствителни данни с цел защита на „общественото здраве“ (член 9, параграф 2, буква и) от ОРЗД на Обединеното кралство), съгласно част 1, точка 3, буква б) от приложение 1, освен проверката за необходимост, се изисква обработването да се извършва „от или под ръководството на медицински специалист“ или „от друго лице, което е обвързано от задължение за поверителност съгласно нормативен акт или правна норма“, включително по силата на утвърденото задължение за поверителност съгласно общото право.

(31) Когато чувствителните данни се обработват по съображения от важен обществен интерес (член 9, параграф 2, буква g) от ОРЗД на Обединеното кралство), в част 2 от приложение 1 към ЗЗД от 2018 г. е предвиден изчерпателен списък от цели, които могат да се считат за цели от важен обществен интерес, и за всяка от тях са определени конкретни допълнителни условия. Например насърчаването на расово и етническо многообразие на висшите равнища в организациите се признава за цел от важен обществен интерес. Обработването на чувствителни данни за тази конкретна цел е предмет на подробни изисквания, които включват то да се извършва в рамките на процедура за определяне на подходящи лица, които да заемат ръководни длъжности, да е необходимо за насърчаване на расовото и етническото многообразие и да е малко вероятно да причини значителна вреда или значителни сътресения на субекта на данни.

(32) В член 11, параграф 1 от ЗЗД от 2018 г. са определени условията за обработване на лични данни при обстоятелствата, описани в член 9, параграф 3 от ОРЗД на Обединеното кралство, свързани със задължението за опазване на професионалната тайна. Това включва обстоятелства, при които обработването се извършва от или под ръководството на медицински специалист или от социален работник, или от друго лице, което при тези обстоятелства е обвързано от задължение за поверителност съгласно нормативен акт или правна норма.

(33) Освен това, за да бъдат приложени много от изключенията, изброени в член 9, параграф 2 от ОРЗД на Обединеното кралство, са необходими подходящи и специфични гаранции. В зависимост от естеството на обработването и равнището на риск за правата и свободите на субектите на данни, в условията за обработване, предвидени в приложение 1 към ЗЗД от 2018 г., са установени различни гаранции. В приложение 1 съответно са определени условията за всеки случай на обработване на данни.

(34) В някои случаи в ЗЗД от 2018 г. видът чувствителни данни, които могат да бъдат обработвани, за да бъде спазено определено правно основание, е регламентиран и ограничен. Например обработването на чувствителни данни с цел насърчаване на равенство на възможностите или еднакво третиране е разрешено съгласно точка 8 от приложение 1. Това условие за обработване на лични данни може да се използва само ако данните разкриват расов или етнически произход, религиозни или философски убеждения, сексуална ориентация, или ако става дума за данни за здравословното състояние.

(35) В някои случаи ЗЗД от 2018 г. ограничава вида администратор на лични данни, който може да използва дадено условие за обработване. Например обработването на чувствителни данни във връзка с отговорите на лица на изборни длъжности пред обществеността е уредено в точка 23 от приложение 1. Това условие за обработване може да се използва само ако администраторът е лицето на изборна длъжност или действа под негово ръководство.

(36) В някои други случаи в ЗЗД от 2018 г. са въведени ограничения относно категориите субекти на данни, за които може да се използва дадено условие за обработване. Например обработването на чувствителни данни, свързани с професионални пенсионни схеми, е уредено в точка 21 от приложение 1. Това условие може да се използва само ако въпросният субект на данни е брат или сестра, родител, баба или дядо на член на пенсионната схема.

(37) Освен това при прилагането на изключения съгласно член 9, параграф 2 от ОРЗД на Обединеното кралство, които са допълнително уточнени в член 10 от ЗЗД от 2018 г. и в приложение 1 към него, в повечето случаи се изисква администраторът на данните да изготви „подходящ документ за политиката“. В него трябва да бъдат описани процедурите на администратора за осигуряване на спазването на принципите, предвидени в член 5 от ОРЗД на Обединеното кралство. В него трябва също така да бъдат определени политиките относно съхраняването и заличаването на данни и да бъде указан вероятният период на съхранение. Администраторите трябва да преразглеждат и актуализират този документ, когато е необходимо. Администраторът трябва да съхранява документа за политиката за срок от шест месеца след приключване на обработването и да го предоставя на комисаря по информацията при поискване ([41]).

(38) Съгласно точка 41 от приложение 1 към ЗЗД от 2018 г. документът за политиката трябва винаги да се придружава от разширен регистър на дейностите по обработване. Този регистър трябва да позволява да се проследят ангажиментите, включени в документа за политиката, т.е. дали данните се заличават или съхраняват в съответствие с политиките. Ако политиките не са били спазени, в регистъра трябва да бъдат вписани причините за това. В него трябва също така да бъдат описани основанията, поради които обработването отговаря на член 6 от ОРЗД на Обединеното кралство (законосъобразност на обработването), и конкретното условие съгласно приложение 1 към ЗЗД от 2018 г., което е било приложено.

(39) И накрая, както в Регламент (ЕС) 2016/679, така и в ОРЗД на Обединеното кралство са предвидени общи гаранции за определени операции по обработването на специални категории данни. Съгласно член 35 от ОРЗД на Обединеното кралство се изисква оценка на въздействието върху защитата на данните, ако специални категории данни се обработват в голям мащаб. В съответствие с член 37 от ОРЗД на Обединеното кралство администраторът или обработващият лични данни трябва да определи длъжностно лице по защита на данните, когато основните му дейности се състоят в обработване на специални категории данни в голям мащаб.

(40) По отношение на личните данни, свързани с присъди и нарушения, член 10 от ОРЗД на Обединеното кралство е идентичен с член 10 от Регламент (ЕС) 2016/679. Обработване на лични данни, свързани с присъди и нарушения, се допуска само под контрола на официален орган или когато обработването е разрешено от националното право, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни.

(41) Когато обработването на лични данни, свързани с присъди и нарушения, не се извършва под контрола на официален орган, в член 10, параграф 5 от ЗЗД от 2018 г. е предвидено, че то може да се осъществява само за специфичните цели и в конкретните случаи, определени в части 1, 2 и 3 от приложение 1 към ЗЗД от 2018 г., и при спазване на конкретните изисквания, определени за всяка от тези цели и за всеки от тези случаи. Например данни за присъди може да бъдат обработвани от структури с нестопанска цел, ако обработването се извършва а) при подходящи гаранции в хода на законните дейности на фондация, сдружение или друга структура с нестопанска цел, с политическа, философска, религиозна или синдикална цел, и б) при условие че i) обработването е свързано единствено с членовете или бившите членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че ii) личните данни не се разкриват без съгласието на субектите на данни.

([41]) Точки 38—40 от приложение 1 към ЗЗД от 2018 г.

(42) Освен това в част 3 от приложение 1 към ЗЗД от 2018 г. са определени допълнителни обстоятелства, при които може да се използват данни за присъди, съответстващи на правното основание за обработване на чувствителни данни, предвидено в член 9, параграф 2 от Регламент (ЕС) 2016/679 и в ОРЗД на Обединеното кралство (напр. съгласие на субекта на данни, жизненоважни интереси на физическо лице, ако субектът на данни е юридически или физически неспособен да даде съгласие, ако данните вече явно са направени обществено достояние от субекта на данни, ако обработването е необходимо с цел установяване, упражняване или защита на правни претенции и др.).

2.5.3. *Ограничение на целите, точност, свеждане на данните до минимум, ограничение на съхранението и сигурност на данните*

(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.

(44) Този принцип е предвиден в член 5, параграф 1, буква б) от Регламент (ЕС) 2016/679 и е запазен без промени в член 5, параграф 1, буква б) от ОРЗД на Обединеното кралство. Условията за по-нататъшно съвместимо обработване съгласно член 6, параграф 4 от Регламент (ЕС) 2016/679 също са запазени без съществени изменения в член 6, параграф 4, букви а)—д) от ОРЗД на Обединеното кралство.

(45) Освен това данните следва да бъдат точни и при необходимост да се актуализират. Те следва също така да са подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват, и по принцип да се съхраняват не по-дълго от необходимото за целите, за които се обработват.

(46) Тези принципи на свеждане на данните до минимум, точност и ограничение на съхранението са постановени в член 5, параграф 1, букви в)—д) от Регламент (ЕС) 2016/679 и са запазени без промени в член 5, параграф 1, букви в)—д) от ОРЗД на Обединеното кралство.

(47) Личните данни също 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 бизнес операторите 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.

(48) Сигурността на данните е залегнала в правото на Обединеното кралство чрез принципа на цялостност и поверителност, предвиден в член 5, параграф 1, буква е) от ОРЗД на Обединеното кралство, и в член 32 от ОРЗД на Обединеното кралство относно сигурността на обработването на данни. Тези разпоредби са идентични със съответните разпоредби от Регламент (ЕС) 2016/679. Освен това съгласно ОРЗД на Обединеното кралство се изисква надзорният орган да бъде уведомяван за нарушения на сигурността на личните данни (член 33 от ОРЗД на Обединеното кралство) и нарушението да бъде съобщено на субекта на данни (член 34 от ОРЗД на Обединеното кралство) при същите условия като тези, посочени в членове 33 и 34 от Регламент (ЕС) 2016/679.

2.5.4. *Прозрачност*

(49) Субектите на данни трябва да бъдат информирани за основните характеристики на обработването на техните лични данни.

(50) Това се гарантира от членове 13 и 14 от ОРЗД на Обединеното кралство, в които, освен общият принцип на прозрачност, са залегнали правила относно информацията, която трябва да се предоставя на субекта на данни ([42]). В ОРЗД на Обединеното кралство не се въведени съществени изменения на тези правила в сравнение със съответните разпоредби на Регламент (ЕС) 2016/679. Както в Регламент (ЕС) 2016/679 обаче, изискванията за прозрачност, предвидени в тези членове, са предмет на няколко изключения, посочени в ЗЗД от 2018 г. (вж. съображения 55—72).

([42]) В член 13, параграф 1, буква е) и в член 14, параграф 1, буква е) позоваванията на решенията на Комисията относно адекватното ниво на защита са заменени с позовавания на равностоен инструмент на Обединеното кралство, т.е. на наредбите относно адекватното ниво на защита съгласно ЗЗД от 2018 г. Освен това в член 14, параграф 5, букви в)—г) позоваванията на правото на ЕС или на държавите членки са заменени с позоваване на националното право (като примери за разпоредби на националното право, които може да попаднат в приложното поле на член 14, параграф 5, буква в), Обединеното кралство е посочило член 7 от Закона за търговците на метален скрап от 2013 г., в който са предвидени правила за регистър на разрешенията за търговия с метален скрап, или част 35 от Закона за дружествата от 2006 г., в който са определени правилата относно дружествения регистър. Сред примерите за актове на националното право, които може да попаднат в приложното поле на член 14, параграф 5, буква г), биха могли да се посочат също актовете, в които са определени правила относно професионалната тайна или задължения, залегнали в трудови договори, или задължението за поверителност съгласно общото право (например лични данни, обработвани от медицински лица, специалисти по човешки ресурси, социални работници и т.н.).

2.5.5. *Индивидуални права*

(51) Субектите на данни следва да имат конкретни права, които може да бъде противопоставени на обработващия лични данни или на администратора, по-специално правото на достъп до данните, правото на възражение срещу тяхното обработване, правото на коригиране или изтриване на данните. В същото време тези права могат да бъдат обект на ограничения, доколкото тези ограничения са необходими и пропорционални с цел да се гарантира обществената сигурност или за други важни цели от широк обществен интерес.

2.5.5.1. Материални права

(52) ОРЗД на Обединеното кралство предоставя на физическите лица същите приложими права като Регламент (ЕС) 2016/679. Разпоредбите, в които са определени правата на физическите лица, са запазени в ОРЗД на Обединеното кралство без съществени промени.

(53) Правата включват правото на достъп на субекта на данни (член 15 от ОРЗД на Обединеното кралство), правото на коригиране (член 16 от ОРЗД на Обединеното кралство), правото на изтриване (член 17 от ОРЗД на Обединеното кралство), правото на ограничаване на обработването (член 18 от ОРЗД на Обединеното кралство), задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването (член 19 от ОРЗД на Обединеното кралство), правото на преносимост на данните (член 20 от ОРЗД на Обединеното кралство) и правото на възражение (член 21 от ОРЗД на Обединеното кралство) ([43]). Последното включва също правото на субекта на данни да възрази срещу обработването на лични данни за целите на директния маркетинг, предвидено в член 21, параграфи 2 и 3 от Регламент (ЕС) 2016/679. Освен това, съгласно член 122 от ЗЗД от 2018 г., комисарят по информацията трябва да изготви кодекс за поведение във връзка с осъществяването на директен маркетинг в съответствие с изискванията на законодателството за защита на данните (и на Наредбите от 2003 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (Директива на ЕС)), както и всякакви други насоки за насърчаване на добри практики в директния маркетинг, които комисарят счита за подходящи. Понастоящем Службата на комисаря по информацията разработва кодекса относно директния маркетинг ([44]).

(54) Правото на субекта на данни да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, което поражда правни последствия за субекта на данни или по подобен начин го засяга в значителна степен, както е предвидено в член 22 от ОРЗД, също е запазено в ОРЗД на Обединеното кралство без съществени промени. Добавен е обаче нов параграф 3А, в който е направено позоваване на член 14 от ЗЗД от 2018 г., съдържащ гаранции за правата, свободите и легитимните интереси на субектите на данни, когато обработването се извършва съгласно член 22, параграф 2, буква б) от ОРЗД на Обединеното кралство. Тази нова разпоредба се прилага само когато основанието за такова решение е разрешение или изискване съгласно правото на Обединеното кралство и не се прилага, когато решението е необходимо съгласно договор или е взето с изричното съгласие на субекта на данни. Когато се прилага член 14 от ЗЗД от 2018 г., администраторът трябва, веднага щом това е практически осъществимо, да уведоми субекта на данни, че е взето решение, основаващо се единствено на автоматизирано обработване. В рамките на един месец от получаване на уведомлението субектът на данни има право да поиска от администратора да преразгледа решението или да вземе ново решение, което не се основава единствено на автоматизирано обработване. Министърът има правомощието да въвежда допълнителни гаранции по отношение на автоматизираното вземане на решения. Това правомощие все още не е упражнявано.

2.5.5.2. Ограничения на индивидуалните права и други разпоредби

(55) В ЗЗД от 2018 г. са предвидени няколко ограничения на индивидуалните права, които се вписват в разпоредбите на член 23 от ОРЗД на Обединеното кралство. В този нормативен акт не са въведени ограничения по отношение на правото на възражение срещу директен маркетинг, както е предвидено в член 21, параграфи 2 и 3 от ОРЗД на Обединеното кралство, нито на правото субектът на данни да не бъде обект на автоматизирано вземане на решения, както е предвидено в член 22 от ОРЗД за Обединеното кралство.

(56) Ограниченията са описани подробно в приложения 2—4 към ЗЗД от 2018 г. Органите на Обединеното кралство поясниха, че са се ръководили от два принципа: принципа на специфичност (възприемане на подробен подход, разделяне на по-общи ограничения на множество, по-конкретни разпоредби) и принципа на обвързаност с условия (всяка разпоредба е съчетана с гаранции под формата на ограничения или условия с цел предотвратяване на злоупотреби) ([45]).

([43]) В член 17, параграф 1, буква д) и в член 17, параграф 3, буква б) позоваванията на правото на ЕС или на държавите членки са заменени с позоваване на националното право (като примери за разпоредби на националното право по член 17, параграф 1, буква д) Обединеното кралство е посочило Наредбите от 2006 г. за образованието (Информация за учениците) (Англия), съгласно които се изисква имената на учениците да бъдат заличени от училищните регистри след напускане на училището, или член 34F от Закона за медицината от 1983 г., в който са определени правилата относно заличаването на имена от Регистъра на общопрактикуващите лекари и от Регистъра на специалистите.

([44]) Проектът на кодекса за поведение може да бъде намерен на следния адрес: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел Е: Ограничения, стр. 1, достъпна на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) Ограниченията, описани в член 23, параграф 1 от ОРЗД на Обединеното кралство, имат за цел да се гарантира, че те ще се прилагат само при определени обстоятелства, когато това е необходимо в едно демократично общество и пропорционално на легитимната цел, която се преследва с тях. Освен това, в съответствие с установената съдебна практика относно тълкуването на ограниченията, изключения от режима на защита на данните във всеки конкретен случай се допускат само ако това е необходимо и пропорционално ([46]). Изисква се проверката за необходимост да бъде „строга, а всякаква намеса в правата на субекта да бъде пропорционална на сериозността на заплахата за обществения интерес. Следователно при извършването ѝ е необходим класически анализ на пропорционалността ([47])."

(58) Целта, която се преследва с тези ограничения, съответства на изброените в член 23 от Регламент (ЕС) 2016/679, с изключение на ограниченията, свързани с националната сигурност и отбрана, които са регламентирани в член 26 от ЗЗД от 2018 г., но подлежат на същите изисквания за необходимост и пропорционалност (вж. съображения 63—66).

(59) При някои ограничения, например тези, свързани с предотвратяване или разкриване на престъпления, задържане или наказателно преследване на нарушители, както и с определяне или събиране на данъци или мита ([48]), се допуска ограничаване на всички индивидуални права и задължения за прозрачност (с изключение на правата по член 21, параграф 2 и член 22). Обхватът на други ограничения се простира единствено до задълженията за прозрачност и правата на достъп, например ограниченията, свързани с адвокатската тайна ([49]), с правото на освобождаване от изискване за предоставяне на информация, която би довела до самоуличаване ([50]), и с корпоративните финанси, особено за предотвратяване на злоупотреба с вътрешна информация ([51]). При малък брой ограничения се допуска да бъдат ограничени задължението на администратора да съобщава на субекта на данни за нарушение на сигурността на неговите данни и принципите на ограничение на целите, както и на законосъобразност, добросъвестност и прозрачност на обработването ([52]).

(60) Някои ограничения се прилагат автоматично „в своята цялост" по отношение на определен вид обработване на лични данни (например задълженията за прозрачност и индивидуалните права не важат, когато личните данни се обработват с цел оценка на годността на дадено лице за съдебна длъжност или личните данни се обработват от съд, правораздавателен орган или физическо лице, действащо в изпълнение на съдебните си функции).

(61) В повечето случаи обаче в съответната точка от приложение 2 към ЗЗД от 2018 г. се уточнява, че ограничението се прилага само когато (и доколкото) прилагането на разпоредбите „има вероятност да накърни" легитимната цел, която се преследва с това ограничение: например изброените разпоредби на ОРЗД на Обединеното кралство не се прилагат по отношение на лични данни, обработвани за предотвратяване или разкриване на престъпления, задържане или наказателно преследване на нарушители, или за определяне или събиране на данък или мито, „ доколкото прилагането на тези разпоредби има вероятност да накърни" някоя от посочените дейности ([53]).

(62) „Вероятността да накърни" се тълкува последователно от съдилищата на Обединеното кралство като „много значима и сериозна възможност да бъдат накърнени определените обществени интереси" ([54]). Следователно ограничение, което подлежи на оценка на вероятността да бъдат накърнени целите, може да се използва само ако и доколкото е налице много значима и сериозна възможност предоставянето на определено право да накърни въпросния обществен интерес. Администраторът носи отговорност да прецени във всеки отделен случай дали тези условия са изпълнени ([55]).

(63) В допълнение към ограниченията, съдържащи се в приложение 2 към ЗЗД от 2018 г., в член 26 от ЗЗД от 2018 г. е предвидено изключение, което може да бъде приложено по отношение на някои разпоредби на ОРЗД на Обединеното кралство и на ЗЗД от 2018 г., ако това е необходимо с цел да се гарантира националната сигурност или за целите на отбраната. Това изключение се прилага по отношение на принципите за защита на данните (с изключение на принципа на законосъобразност), на задълженията за прозрачност, на правата на субекта на данни, на

([46]) *Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), точки 40 и 41.
([47]) *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), т. 43. По този въпрос вж. също *Lin/Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), т. 80.
([48]) Точка 2 от приложение 2 към ЗЗД от 2018 г.
([49]) Точка 19 от приложение 2 към ЗЗД от 2018 г.
([50]) Точка 20 от приложение 2 към ЗЗД от 2018 г.
([51]) Точка 21 от приложение 2 към ЗЗД от 2018 г.
([52]) Например ограничения на правото на уведомление за нарушения на сигурността на данните се допускат само във връзка с престъпления и с данъчно облагане (точка 2 от приложение 2 към ЗЗД от 2018 г.), с парламентарен имунитет (точка 13 от приложение 2 към ЗЗД от 2018 г.) и с обработване за журналистически, академични, художествени и литературни цели (точка 26 от приложение 2 към ЗЗД от 2018 г.).
([53]) Точка 2 от приложение 2 към ЗЗД от 2018 г.
([54]) *R (Lord)/Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), т. 100 и *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), т. 43.
([55]) *Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor,* т. 31.

задължението за уведомяване в случай на нарушение на сигурността на данните, на правилата за международно предаване на данни, на някои задължения и правомощия на комисаря по информацията, както и на правилата относно правните средства за защита, отговорностите и санкциите, с изключение на разпоредбата относно общите условия за налагане на административни наказания „глоба“ или „имуществена санкция“, посочени в член 83 от ОРЗД на Обединеното кралство, и разпоредбата относно санкциите в член 84 от ОРЗД на Обединеното кралство. Освен това с член 28 от ЗЗД от 2018 г. се въвеждат изменения в прилагането на член 9, параграф 1, за да се даде възможност за обработването на специални категории данни, предвидено в член 9, параграф 1 от ОРЗД на Обединеното кралство, доколкото това обработване се извършва с цел защита на националната сигурност или за целите на отбраната и с подходящи гаранции за правата и свободите на субектите на данни ([56]).

(64) Изключението може да се прилага само дотолкова, доколкото е необходимо, за да се гарантира националната сигурност или отбрана. Както и при другите изключения, предвидени в ЗЗД от 2018 г., това изключение трябва да се преценява и прилага от администратора за всеки отделен случай. Освен това всяко негово прилагане трябва да е в съответствие със стандартите за правата на човека (залегнали в Закона за правата на човека от 1998 г.), според които всяка намеса в правата на неприкосновеност на личния живот следва да бъде необходима и пропорционална в едно демократично общество ([57]).

(65) Това тълкуване на изключението се потвърждава от комисаря по информацията, който е издал подробни насоки относно прилагането на изключението, свързано с националната сигурност и отбрана, като ясно посочва, че то трябва да бъде разглеждано и прилагано от администратора за всеки отделен случай ([58]). В насоките по-специално се подчертава, че „[т]ова не е общо изключение“ и че за да бъде използвано, „не е достатъчно данните да се обработват за целите на националната сигурност“. Напротив, за да се позове на него, администраторът трябва да „докаже, че е налице реална възможност за неблагоприятни последици за националната сигурност“, а при необходимост от него се очаква „да предостави [на комисаря по информацията] доказателства за причините, поради които [той] е използвал това изключение“. Насоките съдържат контролен списък и редица примери за допълнително изясняване на условията, при които може да се направи позоваване на това изключение.

(66) Следователно фактът, че данните се обработват за целите на националната сигурност или отбрана, сам по себе си не е достатъчен, за да бъде приложено изключението. Администраторът трябва да вземе предвид действителните последици за националната сигурност, ако трябва да спази конкретната разпоредба за защита на данните. Изключението може да се прилага само по отношение на конкретни разпоредби, за които е установено, че представляват риск, и трябва да се прилага възможно най-ограничително ([59]).

(67) Този подход е потвърден от Съда по въпросите на информацията (*Information Tribunal*) ([60]). В решението си по делото *Baker/Secretary of State for the Home Department* (*Baker/Secretary of State*) Съдът е определил, че е незаконно изключението във връзка с националната сигурност да се прилага като общо изключение по отношение на исканията за достъп, получени от разузнавателните служби. Вместо това изключението трябва да се прилага за всеки отделен случай, като всяко искане се разглежда по същество и с оглед на правото на лицата да бъде зачитана неприкосновеността на личния им живот ([61]).

([56]) Според информацията, предоставена от органите на Обединеното кралство, когато обработването се извършва в контекста на националната сигурност, администраторите обикновено прилагат засилени гаранции и мерки за сигурност по отношение на обработването, които отразяват неговия чувствителен характер. Кои гаранции са подходящи ще зависи от рисковете, породени от извършваното обработване. Това може да включва ограничения на достъпа до данните, така че той да може да се осъществява само от упълномощени лица с подходящо разрешение за достъп, строги ограничения за споделянето на данните и високи стандарти за сигурност, приложими към процедурите за съхранение и обработване.

([57]) Вж. също *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), т. 45; *Lin/Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), т. 80.

([58]) Вж. също насоките на комисаря по информацията относно изключението, свързано с националната сигурност и отбрана, достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) Според пример, предоставен от органите на Обединеното кралство, ако заподозрян терорист, срещу когото е в ход разследване на MI5, отправи искане за достъп до Министерството на вътрешните работи (например тъй като е страна по спор с Министерството на вътрешните работи по имиграционни въпроси), би било необходимо да се защитят от разкриване на субекта на данни всички данни, които MI5 може да е споделила с Министерството на вътрешните работи във връзка с текущи разследвания и които биха могли да засегнат чувствителни източници, методи или техники и/или да доведат до увеличаване на заплахата, която представлява лицето. При такива обстоятелства е вероятно прагът за прилагане на изключението по член 26 да е спазен и изключението от разкриване на информацията да е необходимо, за да се гарантира националната сигурност. Ако обаче Министерството на вътрешните работи разполага и с лични данни за лицето, които не са свързани с разследването на MI5, и тази информация може да бъде предоставена без риск от нанасяне на вреда за националната сигурност, тогава изключението във връзка с националната сигурност не би било приложимо, когато се преценява дали информацията да бъде разкрита на лицето. Комисарят по информацията понастоящем изготвя насоки за подхода, който администраторите следва да прилагат при използването на изключението по член 26. Насоките се очаква да бъдат публикувани в края на март 2021 г.

([60]) Съдът по въпросите на информацията е създаден, за да разглежда жалби във връзка със защита на данни съгласно Закона за защита на данните от 1984 г. През 2010 г., в рамките на реформата в структурата на системата от съдилища в Обединеното кралство, Съдът по въпросите на информацията стана част от отделението „Общи правни въпроси“ (*General Regulatory Chamber*) на трибунала от първа инстанция (*First Tier Tribunal*).

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

2.5.6. *Ограничения по отношение на личните данни, обработвани за журналистически, академични, художествени и литературни цели, както и с цел архивиране и научни изследвания*

(68) Съгласно член 85, параграф 2 от ОРЗД на Обединеното кралство се допуска приемането на разпоредби, въз основа на които личните данни, обработвани за журналистически, художествени, академични и литературни цели, да бъдат изключени от няколко разпоредби на ОРЗД на Обединеното кралство. Изключенията по отношение на обработването на лични данни за тези цели са посочени в част 5 от приложение 2 към ЗЗД от 2018 г. В нея са предвидени изключения по отношение на принципите за защита на данните (с изключение на принципа на цялостност и поверителност), правните основания за обработване (вкл. на специални категории данни, данни за присъди и др.), условията за съгласие, задълженията за прозрачност, правата на субекта на данни, задължението за уведомяване в случай на нарушение на сигурността на данните, и изискването за допитване до комисаря по информацията преди обработването на данни с висок риск и правилата за международно предаване на данни ([62]). В това отношение ОРЗД на Обединеното кралство не се отклонява по същество от Регламент (ЕС) 2016/679, в член 85 от който също е предвидена възможността обработването, извършвано за журналистически цели и за целите на академичното, художественото или литературното изразяване, да бъде изключено от редица изисквания на Регламент (ЕС) 2016/679. Разпоредбите на ЗЗД от 2018 г., по-специално на приложение 2, част 5 към него, са съвместими с ОРЗД на Обединеното кралство.

(69) Основната преценка, която трябва да бъде направена съгласно член 85 от ОРЗД на Обединеното кралство, се отнася до това дали изключението от правилата за защита на данните, споменато в съображение 68, е „необходимо, за да се постигне баланс между правото на защита на личните данни и свободата на изразяване и на информация“ ([63]). Съгласно точка 26, подточки 2 и 3 от приложение 2 към ЗЗД от 2018 г. Обединеното кралство разчита на преценка на „основателното убеждение“, за да бъде постигнат този баланс. За да бъде оправдано изключението, администраторът трябва с основание да е убеден, че i) публикуването е в обществен интерес; и че ii) прилагането на съответната разпоредба от ОРЗД би било несъвместимо с журналистически, академични, художествени или литературни цели. Както се потвърждава от съдебната практика ([64]), преценката на „основателното убеждение“ има както субективен, така и обективен компонент: не е достатъчно администраторът да докаже, че самият той е убеден, че спазването на разпоредбите е несъвместимо с целите. Неговото убеждение трябва да бъде основателно, т.е. да може да бъде споделено от разумен човек, запознат със съответните факти. Следователно администраторът трябва да положи дължимата грижа, когато изгражда убеждението си, за да може да докаже неговата основателност. Според обясненията, предоставени от органите на Обединеното кралство, преценката на „основателното убеждение“ трябва да се извършва за всяко изключение поотделно ([65]). Ако условията са изпълнени, изключението се счита за необходимо и пропорционално съгласно правото на Обединеното кралство.

(70) Съгласно член 124 от ЗЗД от 2018 г. комисарят по информацията трябва да изготви Кодекс за поведение относно защитата на данни и журналистиката. Работата по този кодекс е в ход. Издадени са насоки по въпроса съгласно Закона за защита на данните от 1998 г., в които се подчертава по-специално, че за да бъде приложено това изключение, не е достатъчно само да се заяви, че спазването на разпоредбата би затруднило работата на

([62]) Вж. член 85 от ОРЗД на Обединеното кралство и част 5, точка 26, подточка 9 от приложение 2 към ЗЗД от 2018 г.

([63]) В съответствие с част 5, точка 26, подточка 2 от приложение 2 към ЗЗД от 2018 г. изключението се прилага по отношение на обработването на лични данни, извършвано за специални цели (журналистически, академични, художествени и литературни), ако то се осъществява с оглед на публикуването от страна на физическо лице на журналистически, академичен, художествен или литературен материал и администраторът с основание е убеден, че публикуването на този материал би било в обществен интерес. Когато преценява дали дадена публикация би била в обществен интерес, администраторът трябва да вземе предвид особената важност на обществения интерес за свободата на изразяване и на информация. Освен това администраторът трябва да вземе предвид кодексите на поведение или насоките, които имат отношение към въпросната публикация (Редакционните насоки на Би Би Си (BBC Editorial Guidelines), Кодекса за телевизионно и радиоразпръскване на Службата по съобщенията (Ofcom Broadcasting Code) и Кодекса за поведение на редакторите (Editors' Code of Practice). Освен това, за да се приложи дадено изключение, администраторът трябва с основание да е убеден, че спазването на съответната разпоредба би било несъвместимо със специалните цели (точка 26, подточка 3 от приложение 2 към ЗЗД от 2018 г.).

([64]) В решението по делото *NT1/Google* [2018] EWHC 799 (QB), т. 102 е разгледан подробно въпросът дали администраторът на данни е бил убеден с основание, че публикуването е в обществен интерес и че спазването на съответните разпоредби е несъвместимо със специалните цели. Съдът се е произнесъл, че разпоредбите на член 32, параграф 1, букви б) и в) от Закона за защита на данните от 1998 г. имат субективен и обективен елемент: администраторът на данни трябва да докаже, че е бил убеден, че публикуването би било в обществен интерес, и че това убеждение обективно е основателно; той трябва да докаже и субективното убеждение, че спазването на разпоредбата, от която се иска изключение, би било несъвместимо с въпросната специална цел.

([65]) Пример за прилагането на изискването за преценка на „основателното убеждение“ се съдържа в решението на комисаря по информацията за налагането на глоба на *True Visions Productions*, прието съгласно Закона за защита на данните от 1998 г. Комисарят по информацията е приел, че е налице субективно убеждение на администратора на медийна информация, че спазването на първия принцип за защита на данните (добросъвестност и законосъобразност) е несъвместимо с журналистическите цели. Той обаче не се е съгласил, че това убеждение обективно е основателно. Решението на комисаря по информацията е достъпно на следния адрес: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

журналистите, а трябва да е налице ясен аргумент, че въпросната разпоредба възпрепятства отговорната журналистика ([66]). Насоки за прилагането на изискването за обществен интерес и за постигането на баланс между обществения интерес и интереса на лицата от неприкосновеност на личния живот също са публикувани от регулатора на Обединеното кралство в областта на далекосъобщенията — Службата по съобщенията, и от Би Би Си в техните редакционни насоки ([67]). В насоките по-специално са дадени примери за информация, за която може да се смята, че е в обществен интерес, и е разяснена необходимостта да се докаже, че общественият интерес има превес над правата на неприкосновеност на личния живот при конкретните обстоятелства по случая.

(71) Подобно на предвиденото в член 89 от ОРЗД, личните данни, обработвани за целите на архивирането в обществен интерес, за научни или исторически изследвания, или за статистически цели, също може да бъдат освободени от редица изброени разпоредби на ОРЗД на Обединеното кралство ([68]). По отношение на научните изследвания и статистиката са възможни изключения от разпоредбите на ОРЗД на Обединеното кралство, свързани с потвърждаване на обработването и достъпа до данни и гаранциите за предаване към трети държави; правото на коригиране; ограничаване на обработването и възражение срещу обработването. Що се отнася до архивирането в обществен интерес, са възможни изключения и от задължението за уведомяване относно коригирането или заличаването на лични данни или ограничаването на обработването, както и от правото на преносимост на данните.

(72) Съгласно точка 27, подточка 1 и точка 28, подточка 1 от приложение 2 към ЗЗД от 2018 г. изключения от изброените разпоредби на ОРЗД на Обединеното кралство са възможни, когато прилагането на разпоредбите би „направило невъзможно или сериозно би затруднило постигането“ на въпросните цели ([69]).

(73) Като се има предвид тяхното значение за ефективното упражняване на индивидуалните права, всяка относима промяна по отношение на тълкуването и прилагането на практика на горепосочените изключения (в допълнение към това, свързано с поддържането на ефективен имиграционен контрол, както е обяснено в съображение 6), включително всяко по-нататъшно развитие на съдебната практика и на насоките на комисаря по информацията и изпълнителните действия, ще бъде надлежно взето предвид в контекста на непрекъснатото наблюдение на настоящото решение ([70]).

2.5.7. *Ограничения на последващото предаване на данни*

(74) Нивото на защита на личните данни, което се осигурява за данните, предавани от Европейския съюз към администратори или обработващи лични данни в Обединеното кралство, не трябва да бъде подкопавано от по-нататъшното предаване на тези данни към получатели в трета държава. Подобно „последващо предаване“, което от гледна точка на администратора или на обработващия лични данни в 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. Поради тази причина прилагането на правилата на ОРЗД на Обединеното кралство и на ЗЗД от 2018 г. относно международното предаване на лични данни е важен фактор за гарантиране на непрекъснатостта на защитата в случай на лични данни, предадени от Европейския съюз към Обединеното кралство съгласно настоящото решение.

([66]) Съгласно насоките организациите трябва да са в състояние да обяснят защо спазването на съответната разпоредба на Закона за защита на данните от 1998 г. е несъвместимо с целите на журналистиката. По-специално администраторите трябва да постигнат баланс между неблагоприятните последици, които спазването на разпоредбите би имало за журналистиката, и неблагоприятните последици, които неспазването им би имало за правата на субекта на данни. Ако е основателно да се смята, че един журналист може да постигне редакционните си цели при спазване на стандартните разпоредби на ЗЗД, те трябва да се спазват. Организациите трябва да са в състояние да обосноват прилагането на ограничението по отношение на всяка разпоредба, която не са спазили. „Защита на данните и журналистика: ръководство за медиите“ (*Data protection and journalism: a guide for the media*), достъпно на следния адрес: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

([67]) Общественият интерес би могъл да включва например разобличаване или разкриване на престъпления, защита на общественото здраве или безопасност, разобличаване на подвеждащи твърдения, отправени от лица или организации, или разкриване на некомпетентност, която засяга обществеността. Вж. насоките на Службата по съобщенията, достъпни на следния адрес: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf, и Редакционните насоки на Би Би Си, достъпни на следния адрес: https://www.bbc.com/editorialguidelines/guidelines/privacy

([68]) Вж. член 89 от ОРЗД на Обединеното кралство и част 6, точка 27, подточка 2 и точка 28, подточка 2 от приложение 2 към ЗЗД от 2018 г.

([69]) При спазване на изискването личните данни да се обработват в съответствие с член 89, параграф 1 от ОРЗД на Обединеното кралство, допълнен от член 19 от ЗЗД от 2018 г.

([70]) Вж. съображения 281—287.

(75) Режимът относно международното предаване на лични данни от Обединеното кралство е установен в членове 44—49 от ОРЗД на Обединеното кралство, допълнен от ЗЗД от 2018 г., и по същество е идентичен с правилата, предвидени в глава V от Регламент (ЕС) 2016/679 ([71]). Предаването на лични данни на трета държава или на международна организация може да се извършва само въз основа на наредби относно адекватното ниво на защита (еквивалента в Обединеното кралство на решението относно адекватното ниво на защита съгласно Регламент (ЕС) 2016/679) или при липса на наредби относно адекватното ниво на защита — при условие че администраторът или обработващият лични данни е предоставил подходящи гаранции в съответствие с член 46 от ОРЗД на Обединеното кралство. При липсата на наредби относно адекватното ниво на защита или на подходящи гаранции предаването може да се извърши само въз основа на дерогации, посочени в член 49 от ОРЗД на Обединеното кралство.

(76) В наредбите относно адекватното ниво на защита, издадени от министъра, може да се предвижда, че трета държава (или територия или сектор в рамките на трета държава) или международна организация, или описание ([72]) на такава държава, територия, сектор или организация, трябва да гарантира адекватно ниво на защита на личните данни. Когато оценява адекватността на нивото на защита, министърът трябва да вземе предвид съвсем същите елементи, които Комисията е длъжна да оцени съгласно член 45, параграф 2, букви а)—в) от Регламент (ЕС) 2016/679, тълкувани във връзка със съображение 104 от Регламент (ЕС) 2016/679, и запазената съдебна практика на ЕС. Това означава, че когато се оценява адекватното ниво на защита на трета държава, съответният стандарт трябва да бъде дали въпросната трета държава осигурява ниво на защита, „по същество равностойно“ на това, гарантирано в рамките на Обединеното кралство.

(77) Що се отнася до процедурата, спрямо наредбите тносно адекватното ниво на защита се прилагат „общите“ процесуални изисквания, предвидени в член 182 от ЗЗД от 2018 г. В рамките на тази процедура, когато предлага да се приемат наредби на Обединеното кралство относно адекватното ниво на защита ([73]), 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 наредбите и имат правомощието да приемат предложение за отмяна на наредбите в срок от 40 дни ([74]).

(78) Съгласно член 17 В, 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. Тези процедурни аспекти също отразяват съответните изисквания на Регламент (ЕС) 2016/679.

([71]) С изключение на член 48 от Регламент (ЕС) 2016/679, който Обединеното кралство е решило да не включва в ОРЗД на Обединеното кралство. В тази връзка най-напред следва да се припомни, че стандартът, за който следва да се счита, че осигурява адекватно ниво на защита, е по-скоро стандарт за „равностойност по същество“, а не за идентичност, както е уточнено от Съда на ЕС (дело *Schrems I*, точки 73—74) и признато от ЕКЗД (Референтен документ за адекватното ниво на защита, стр. 3). Поради това, както е обяснено от ЕКЗД в неговия Референтен документ за адекватното ниво на защита, „целта не е да се отрази точка по точка европейското законодателство, а да се установят съществените, основните изисквания на това законодателство“. В това отношение е важно да се отбележи, че макар правният ред на Обединеното кралство формално да не съдържа разпоредба, идентична с член 48, същият ефект се гарантира от други правни разпоредби и принципи, т.е. че в отговор на искане за лични данни от страна на съд или административен орган в трета държава личните данни могат да бъдат предадени на тази трета държава само ако е налице международно споразумение — въз основа на което въпросното съдебно решение или административно решение на третата държава се признава или изпълнява в Обединеното кралство — или ако това се основава на един от механизмите за предаване, предвидени в глава V от ОРЗД на Обединеното кралство. По-специално, за да приведат в изпълнение чуждестранно съдебно решение, съдилищата в Обединеното кралство трябва да могат да се позоват на общото право или на закон, който позволява изпълнението на това решение. Нито общото право обаче (вж. *Adams u др./Cape Industries Plc.*, [1990] 2 W.L.R. 657), нито писаните закони предвиждат изпълнение на чуждестранни решения, съгласно които се изисква предаване на данни, без да е налице международно споразумение. В резултат на това съгласно правото на Обединеното кралство исканията за данни не подлежат на изпълнение при липса на такова международно споразумение. Освен това всяко предаване на лични данни към трети държави — включително по искане на чуждестранен съд или административен орган — остава подчинено на ограниченията, посочени в глава V от ОРЗД на Обединеното кралство, които са идентични със съответните разпоредби на Регламент (ЕС) 2016/679, и поради това се изисква позоваване на някое от основанията за предаване по глава V в съответствие със специфичните условия, на които то е подчинено съгласно посочената глава.

([72]) 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. наредби относно адекватното ниво на защита по отношение само на определен вид предаване на данни).

([73]) Вж. Меморандума за разбирателство между министъра на цифровите технологии, културата, медиите и спорта и Службата на комисаря по информацията относно ролята на ICO във връзка с новата оценка на адекватността на 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.

([74]) Ако бъде направено такова гласуване, в крайна сметка наредбите ще престанат да пораждат правно действие за в бъдеще.

(79) При липса на наредби относно адекватното ниво на защита международно предаване може да се извършва само когато администраторът или обработващият лични данни е предвидил подходящи гаранции в съответствие с член 46 от ОРЗД на Обединеното кралство. Тези гаранции са подобни на предвидените съгласно член 46 от Регламент (ЕС) 2016/679. Те включват инструменти със задължителен характер и с изпълнителна сила между публичните органи или структури, задължителни фирмени правила ([75]), стандартни клаузи за защита на данните, одобрени кодекси за поведение, одобрени механизми за сертифициране и — с разрешението на комисаря по информацията — договорни клаузи между администраторите (или обработващите лични данни) или административни договорености между публичните органи. Правилата обаче са променени от процедурна гледна точка, така че да съответстват на уредбата на Обединеното кралство, по-специално по отношение на стандартните клаузи за защита на данните, които съгласно ЗЗД от 2018 г. могат да се приемат от министъра (член 17Б) или от комисаря по информацията (член 119А).

(80) При липса на решение относно адекватното ниво на защита или на подходящи гаранции предаване може да се извършва само въз основа на дерогациите, предвидени в член 49 от ОРЗД на Обединеното кралство ([76]). С ОРЗД на Обединеното кралство не се въвеждат съществени промени в дерогациите в сравнение със съответните правила, залегнали в Регламент (ЕС) 2016/679. Съгласно ОРЗД на Обединеното кралство, както и съгласно Регламент (ЕС) 2016/679, на някои дерогации може да се разчита само ако предаването на данни е спорадично ([77]). Освен това в своите насоки относно международното предаване на данни комисарят по информацията пояснява: „Следва да използвате [дерогациите] само като действителни „изключения“ от общото правило, че не следва да извършвате ограничено предаване на данни, освен ако то не е обхванато от решение относно адекватното ниво на защита или не са налице подходящи гаранции“ ([78]). По отношение на предаването на данни, които са необходими по важни причини от обществен интерес (член 49, параграф 1, буква г), министърът може да въведе разпоредби, за да уточни обстоятелствата, при които предаването на лични данни към трета държава или към международна организация не е необходимо поради важни причини от обществен интерес. Освен това министърът може да ограничи с наредби предаването на категория лични данни на трета държава или на международна организация, когато то не може да се извърши въз основа на наредби относно адекватното ниво на защита, а министърът смята, че ограничението е необходимо поради важни причини от обществен интерес. Такива наредби все още не са приети.

(81) Тази рамка за международно предаване на данни започна да се прилага в края на преходния период ([79]). В точка 4 от приложение 21 към ЗЗД от 2018 г. (въведено с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС) 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 от ЕИП, към територията на Гибралтар, към институция, орган, служба или агенция на Съюза, създадени по силата или въз основа на Договора за ЕС, и към трети държави, спрямо които в края на преходния период се е прилагало решение на ЕС относно адекватното ниво на защита. Следователно предаването към тези държави може да

([75]) В ОРЗД на Обединеното кралство са запазени правилата, предвидени в член 47 от Регламент (ЕС) 2016/679, като са извършени изменения само с оглед на съответствието им с националната уредба, например препратките към компетентния надзорен орган са заменени с препратки към комисаря по информацията, препратката към механизма за съгласуваност е премахната от параграф 1 и целият параграф 3 е заличен.

([76]) Съгласно член 49 от ОРЗД за Обединеното кралство предаването на данни е възможно, ако е изпълнено едно от следните условия: а) субектът на данни изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за възможните рискове, свързани с предаването, за субекта на данни поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции; б) предаването е необходимо за изпълнението на договор между субекта на данни и администратора или за изпълнението на преддоговорни мерки, предприети по искане на субекта на данни; в) предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данни между администратора и друго физическо или юридическо лице; г) предаването е необходимо поради важни причини от обществен интерес; д) предаването е необходимо за установяването, упражняването или защитата на правни претенции; е) предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данни или на други лица, когато субектът на данни е физически или юридически неспособен да даде своето съгласие; ж) предаването се извършва от регистър, който съгласно националното право е предназначен за предоставяне на информация на обществеността и е открит за извършване на справки от широката общественост или от всяко лице, което може да докаже легитимен интерес, но само при условие че в конкретния случай са изпълнени предвидените в националното право условия за извършване на справки. Освен това, когато никое от горните условия не е приложимо, предаването на данни може да се извършва само ако не е повтаряемо, засяга само ограничен брой субекти на данни, необходимо е за целите на неоспоримите легитимни интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данни, и администраторът е оценил всички обстоятелства, свързани с предаването на данните, и въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни.

([77]) В съображение 111 от ОРЗД на Обединеното кралство се посочва, че предаването на данни във връзка с договор или правни претенции може да се извършва само спорадично.

([78]) Насоки на комисаря по информацията относно международното предаване на данни, достъпни на следния адрес: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

([79]) За срок от максимум шест месеца, приключващ най-късно на 30 юни 2021 г., 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

продължи 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.

(82) И накрая, що се отнася до бъдещото развитие на режима на Обединеното кралство за международно предаване на данни — чрез приемането на нови наредби относно адекватното ниво на защита, сключването на международни споразумения или разработването на други механизми за предаване — Комисията ще наблюдава отблизо ситуацията, ще преценява дали различните механизми за предаване се използват по начин, който гарантира непрекъснатост на защитата, и ако е необходимо, ще предприеме подходящи мерки за справяне с възможните неблагоприятни последици за тази непрекъснатост (вж. съображения 278—287). Тъй като ЕС и Обединеното кралство имат сходни правила относно международното предаване на данни, очаква се проблематичните различия да могат да бъдат избегнати и чрез сътрудничество, обмен на информация и споделяне на опит, включително между комисаря по информацията и ЕКЗД.

2.5.8. *Отчетност*

(83) Съгласно принципа на отчетност 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.

(84) Принципът на отчетност, предвиден в Регламент (ЕС) 2016/679, е запазен в член 5, параграф 2 от ОРЗД на Обединеното кралство без съществени промени, като същото важи за член 24 относно отговорността на администратора, член 25 относно защитата на данните на етапа на проектирането и по подразбиране и член 30 относно регистрите на дейностите по обработване. Запазени са също членове 35 и 36 относно оценката на въздействието върху защитата на данните и относно предварителната консултация с надзорния орган. Членове 37—39 от Регламент (ЕС) 2016/679 относно определянето и задачите на длъжностните лица по защита на данните са запазени в ОРЗД на Обединеното кралство без съществени промени. Освен това разпоредбите на членове 40 и 42 от Регламент (ЕС) 2016/679 относно кодексите за поведение и сертифицирането са запазени в ОРЗД на Обединеното кралство ([80]).

2.6. **Надзор и привеждане в изпълнение**

2.6.1. *Независим надзор*

(85) С цел да се гарантира, че адекватното ниво на защита на данните се осигурява 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.

(86) 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. 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 ([81]). Комисарят по информацията е на бюджетна издръжка на Министерството на цифровите технологии, културата, медиите и спорта (DCMS) ([82]).

(87) Независимостта на комисаря е изрично уредена в член 52 от ОРЗД на Обединеното кралство, с който не се правят съществени промени спрямо член 52, параграфи 1—3 от ОРЗД. 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

([80]) Когато е необходимо, тези препратки се заменят с препратки към органите на Обединеното кралство. Например съгласно раздел 17 от ЗЗД от 2018 г. комисарят по информацията или националният орган по акредитация на Обединеното кралство може да акредитира лице, отговарящо на изискванията, посочени в член 43 от ОРЗД на Обединеното кралство, да наблюдава съответствието с изискванията за сертифициране.

([81]) 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.

([82]) Отношенията им се уреждат със споразумение за управление. По-специално основните отговорности на DCMS като финансиращо ведомство включват: да гарантира, че комисарят по информацията е обезпечен с адекватно финансиране и ресурси; да представлява на интересите на комисаря по информацията пред Парламента и други държавни ведомства; да осигури наличието на солидна национална уредба за защита на данните; и да предоставя насоки и подкрепа на Службата на комисаря по информацията 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)

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.

(88) 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 Нейно Величество 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 ([83]) 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 ([84]).

(89) Комисарят по информацията има мандат до седем години. Едно и също лице не може да бъде назначено като комисар по информацията повече от веднъж. Комисарят по информацията може да бъде отстранен от длъжност от Нейно величество след обръщение от страна на двете камари на Парламента ([85]). 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 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 ([86]).

(90) 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 ([87]) (Наредба за защита на данните (такси и информация) от 2018 г.), и възлизат на 85—90 % от годишния бюджет на Службата ([88]); ii) безвъзмездна помощ, изплатена от правителството на комисаря по информацията. Безвъзмездната помощ се използва главно за финансиране на неговите оперативни разходи във връзка със задачи, които не са свързани със защитата на данните ([89]); и iii) таксите, събирани за услуги ([90]). Понастоящем не се събират такива такси.

(91) Общите функции на комисаря по информацията във връзка с обработването на лични данни, които попадат в приложното поле на ОРЗД на Обединеното кралство, са определени в член 57 от него и отразяват в голяма степен съответните правила, предвидени в Регламент (ЕС) 2016/679. Неговите функции включват наблюдение и прилагане на ОРЗД на Обединеното кралство, насърчаване на обществената осведоменост, разглеждане на жалби, подадени от субектите на данни, провеждане на разследвания и др. Освен това в член 115 от ЗЗД от 2018 г. са определени други общи функции на комисаря, които включват задължение да съветва Парламента, правителството и други институции и органи относно законодателни и административни мерки, свързани със защитата на правата и свободите на лицата по отношение на обработването на лични данни, както и правомощия да дава становища, по собствена инициатива

([83]) Кодекс за управление на публичните назначения, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf.

([84]) 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.

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

([86]) Точка 3, подточка 3 от приложение 12 към ЗЗД от 2018 г.

([87]) Член 137 от ЗЗД от 2018 г., вж. съображение 17.

([88]) 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 се изброяват обстоятелствата, които министърът трябва да вземе предвид при приемането на наредби за определяне на сумите, дължими от различните организации. На второ място, 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.

([89]) 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 82).

([90]) Вж. член 134 от ЗЗД от 2018 г.

или при поискване, на Парламента, на правителството или на други институции и органи, и на обществеността по всички въпроси, свързани със защитата на личните данни. 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 (вж. съображения 99—103).

2.6.2. *Привеждане в изпълнение, включително санкции*

(92) Правомощията на комисаря по информацията са изброени в член 58 от ОРЗД на Обединеното кралство, с който не се въвеждат съществени промени в съответния член на Регламент (ЕС) 2016/679. В ЗЗД от 2018 г. са определени допълнителни правила за това как тези правомощия могат да бъдат упражнявани. По-специално комисарят има правомощия: а) 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“) ([91]); б) да провежда разследвания и одити, като издава ревизионно постановление, чрез което 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 и т.н. („ревизионно постановление“) ([92]); в) да получава по друг начин достъп до документите и др. 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“); г) 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, включително да разпореди на администратора или обработващия лични данни да извърши някое от действията по член 58, параграф 2, букви c)—g) и j) от ОРЗД на Обединеното кралство („изпълнително постановление“) ([93]); и д) да налага административни наказания „глоба“ или „имуществена санкция“ под формата на наказателно постановление („наказателно постановление“) ([94]). Последното може да бъде издадено и в случай че публичен орган не е спазил разпоредбите на ОРЗД на Обединеното кралство ([95]).

(93) В Политиката на ICO за регулаторните действия се определят обстоятелствата, при които тя издава информационно, ревизионно, изпълнително или наказателно постановление ([96]). С изпълнително постановление, издадено в отговор на неизпълнение от страна на администратора или обработващия лични данни, може да бъдат наложени само изисквания, които комисарят смята за подходящи с цел отстраняване на неизпълнението. Изпълнителни и наказателни постановления могат да бъдат издавани на администратор или обработващ лични данни във връзка с нарушения на глава II от ОРЗД на Обединеното кралство (принципи на обработване), членове 12—22 (права на субекта на данни), членове 25—39 (задължения на администраторите и на обработващите лични данни) и членове 44—49 (международно предаване на данни) от ОРЗД на Обединеното кралство. Изпълнително постановление може да бъде издадено също, когато администраторът не е спазил изискването за плащане на такса, предвидена в наредбите, изготвени съгласно член 137 от ЗЗД от 2018 г. Освен това изпълнително постановление може да бъде издадено на надзорен орган по член 41 или на доставчик на сертифициране, ако не са изпълнили задълженията си съгласно ОРЗД на Обединеното кралство. Наказателно постановление може да бъде връчено и на лице, което не е изпълнило информационно постановление, ревизионно постановление или изпълнително постановление.

(94) С наказателното постановление лицето се задължава да плати на комисаря по информацията посочена в постановлението сума. Когато преценява дали да издаде наказателно постановление на лице и когато определя размера на санкцията, комисарят по информацията трябва да вземе предвид обстоятелствата, изброени в член 83, параграфи 1 и 2 от ОРЗД на Обединеното кралство, които са идентични със съответните правила, предвидени в Регламент (ЕС) 2016/679 ([97]). Съгласно член 83, параграфи 4 и 5 максималният размер на административните наказания „глоба“ или „имуществена санкция“ за неизпълнение на задълженията, упоменати в тези разпоредби, е съответно 8 700 000 или 17 500 000 британски лири. В случай на предприятие комисарят по информацията може

([91]) Член 142 от ЗЗД от 2018 г. (при спазване на ограниченията по член 143 от ЗЗД от 2018 г.).

([92]) Член 146 от ЗЗД от 2018 г. (при спазване на ограниченията по член 147 от ЗЗД от 2018 г.).

([93]) Членове 149—151 от ЗЗД от 2018 г. (при спазване на ограниченията по член 152 от ЗЗД от 2018 г.).

([94]) Член 155 от ЗЗД от 2018 г. и член 83 от ОРЗД на Обединеното кралство.

([95]) Това следва от член 155, параграф 1 от ЗЗД от 2018 г., във връзка с член 149, параграфи 2 и 5 от Закона за защита на данните от 2018 г., и от член 156, параграф 4 от ЗЗД от 2018 г., с който издаването на наказателни постановления се ограничава само до комисарите по имотите и собствеността на Короната и администраторите за Кралския двор съгласно член 209, параграф 4 от ЗЗД от 2018 г.

([96]) Политика за регулаторните действия, достъпна на следния адрес: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

([97]) Включително естеството и тежестта на неизпълнението (като се вземат предвид естеството, обхвата или целта на съответното обработване, както и броят на засегнатите субекти на данни и нивото на вредите, които са претърпели), 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 техническите и организационните мерки, въведени от администратора или обработващия лични данни), евентуалните свързани предишни неизпълнения на администратора или обработващия лични данни; степента на сътрудничество с комисаря, категориите лични данни, засегнати от неизпълнението, всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението.

също така да налага санкции, изразяващи се в процент от годишния световен оборот, ако сумата е по-голяма. Както в равностойните разпоредби на Регламент (ЕС) 2016/679, размерът е определен на 2 % и на 4 % съответно в член 83, параграф 4 и параграф 5. При неизпълнение на информационно постановление, ревизионно постановление или изпълнително постановление максималният размер на санкцията, която може да бъде наложена с наказателно постановление, е по-голямата сума измежду 17 500 000 британски лири или в случай на предприятие — 4 % от годишния световен оборот.

(95) С ОРЗД на Обединеното кралство и със ЗЗД от 2018 г. са укрепени и други правомощия на комисаря по информацията. Например комисарят вече може да извършва задължителни одити по отношение на всички администратори и обработващи лични данни посредством ревизионни постановления, докато съгласно предишното законодателство — Закона за защита на данните от 1998 г. — той е имал това правомощие само по отношение на централни държавни органи и здравни институции, докато всички останали е трябвало да дадат съгласие, за да им бъде извършен одит.

(96) От въвеждането на Регламент (ЕС) 2016/679 насам комисарят по информацията годишно ([98]) разглежда около 40 000 жалби от субекти на данни и освен това извършва около 2 000 служебни разследвания ([99]). Повечето жалби са свързани с правото на достъп до данни и разкриване на данни. След разследванията си комисарят предприема мерки за изпълнение в широк кръг от сектори. По-конкретно, според последния годишен доклад на комисаря по информацията (2019—2020 г.) ([100]), комисарят е издал 54 информационни постановления, 8 ревизионни постановления, 7 изпълнителни постановления и 4 предупреждения, завел е 8 наказателни дела и е наложил 15 глоби или имуществени санкции през отчетния период ([101]).

(97) Това включва няколко значителни парични санкции, наложени съгласно Регламент (ЕС) 2016/679 и ЗЗД от 2018 г. По-специално през октомври 2020 г. комисарят по информацията глоби британска авиокомпания с 20 милиона британски лири за нарушение на сигурността на личните данни, засягащо над 400 000 клиенти. В края на октомври 2020 г. международна хотелска верига беше глобена с 18,4 милиона британски лири за това, че не е запазила сигурността на личните данни на милиони клиенти, а през ноември 2020 г. британски доставчик на услуги, продаващ билети за събития онлайн, беше глобен с 1,25 милиона британски лири за неспособността му да защити данните на клиентите, свързани с плащания ([102]).

(98) В допълнение към правомощията за привеждане в изпълнение на комисаря по информацията, описани в съображение 92, 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, съзнателно или поради небрежност, без съгласието на администратора, за предоставянето на друго лице на разкритите лични данни без съгласието на администратора ([103]), реидентифицирането на информация, която представлява деидентифицирани лични данни, без съгласието на администратора, отговарящ за деидентифицирането на личните данни ([104]), умишленото възпрепятстване на комисаря да упражнява правомощията си за проверката на лични данни в съответствие с международни задължения ([105]), представянето на неверни данни в отговор на информационно постановление или унищожаването на информация във връзка с информационни и ревизионни постановления ([106]).

([98]) Според информацията, предоставена от органите на Обединеното кралство, през периода, обхванат от Годишния доклад на комисаря по информация за 2019—2020 г., в около 25 % от случаите не е установено нарушение, в около 29 % от случаите субектът на данни е поканен да внесе жалба до администратора на данни за първи път, да изчака отговора на администратора или да продължи вече започнал диалог с администратора на данни, в около 17 % от случаите не е установено нарушение, но е издадено предписание на администратора на данни, в около 25 % от случаите комисарят по информацията е установил нарушение и е издал предписание на администратора на данни, или администраторът на данни е задължен да предприеме определени действия, в около 3 % от случаите е установено, че жалбата не е попада в приложното поле на Регламент (ЕС) 2016/679, и около 1 % от случаите са били пренасочени към друг орган за защита на личните данни в рамките на Европейския комитет по защита на данните.

([99]) Комисарят по информацията може да започва такива разследвания въз основа на информация, получена от различни източници, включително уведомления за нарушение на сигурността на личните данни, сезиране от други публични органи на Обединеното кралство или от чуждестранни органи за защита на личните данни и жалби от лица или организации на гражданското общество.

([100]) Годишен доклад и годишни финансови отчети на комисаря по информацията за 2019—2020 г. (вж. бележка под линия 81).

([101]) Според предходния годишен доклад, обхващащ периода 2018—2019 г., комисарят по информацията е издал 22 наказателни постановления съгласно ЗЗД от 1998 г. през отчетния период и е наложил глоби или имуществени санкции на обща стойност 3 010 610 британски лири, включително две глоби или имуществени санкции в размер на 500 000 британски лири (максималният разрешен размер съгласно ЗЗД от 1998 г.). През 2018 г. комисарят по информацията е провел по-специално разследване относно използването на анализ на данни за политически цели след разкритията, свързани с Cambridge Analytica. В резултат на разследването са изготвени доклад за политиката и набор от препоръки, наложена е санкция на Facebook в размер на 500 000 британски лири и е издадено изпълнително постановление на Aggregate IQ — канадски брокер на данни, с което на компанията се нарежда да заличи личните данни, които притежава за граждани и жители на Обединеното кралство (вж. Годишен доклад и годишни финансови отчети на комисаря по информацията за 2018—2019 г., достъпен на следния адрес: https://ico.org.uk/media/about-the-ico/documents/2615262/anniversary-report-201819.pdf).

([102]) За обобщение на предприетите изпълнителни действия, вж. уебсайта на комисаря по информацията, достъпен на следния адрес: https://ico.org.uk/action-weve-taken/enforcement/.

([103]) Член 170 от ЗЗД от 2018 г.

([104]) Член 171 от ЗЗД от 2018 г.

([105]) Член 119 от ЗЗД от 2018 г.

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

2.6.3. *Надзор на съдебната власт*

(99) 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 ICO. Когато администраторът действа в изпълнение на съдебните си функции, ICO не може да упражнява надзорните си функции ([107]) и надзорът се осъществява от специални органи. Това отразява подхода, възприет в Регламент (ЕС) 2016/679 (член 55, параграф 3).

(100) 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 ([108]). Освен това главният съдия (*Lord Chief Justice*) и първият председател (*Senior President*) на трибуналите са издали декларация за поверителност ([109]), в която се посочва как съдилищата в Англия и Уелс обработват лични данни при изпълнение на съдебни функции. Подобна декларация е издадена от северноирландската ([110]) и шотландската ([111]) съдебни власти.

(101) Освен това в Северна Ирландия главният съдия на Северна Ирландия назначи съдия от Висшия съд като съдия по надзора на данните (DSJ) ([112]). 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 ([113]).

(102) 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 ([114]).

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

2.6.4. *Средства за правна защита*

(104) 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.

([107]) Член 117 от ЗЗД от 2018 г.

([108]) 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.

([109]) 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

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

([111]) 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

([112]) 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.

([113]) 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.

([114]) 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).

(105) 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 ОРЗД на Обединеното кралство ([115]). В ОРЗД на Обединеното кралство правилата, предвидени в член 77 от Регламент (ЕС) 2016/679 относно това право, са запазени без съществени изменения. Същото се отнася и за член 57, параграф 1, буква f) и член 57, параграф 2, в който са определени задачите на комисаря във връзка с разглеждането на жалби. Както е описано в съображения 92 и 98 по-горе, комисарят по информацията има правомощието да преценява спазването от администратора и обработващия лични данни на ОРЗД на Обединеното кралство и 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.

(106) Второ, в ОРЗД на Обединеното кралство и ЗЗД от 2018 г. се предвижда право на средства за правна защита срещу комисаря по информацията. Съгласно член 78, параграф 1 от ОРЗД на Обединеното кралство всяко лице има право на ефективно средство за правна защита срещу правнообвързващо решение на комисаря, което го засяга. В контекста на съдебния контрол съдията разглежда решението, което се оспорва в исковата молба, и преценява дали комисарят по информацията е действал законосъобразно. Освен това, съгласно член 78, параграф 2 от ОРЗД на Обединеното кралство, ако комисарят не разгледа по подходящ начин жалба, внесена от субекта на данни ([116]), жалбоподателят има достъп до средства за правна защита. Той може да поиска от трибунала от първа инстанция да разпореди на комисаря да предприеме подходящи действия, за да отговори на жалбата, или да информира жалбоподателя за напредъка по жалбата ([117]). Освен това всяко лице, на което комисарят е връчил някое от посочените по-горе постановления (информационно, ревизионно, изпълнително или наказателно постановление), може да го обжалва пред трибунала от първа инстанция ([118]). 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.

(107) Трето, физическите лица могат да получат съдебна защита срещу администраторите и обработващите лични данни пряко пред съдилищата съгласно член 79 от ОРЗД на Обединеното кралство и 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.

(108) Освен това, съгласно член 82 от ОРЗД на Обединеното кралство и член 168 от ЗЗД от 2018 г., всяко лице, което е претърпяло имуществени или неимуществени вреди в резултат на нарушение на ОРЗД на Обединеното кралство, има право да получи обезщетение от администратора или от обработващия лични данни за претърпените вреди. Правилата относно обезщетението и отговорността, предвидени в член 82, параграфи 1—5 от ОРЗД на Обединеното кралство, са идентични със съответните правила в Регламент (ЕС) 2016/679. Съгласно член 168 от ЗЗД от 2018 г. неимуществените вреди включват и емоционално страдание. Съгласно член 80 от ОРЗД на Обединеното кралство субектът на данни има също така право да упълномощи представителен орган или организация да подаде жалбата до комисаря от негово име (съгласно член 77 от ОРЗД на Обединеното кралство) и да упражнява от негово име правата, посочени в член 78 (право на ефективно средство за правна защита срещу комисаря), член 79 (право на ефективно средство за правна защита срещу администратор или обработващ лични данни) и член 82 (право на обезщетение и отговорност) от ОРЗД на Обединеното кралство.

(109) Четвърто, и в допълнение към описаните по-горе възможности за правна защита, всяко лице, което смята, че неговите права, включително правото на неприкосновеност на личния живот и на защита на данните, са били нарушени от публичните органи, може да получи правна защита пред съдилищата на Обединеното кралство съгласно Закона за правата на човека от 1998 г. ([119]) 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.

(110) 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 ([120]). Съдът може също така да обяви разпоредба от първичното право за несъвместима с право по Конвенцията.

([115]) Член 77 от ОРЗД на Обединеното кралство.

([116]) 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.

([117]) Член 78, параграф 2 от ОРЗД на Обединеното кралство и член 166 от ЗЗД от 2018 г.

([118]) Член 78, параграф 1 от ОРЗД на Обединеното кралство и член 162 от ЗЗД от 2018 г.

([119]) Член 7, параграф 1 от Закона за правата на човека от 1998 г. Съгласно член 7, параграф 7 дадено лице е жертва на незаконосъобразно действие само ако би било жертва по смисъла на член 34 от Европейската конвенция за правата на човека, в случай че бъде образувано производство в Европейския съд по правата на човека по отношение на това действие.

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

(111) 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 Европейската конвенция за правата на човека.

3. ДОСТЪП И ИЗПОЛЗВАНЕ ОТ ПУБЛИЧНИ ОРГАНИ В ОБЕДИНЕНОТО КРАЛСТВО НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ

(112) Комисията също така направи оценка на правната уредба на Обединеното кралство за събиране и последващо използване на лични данни, предавани на стопански оператори в Обединеното кралство от публичните органи на Обединеното кралство в обществен интерес, по-специално за целите на наказателното правоприлагане и на националната сигурност (наричано по-долу „държавен достъп“). При оценката дали условията, при които държавният достъп до данни, предавани на Обединеното кралство съгласно настоящото решение, биха отговаряли на критерия за „равностойност по същество“ съгласно член 45, параграф 1 от Регламент (ЕС) 2016/679, както се тълкува от Съда на Европейския съюз в светлината на Хартата на основните права, Комисията взе предвид по-специално следните критерии.

(113) Първо, всяко ограничаване на упражняването на правото на защита на личните данни трябва да бъде предвидено в закон, а самото правно основание, позволяващо намеса в това право, трябва да определя обхвата на ограничението при упражняване на съответното право ([121]).

(114) Второ, за да удовлетвори изискването за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат само доколкото са строго необходими в едно демократично общество, за да се постигнат конкретни цели от общ интерес, равностойни на тези, признати от Съюза, законодателството на въпросната трета държава, позволяващо намесата, трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданите мерки и да налагат минимални изисквания, така че лицата, чиито данни са били предадени, да разполагат с достатъчно гаранции, позволяващи ефективна защита на техните лични данни срещу рискове от злоупотреби ([122]). Законодателството трябва в частност да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на такива данни ([123]), както и да предвиди над изпълнението на такива изисквания да се упражнява независим надзор ([124]).

(115) Трето, това законодателство трябва да бъде правнообвързващо съгласно националното право и тези правни изисквания трябва да бъдат не само задължителни за органите, но и противопоставими пред съдилищата на органите на въпросната трета държава ([125]). По-специално субектите на данни трябва да имат възможността да заведат дело пред независим и безпристрастен съд, за да получат достъп до отнасящи се до тях лични данни или да коригират или изтриват такива данни ([126]).

3.1. **Обща правна уредба**

(116) Тъй като представлява упражняване на власт от страна на публичен орган, държавният достъп в Обединеното кралство трябва да се осъществява при пълно спазване на закона. Обединеното кралство е ратифицирало Европейската конвенция за правата на човека (вж. съображение 9) и всички публични органи в Обединеното кралство са длъжни да действат в съответствие с нея ([127]). Член 8 от Конвенцията предвижда, че всяка намеса в неприкосновеността на личния живот трябва да бъде в съответствие със закона, в интерес на една от целите, посочени в член 8, параграф 2, и да е пропорционална с оглед на тази цел. Съгласно член 8 също така се изисква намесата да е „предвидима“, т.е. да има ясно и достъпно основание в закона и в него да се съдържат подходящи гаранции за предотвратяване на злоупотреби.

(117) Освен това в своята съдебна практика Европейският съд по правата на човека е уточнил, че всяка намеса в правото на неприкосновеност на личния живот и в правото на защита на личните данни следва да бъде обект на ефективна, независима и безпристрастна система за надзор, който трябва да бъде осигурен или от съдия, или от друг независим орган ([128]) (напр. административен орган или парламентарен орган).

([121]) Вж. решение по дело *Schrems II*, т. 174—175 и цитираната съдебна практика. По отношение на достъпа от страна на публични органи на държави членки вж. също решението по дело C-623/17 *Privacy International*, ECLI:EU:C:2020:790, т. 65; и решението по съединени дела C-511/18, C-512/18 и C-520/18 *La Quadrature du Net и др.*, ECLI:EU:C:2020:791, т. 175.

([122]) Вж. решение по дело *Schrems II*, т. 176 и 181, както и цитираната съдебна практика. По отношение на достъпа от страна на публични органи на държави членки вж. също решението по дело *Privacy International*, т. 68 и по дело *La Quadrature du Net и др.*, т. 132.

([123]) Вж. решение по дело *Schrems II*, т. 176. По отношение на достъпа от страна на публични органи на държави членки вж. също решението по дело *Privacy International*, т. 68 и по дело *La Quadrature du Net и др.*, т. 132.

([124]) Вж. решение по дело *Schrems II*, т. 179.

([125]) Вж. решение по дело *Schrems II*, т. 181—182.

([126]) Вж. решение по дело *Schrems I*, т. 95, и решение по дело *Schrems II*, т. 194. В това отношение Съдът на Европейския съюз специално подчертава, че спазването на член 47 от Хартата на основните права, гарантиращо правото на ефективно средство за правна защита пред независим и безпристрастен съд, „също е част от изискваното ниво на защита в Съюза [и] Комисията трябва да [го] констатира, преди да приеме решение относно адекватното ниво на защита съгласно член 45, параграф 1 от [Регламент (ЕС) 2016/679]“ (дело *Schrems II*, т. 186).

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

([128]) Европейски съд по правата на човека, *Klass и др./Германия*, жалба № 5029/71, т. 17—51.

(118) Освен това на лицата трябва да се осигури ефективна защита, а Европейският съд по правата на човека е пояснил, че тази защита трябва да се предлага от независим и безпристрастен орган, който е приел свой процедурен правилник и се състои от членове, които трябва да заемат или да са заемали висша съдебна длъжност, или да са опитни адвокати, както и че за подаването на жалба до този орган не трябва да се изисква представянето на доказателства. При разглеждането на жалби на лица независимият и безпристрастен орган следва да има достъп до цялата съответна информация, включително до поверителни материали. Накрая, той следва да има правомощията да отстрани несъответствието ([129]).

(119) Обединеното кралство също така ратифицира Конвенцията на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни (Конвенция № 108) и през 2018 г. подписа Протокола за изменение на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (известна като „Конвенция 108 +“) ([130]). В член 9 от Конвенция № 108 е предвидено, че дерогации от общите принципи за защита на данните (член 5 „Качество на данните“) и от правилата, уреждащи специалните категории данни (член 6 „Специални категории данни“) и правата на субекта на данни (член 8 „Допълнителни гаранции за субекта на данни“), са допустими само когато такава дерогация е предвидена в законодателството на страната по Конвенцията и представлява необходима мярка в едно демократично общество в интерес на защитата на държавната сигурност, обществената безопасност, паричните интереси на държавата или борбата с престъпленията, или за защита на субекта на данни или на правата и свободите на другите ([131]).

(120) Следователно чрез членството на Обединеното кралство в Съвета на Европа, спазването от него на Европейската конвенция за правата на човека и признаването на юрисдикцията на Европейския съд по правата на човека спрямо него се прилагат редица задължения, залегнали в международното право, които оформят неговата система за държавен достъп въз основа на принципи, гаранции и индивидуални права, подобни на тези, гарантирани от законодателството на ЕС и приложими за държавите членки. Следователно, както се подчертава в съображение 19, спазването на такива инструменти е особено важен елемент от оценката, на която се основава настоящото решение.

(121) Освен това специфичните гаранции и права за защита на личните данни са гарантирани от ЗЗД от 2018 г., когато данните се обработват от публични органи, включително от правоприлагащи органи и органи за национална сигурност.

(122) По-специално режимът за обработване на лични данни в контекста на наказателното правоприлагане е уреден в част 3 от ЗЗД от 2018 г., която е приета с цел транспониране на Директива (ЕС) 2016/680. Част 3 от ЗЗД от 2018 г. се прилага спрямо 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 ([132]).

(123) Понятието „компетентен орган“ е определено в член 30 от ЗЗД като лице, включено в приложение 7 към ЗЗД от 2018 г., както и всяко друго лице, доколкото лицето изпълнява законоустановени функции за целите на правоприлагането ([133]). Както е обяснено по-долу (вж. съображение 139), някои компетентни органи (например Националната агенция по престъпността) могат при определени условия да използват правомощията, предвидени в Закона за правомощията за разследване от 2016 г. (ЗПР от 2016 г.). В този случай гаранциите, предвидени в ЗПР от 2016 г., ще се прилагат в допълнение към предвидените в част 3 от ЗЗД от 2018 г. Разузнавателните служби (Службата за тайно разузнаване, Службата за сигурност и Правителствената централа за комуникации) не са „компетентни органи“ ([134]), попадащи в обхвата на част 3 от ЗЗД за 2018 г., и следователно предвидените там правила не се прилагат за никоя от техните дейности. Специална част от ЗЗД от 2018 г. (част 4) е посветена на обработването на лични данни от разузнавателните служби (за повече подробности вж. съображение 125).

([129]) Европейски съд по правата на човека, *Kennedy/Обединено кралство*, жалба № 26839/05 (решение *Kennedy*), т. 167 и 190.

([130]) За повече информация относно Европейската конвенция за правата на човека и нейното включване в правото на Обединеното кралство чрез Закона за правата на човека от 1998 г., както и относно Конвенция № 108, вж. съображение 9.

([131]) Също така съгласно член 11 от Конвенция № 108+ ограниченията на някои специфични права и задължения на Конвенцията за целите на националната сигурност или за предотвратяване, разследване и преследване на престъпления и изпълнение на наказания са допустими само когато такива ограничения са предвидени в закона, прилагат се при зачитане на същността на основните права и свободи и представляват необходима и пропорционална мярка в едно демократично общество. Дейностите по обработване на лични данни за целите на националната сигурност и отбрана също трябва да бъдат обект на независим и ефективен преглед и надзор съгласно националното законодателство на съответната страна по Конвенцията.

([132]) Член 31 от ЗЗД от 2018 г.

([133]) 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. комисаря на Кралската данъчна и митническа служба, Националната агенция по престъпността, органа по приходите на Уелс, Органа за защита на конкуренцията и пазарите или Кралския имотен регистър), органи за наказателно преследване, други органи за наказателно правосъдие и други субекти или организации, които извършват дейности по правоприлагане (сред тях в приложение 7 към ЗЗД от 2018 г. са изброени главният прокурор, главният прокурор за Северна Ирландия или комисарят по информацията).

([134]) Член 30, параграф 2 от ЗЗД от 2018 г.

(124) Както в Директива (ЕС) 2016/680, така и в част 3 от ЗЗД от 2018 г. са определени принципите на законосъобразност и добросъвестност ([135]), ограничение на целите ([136]), свеждане на данните до минимум ([137]), точност ([138]), ограничение на съхранението ([139]) и сигурност ([140]). Законодателството налага специфични задължения за прозрачност ([141]) и предоставя на лицата право на достъп ([142]), коригиране и заличаване ([143]) и правото спрямо тях да не се прилага автоматизирано вземане на решения ([144]). От компетентните органи се изисква също така да създават предпоставки за защита на данните на етапа на проектирането и по подразбиране, да водят регистри на дейностите по обработване и на някои операции по обработване, да извършват оценки на въздействието върху защитата на данните и да се консултират предварително с комисаря по информацията ([145]). Съгласно член 56 от ЗЗД от 2018 г. от тях се изисква да докажат съответствие. Освен това от тях се изисква да въведат подходящи мерки за гарантиране на сигурността на обработването ([146]) и да изпълняват специфични задължения в случай на нарушение на сигурността на личните данни, включително да уведомяват комисаря по информацията и субектите на данни за такива нарушения ([147]). Както в Директива (ЕС) 2016/680, предвидено е и изискване администраторът (освен ако не е съд или друг съдебен орган, който действа в изпълнение на съдебните си функции) да определи длъжностно лице по защита на данните ([148]), което да подпомага администратора при спазването на неговите задължения, както и да наблюдава изпълнението им ([149]). Освен това законодателството налага конкретни изисквания относно международното предаване на лични данни за целите на правоприлагането към трети държави или към международни организации, за да се осигури непрекъснатост на защитата ([150]). На датата на настоящото решение Комисията прие решение относно адекватното ниво на защита въз основа на член 36, параграф 3 от Директива (ЕС) 2016/680, в което заключава, че режимът за защита на данните, приложим по отношение на обработването на лични данни от органите за наказателно правоприлагане в Обединеното кралство, осигурява ниво на защита, което по същество е равностойно на гарантираното от Директива (ЕС) 2016/680.

(125) Част 4 от ЗЗД от 2018 г. се прилага за всяко обработване от разузнавателните служби или от тяхно име. По-специално в нея се определят основните принципи за защита на данните (законосъобразност, добросъвестност и прозрачност ([151]); ограничение на целите ([152]); свеждане на данните до минимум ([153]); точност ([154]); ограничение на съхранението ([155]) и сигурност ([156])), поставят се условия за обработването на специални категории данни ([157]), предоставят се права на субектите на данни ([158]),

([135]) Член 35 от ЗЗД от 2018 г.
([136]) Член 36 от ЗЗД от 2018 г.
([137]) Член 37 от ЗЗД от 2018 г.
([138]) Член 38 от ЗЗД от 2018 г.
([139]) Член 39 от ЗЗД от 2018 г.
([140]) Член 40 от ЗЗД от 2018 г.
([141]) Член 44 от ЗЗД от 2018 г.
([142]) Член 45 от ЗЗД от 2018 г.
([143]) Членове 46 и 47 от ЗЗД от 2018 г.
([144]) Членове 49 и 50 от ЗЗД от 2018 г.
([145]) Членове 56—65 от ЗЗД от 2018 г.
([146]) Член 66 от ЗЗД от 2018 г.
([147]) Членове 67—68 от ЗЗД от 2018 г.
([148]) Членове 69—71 от ЗЗД от 2018 г.
([149]) Членове 67—68 от ЗЗД от 2018 г.
([150]) Част 3, глава 5 от ЗЗД от 2018 г.
([151]) Съгласно член 86, параграф 6 от ЗЗД от 2018 г., за да се определят добросъвестността и прозрачността на обработването, трябва да се вземе предвид методът, по който са получени данните. В този смисъл изискването за добросъвестност и прозрачност е изпълнено, ако данните са получени от лице, което е законно оправомощено или е длъжно да ги предостави.
([152]) 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 от ЗЗД от 2018 г. 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.).
([153]) Личните данни трябва да бъдат подходящи, относими и да не надхвърлят необходимото (член 88 от ЗЗД от 2018 г.).
([154]) Личните данни трябва да бъдат точни и актуални (член 89 от ЗЗД от 2018 г.).
([155]) Личните данни не трябва да се съхраняват по-дълго от необходимото (член 90 от ЗЗД от 2018 г.).
([156]) 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.
([157]) Член 86, параграф 2, буква b) и приложение 10 от ЗЗД от 2018 г.
([158]) 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. Както е обяснено в насоките на ICO относно обработването от разузнавателните служби, физическите лица могат да упражняват всичките си права (включително искане за коригиране), като подадат жалба до ICO или отнесат въпроси в съда (вж. Ръководството на ICO за обработка на разузнавателните служби, достъпно на следния линкhttps://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

изисква се защита на данните на етапа на проектирането ([159]) и се урежда международното предаване на лични данни ([160]). Неотдавна комисарят по информацията издаде подробни насоки относно обработването от разузнавателните служби съгласно част 4 от ЗЗД от 2018 г. ([161]).

(126) 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. ([162]), когато такова освобождаване е необходимо за гарантиране на националната сигурност. Това освобождаване може да се използва въз основа на анализа на всеки отделен случай ([163]). Както е обяснено от органите на Обединеното кралство и потвърдено от съдебната практика, „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“ ([164]). Дали освобождаването е било използвано по подходящ начин, подлежи на надзор от страна на ICO ([165]).

(127) Освен това, във връзка с възможността за ограничаване на прилагането на горепосочените определени разпоредби с цел защита на „националната сигурност“, съгласно член 111 от ЗЗД от 2018 г. администраторът може да подаде заявление за удостоверение, подписано от министър или от главния прокурор, удостоверяващо, че ограничаването на тези права представлява необходима и пропорционална мярка за защита на националната сигурност ([166]).

(128) Правителството на Обединеното кралство издаде насоки с цел подпомагане на администраторите при вземането на решение дали да подадат заявление за удостоверение 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 ([167]). Всички удостоверения за национална сигурност трябва да бъдат публикувани на уебсайта на комисаря по информацията ([168]).

([159]) Член 103 от ЗЗД от 2018 г.

([160]) 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.

([161]) Насоки на комисаря по информацията, вж. бележка под линия 158.
Член 30 от ЗЗД от 2018 г. и приложение 7 към ЗЗД от 2018 г.

([162]) 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.

([163]) Вж. *Baker/Secretary of State*, вж. бележка под линия 61.

([164]) Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална рамка за защита на данните и правомощията за разследване, стр. 15—16 (вж. бележка под линия 31). Вж. също решение по дело *Baker/Secretary of State* (вж. бележка под линия 61), в което съдът 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.

([165]) 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 адрес: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf.

([166]) Със ЗЗД от 2018 г. беше отменена възможността за издаване на удостоверения съгласно член 28, параграф 2 от Закона за защита на данните от 1998 г. Въпреки това все още съществува възможност за издаване на „стари удостоверения“ дотолкова, доколкото се оспорва минало прилагане на 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, като например случаите, при които субектът на данни оспорва използването на изключението във връзка с националната сигурност по отношение на обработване от страна на 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 в своята цялост, което следователно включва възможността субектът на данни да оспори удостоверението пред Съда.

([167]) 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. Според разясненията, предоставени от органите на Обединеното кралство, макар удостоверението да е убедително доказателство, че изключението е приложимо по отношение на описаните в него данни или дейности по обработване, то не освобождава администратора от изискването да преценява във всеки отделен случай дали прилагането на изключението е необходимо.

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

(129) Удостоверението следва да бъде за определен срок, не по-дълъг от пет години, така че да бъде редовно преразглеждано от орган на изпълнителната власт ([169]). 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 ([170]).

(130) Важно е да се отбележи, че с удостоверенията за национална сигурност не се предвижда допълнително основание за ограничаване на правата на 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 изключението във връзка с националната сигурност, като то трябва да се прилага, както беше обяснено по-горе, въз основа на анализа на всеки отделен случай ([171]). 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 изключението във връзка с националната сигурност ([172]).

(131) Всяко лице, пряко засегнато от издаването на удостоверението, може да обжалва решението за издаване на удостоверението ([173]) пред трибунала от по-горна инстанция ([174]) или, когато удостоверението идентифицира данни чрез общо описание, да оспори прилагането на удостоверението по отношение на конкретни данни ([175]). Трибуналът ще преразгледа решението за издаване на удостоверение и ще реши дали са били налице основателни причини за издаването му ([176]). 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 ([177]).

(132) 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. ([178]) 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 ([179]). 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“) ([180]). Позоваване на освобождаването на база накърняване може да се прави само дотолкова, доколкото прилагането на въпросната разпоредба за защита на данните би могло

([169]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност, точка 15, вж. бележка под линия 167.

([170]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност, точка 5, вж. бележка под линия 167.

([171]) Вж. бележка под линия 164.

([172]) В член 102 от ЗЗД от 2018 г. се 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: е достъпен на следния адрес: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

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

([174]) 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.

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

([176]) По дело *Baker/Secretary of State* (вж. по-горе бележка под линия 61), Съдът по въпросите на информацията 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.

([177]) Насоки на правителството на Обединеното кралство относно удостоверенията за национална сигурност, точка 25, вж. бележка под линия 167.

([178]) 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.

([179]) В част 4 от ЗЗД от 2018 г. е предвидена правната уредба, която се прилага за всички видове обработване на лични данни, извършвано от разузнавателните служби (а не само за изпълнението на техните задачи, свързани с националната сигурност). Поради това част 4 се прилага и когато разузнавателните служби обработват данни например за целите на управлението на човешките ресурси, в контекста на съдебни спорове или на обществени поръчки. Ограниченията, изброени в приложение 11, са предвидени да се прилагат основно в този друг контекст. Например в контекста на съдебен спор със служител може да се направи позоваване на ограничението за целите на „съдебното производство“ или в контекста на обществените поръчки може да се направи позоваване на ограничението за целите на „преговорите“ и т.н. Това е отразено в насоките на ICO относно обработването от разузнавателните служби, в които преговорите по спогодба между разузнавателна служба и бивш служител, който предявява иск по трудово правоотношение, са посочени като пример за прилагането на ограниченията по приложение 11 (вж. бележка под линия 161). Следва да се отбележи още, че съгласно част 2 от приложение 2 към ЗЗД от 2018 г. същите ограничения могат да се използват и от други публични органи.

([180]) Съгласно Обяснителната рамка на Обединеното кралство освобождаванията 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 31.

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 освобождаванията 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.

(133) 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.

3.2. **Достъп и използване от публични органи на Обединеното кралство за целите на наказателното правоприлагане**

(134) Законодателството на Обединеното кралство налага редица ограничения на достъпа и използването на лични данни за целите на наказателното правоприлагане и осигурява механизми за надзор и правна защита в тази област, които са в съответствие с изискванията, посочени в съображения 113—115 от настоящото решение. Условията, при които може да се осъществи такъв достъп, и гаранциите, приложими за упражняването на тези правомощия, са подробно разгледани в следващите раздели.

3.2.1. *Правни основания и приложими ограничения/гаранции*

(135) В съответствие с принципа на законосъобразност, гарантиран по член 35 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 ([181]), или обработването е необходимо за изпълнението на задача, осъществявана за тази цел от компетентен орган.

3.2.1.1. Заповеди за претърсване и заповеди за предоставяне

(136) В правната уредба на Обединеното кралство събирането на лични данни от стопански оператори, включително такива, които биха обработвали данни, предадени от ЕС съгласно настоящото решение относно адекватното ниво на защита, за целите на наказателното правоприлагане, е допустимо въз основа на заповеди за претърсване ([182]) и заповеди за предоставяне ([183]).

(137) Заповедите за претърсване се издават от съд, обикновено по молба на разследващия служител. Те дават право на служителя да влезе в определени помещения, за да търси материали или лица, свързани с провежданото от него разследване, и да задържи всичко, за което е разрешено претърсването, включително всички относими документи или материали, съдържащи лични данни ([184]). Заповедта за предоставяне, която също трябва да бъде издадена от съд, задължава лицето, посочено в нея, да предостави или да осигури достъп до материалите, които притежава или контролира. Молителят трябва да обоснове пред съда защо е необходима заповедта за претърсване или за предоставяне, както и защо това е в обществен интерес. Има няколко

([181]) Получаването на съгласие не изглежда релевантно, когато става дума за гарантиране на адекватно ниво на защита, тъй като при предаването данните няма да бъдат събрани директно от правоприлагащия орган на Обединеното кралство от субект на данни от ЕС въз основа на съгласие.

([182]) За съответното правно основание вж. член 8 и сл. от Закона за полицията и доказателствата в наказателния процес от 1984 г. (за Англия и Уелс), член 10 и сл. от Наредбата за полицията и доказателствата в наказателния процес (Северна Ирландия) от 1989 г. и разпоредбите на общото право за Шотландия (вж. член 46 от Закона за наказателното правосъдие (Шотландия) от 2016 г. и член 23B от Наказателния закон (консолидиран) (Шотландия). За заповед за претърсване, издадена след задържане, правното основание е член 18 от Закона за полицията и доказателствата в наказателния процес от 1984 г. (за Англия и Уелс), член 20 и сл. от Наредбата за полицията и доказателствата в наказателния процес (Северна Ирландия) от 1989 г. и разпоредбите на общото право за Шотландия (вж. член 46 от Закона за наказателното правосъдие (Шотландия) от 2016 г.). Органите на Обединеното кралство поясниха, че заповедите за претърсване се издават от съд по молба на разследващия служител. Те дават право на служителя да влезе в определени помещения, за да търси материали или лица, свързани с провежданото от него разследване; за изпълнението на заповедта често е необходимо съдействието на полицейски служител.

([183]) Когато разследването се отнася за изпиране на пари (включително процедури за конфискация и граждански искове за възстановяване), съответното правно основание за подаване на молба за заповед за предоставяне е член 345 и сл. за Англия, Уелс и Северна Ирландия и член 380 и сл. от Закона за приходите от престъпна дейност от 2002 г. за Шотландия. Когато разследването се отнася за други въпроси, различни от изпирането на пари, молба за заповед за предоставяне може да бъде подадена съгласно член 9 от Закона за полицията и доказателствата в наказателния процес от 1984 г. и приложение 1 към него — за Англия и Уелс, и член 10 и сл. от Наредбата за полицията и доказателствата в наказателния процес (Северна Ирландия) от 1989 г. — за Северна Ирландия. За Шотландия правното основание се съдържа в разпоредбите на общото право (вж. член 46 от Закона за наказателното правосъдие (Шотландия) от 2016 г. и член 23B от Наказателния закон (консолидиран) (Шотландия). Органите на Обединеното кралство поясниха, че заповедта за предоставяне задължава лицето, посочено в нея, да предостави или да осигури достъп до материалите, които притежава или контролира (вж. точка 4 от приложение 1 към Закона за полицията и доказателствата в наказателния процес от 1984 г.).

([184]) Например в членове 8 и 18 от Закона за полицията и доказателствата в наказателния процес от 1984 г. са предвидени правомощия за изземване и задържане на всичко, за което е разрешено претърсването.

законоустановени правомощия, които позволяват издаването на заповеди за претърсване и заповеди за предоставяне. Всяка разпоредба съдържа определен набор от законоустановени условия, които трябва да бъдат изпълнени, за да бъде издадена заповед за претърсване ([185]) или заповед за предоставяне ([186]).

(138) Заповедите за претърсване и заповедите за предоставяне могат да бъдат обжалвани по линия на съдебния контрол ([187]). По отношение на гаранциите всички органи за наказателно правоприлагане, попадащи в обхвата на част 3 от ЗЗД от 2018 г., могат да имат достъп до лични данни — което представлява форма на

([185]) В членове 8 и 18 от Закона за полицията и доказателствата в наказателния процес са уредени съответно правомощията на мировите съдии да издават заповеди за претърсване и на полицейските служители да претърсват помещения. В първия случай (член 8), преди да издаде заповед за претърсване, мировият съдия трябва първо да се убеди, че са налице основателни причини да се предполага, че: i) е извършено престъпление от общ характер; ii) в помещенията има материали, които е вероятно да са от съществено значение (сами по себе си или заедно с други материали) за разследването на престъплението; iii) материалите е вероятно да представляват релевантно доказателство; iv) материалите не представляват, нито включват елементи, обект на адвокатска тайна, изключени материали или материали, подлежащи на специален режим; и v) не би било възможно да се получи достъп до помещенията без използването на заповед за претърсване. Във втория случай член 18 дава възможност полицейски служител да извърши претърсване в помещенията на лице, задържано за престъпление от общ характер, във връзка с материали, които не са обект на адвокатска тайна, ако има основателни причини да подозира, че в помещенията съществуват доказателства, свързани с това или с друго подобно или свързано престъпление от общ характер. Претърсването трябва да бъде ограничено до разкриването на такива материали и трябва да бъде разрешено писмено от полицейски служител най-малко с ранг инспектор, освен ако не е необходимо за разследването на престъплението. В такъв случай служител най-малко с ранг инспектор трябва да бъде информиран възможно най-скоро след извършването на претърсването. Основанията за претърсването и естеството на търсените доказателства трябва да бъдат документирани. Освен това в членове 15 и 16 от Закона за полицията и доказателствата в наказателния процес от 1984 г. са предвидени законоустановени гаранции, които трябва да се спазват при внасянето на молби за заповед за претърсване. В член 15 са посочени изискванията, приложими за издаването на заповед за претърсване (включително съдържанието на молбата, внасяна от полицейския служител, и фактът, че в заповедта трябва да бъде упоменат, наред с другото, актът, въз основа на който е издадена, и да бъдат посочени конкретно, доколкото е възможно, вещите и лицата, които ще се търсят, и помещенията, които ще бъдат претърсвани). Член 16 урежда как трябва да бъде извършено претърсването съгласно заповед за претърсване (напр.: в член 16, параграф 5 се предвижда, че служителят, изпълняващ заповедта за претърсване, представя на обитателя копие от заповедта; съгласно член 16, параграф 11 се изисква, след като бъде изпълнена, заповедта да се съхранява за период от 12 месеца; член 16, параграф 12 дава право на обитателя да прегледа заповедта през този период, ако желае). Тези разпоредби спомагат да се гарантира спазването на член 8 от ЕКПЧ (вж. напр. *Kent Pharmaceuticals/Director of the Serious Fraud Office* [2002] EWHC 3023 (QB), т. 30, главен съдия лорд Woolf). Неспазването на тези гаранции може да доведе до обявяването на претърсването за незаконно (вж. напр. *R (Brook)/Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95; *R (Superior Import / Export Ltd)/Revenue and Customs Commissioners* [2017] EWHC 3172 (Admin), [2018] Lloyd's Rep FC 115; и *R (F)/Blackfriars Crown Court* [2014] EWHC 1541 (Admin). Членове 15 и 16 от Закона за полицията и доказателствата в наказателния процес от 1984 г. са допълнени с Кодекс В към Закона — кодекс за поведение, който урежда упражняването на полицейските правомощия за извършване на претърсване на помещения.

([186]) Например, когато се издава заповед за предоставяне съгласно Закона за приходите от престъпна дейност от 2002 г., освен изискването да са налице основателни причини за изпълнение на условията, определени в член 346, параграф 2 от Закона за приходите от престъпна дейност, трябва да има основателни причини да се предполага, че лицето притежава или контролира посочените материали и че те вероятно са от съществено значение. Освен това друго изискване за издаване на заповед за предоставяне е, че трябва да има основателни причини да се предполага, че предоставянето на материалите или осигуряването на достъп до тях е в обществен интерес, като се вземе предвид а) ползата, която е вероятно придобиването на материалите да донесе за разследването; и б) обстоятелствата, при които лицето, посочено в молбата, за което се предполага, че притежава или контролира материалите, разполага с тях. Съдът, който разглежда молба за издаване на заповед за предоставяне съгласно приложение 1 към Закона за полицията и доказателствата в наказателния процес от 1984 г., също трябва да се увери, че са изпълнени конкретни условия. По-специално в приложение 1 към Закона за полицията и доказателствата в наказателния процес са определени два отделни алтернативни набора от условия, единият от които трябва да бъде изпълнен, за да може съдията да издаде заповед за предоставяне. Съгласно първия набор от условия съдията трябва да има основателни причини да предполага, че i) е извършено престъпление от общ характер; ii) материалите, търсени в помещенията, представляват или включват материали, подлежащи на специален режим, но не и изключени материали; iii) материалите е вероятно да са от съществено значение, сами по себе си или заедно с други материали, за разследването; iv) материалите е вероятно да представляват релевантно доказателство; v) направен е опит материалите да бъдат придобити с други методи или не е правен такъв опит, тъй като той би бил обречен на неуспех; и vi) като се има предвид ползата за разследването и обстоятелствата, при които лицето притежава материалите, е в обществен интерес те да бъдат предоставени или да бъде осигурен достъп до тях. Съгласно втория набор от условия: i) в помещенията трябва да се съхраняват материали, които представляват материали, подлежащи на специален режим, или изключени материали; ii) ако съгласно законодателството, прието преди Закона за полицията и доказателствата в наказателния процес, не е съществувала забрана за извършване на претърсване по отношение на материали, подлежащи на специален режим, би могло да бъде издадена заповед за претърсване по отношение на тези материали; и iii) издаването на такава заповед би било уместно.

([187]) Правната процедура за обжалване на решения на публичен орган пред Висшия съд е съдебният контрол. Съдилищата разглеждат обжалваното решение и решават дали има основание да се твърди, че решението е неправилно от правна гледна точка, като се вземат предвид публичноправните концепции/принципи. Главните основания за съдебен контрол включват по-специално незаконосъобразност, необоснованост, процесуални нередности, пренебрегване на принципа на оправданите правни очаквания и нарушаване на правата на човека. След успешно обжалване по линия на съдебния контрол съдът може да разпореди редица различни средства за правна защита; най-често срещаното от тях е определение за отмяна (с което първоначалното решение — т.е. решението за издаване на заповед за претърсване — се отменя); при някои обстоятелства това може да включва и присъждане на финансово обезщетение. Допълнителни подробности относно съдебния контрол в Обединеното кралство могат да бъдат намерени в изданието на Правния отдел на правителството „Под зоркото око на съдията — ръководство за добро вземане на решения“ (Judge Over Your Shoulder — a guide to good decision-making), достъпно на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf.

обработване — само при спазване на принципите и изискванията, посочени в ЗЗД от 2018 г. (вж. съображения 122 и 124 по-горе). Следователно всяка молба, отправена от правоприлагащ орган, трябва да е в съответствие с принципа, съгласно който целите на обработването трябва да бъдат конкретни, изрично указани и легитимни ([188]), а личните данни, обработвани от компетентен орган, трябва да имат отношение към тези цели и да не надхвърлят необходимото във връзка с тези цели ([189]).

3.2.1.2. Правомощия за разследване за целите на правоприлагането

(139) За целите на предотвратяването или разкриването на тежки престъпления ([190]) някои правоприлагащи органи, например Националната агенция по престъпността или началникът на полицията ([191]), може да се ползват с целеви правомощия за разследване съгласно ЗПР от 2016 г. В този случай гаранциите, предвидени в ЗПР от 2016 г., ще се прилагат в допълнение към предвидените в част 3 от ЗЗД от 2018 г. Конкретните правомощия за разследване, на които тези правоприлагащи органи могат да разчитат, са: правомощия за целево прихващане на данни (част 2 от ЗПР от 2016 г.), събиране на комуникационни данни (част 3 от ЗПР от 2016 г.), съхраняване на комуникационни данни (част 4 от ЗПР от 2016 г.) и целева намеса в оборудването (част 5 от ЗПР от 2016 г.). Прихващането обхваща придобиването на достъп до съдържанието на комуникация ([192]), докато получаването и съхраняването на комуникационни данни не е насочено към придобиване на съдържанието на комуникацията, а към това кой, кога, къде и как я е осъществил. Това включва например времето и продължителността на комуникацията, телефонния номер или адреса на електронната поща на изпращача и получателя на комуникацията, а понякога и местоположението на устройствата, от които е осъществена комуникацията, абоната на телефонната услуга или подробна фактура ([193]). Намесата в оборудването се състои от набор от техники, използвани за получаване на разнообразни данни от оборудването, което включва компютри, таблети и смартфони, както и кабели, проводници и устройства за съхранение ([194]).

(140) Правомощията за целево прихващане може също да се упражняват, когато „е необходимо с цел прилагане на разпоредбите на инструмент на ЕС за взаимопомощ или на международно споразумение за взаимопомощ“ (така наречената „заповед за взаимопомощ“ ([195])). Заповеди за взаимопомощ се издават само във връзка с прихващане, а не със събиране на комуникационни данни или намеса в оборудването. Тези целеви правомощия са уредени в Закона за правомощията за разследване от 2016 г. (ЗПР от 2016 г.) ([196]), който, заедно със Закона за уреждане на правомощията за разследване от 2000 г. (ЗУПР) за Англия, Уелс и Северна Ирландия и Закона за уреждане на правомощията за разследване (Шотландия) от 2000 г. (ЗУПРШ) за Шотландия, дава правното основание и определя ограниченията и гаранциите за упражняването на тези правомощия. В ЗПР от 2016 г. е предвиден също така режим на упражняване на правомощия за разследване по отношение на масово събирани данни, който обаче не може да се ползва от правоприлагащите органи (а само от разузнавателните служби) ([197]).

([188]) Член 36, параграф 1 от ЗЗД на Обединеното кралство от 2018 г.

([189]) Член 37 от ЗЗД на Обединеното кралство от 2018 г.

([190]) Съгласно член 263, параграф 1 от ЗПР от 2016 г. „тежко престъпление“ означава престъпление, за което пълнолетно, неосъждано лице може основателно да се очаква, че ще бъде осъдено на лишаване от свобода за срок от 3 години или повече, или деянието е извършено с насилие, води до значителна финансова изгода или е извършено от голям брой лица. Освен това за целите на събирането на комуникационни данни съгласно част 4 от ЗПР от 2016 г. в член 87, параграф 10В е предвидено, че „тежко престъпление“ е престъпление, за което може да бъде наложено наказание лишаване от свобода от 12 месеца или повече, или престъпление, чийто извършител не е физическо лице, или престъпление, неразделна част от което е изпращането на комуникация или нарушаването на неприкосновеността на личния живот на дадено лице.

([191]) По-специално, заповед за целево прихващане може да се иска от следните правоприлагащи органи: генералния директор на Националната агенция по престъпността, комисаря на Метрополната полиция, началника на полицейската служба на Северна Ирландия, началника на полицейската служба на Шотландия, комисаря на Кралската данъчна и митническа служба, директора на Военното разузнаване и лице, което е компетентен орган на държава или територия извън Обединеното кралство за целите на инструмент на ЕС за взаимопомощ или на международно споразумение за взаимопомощ (член 18, параграф 1 от ЗПР от 2016 г.).

([192]) Вж. член 4 от ЗПР от 2016 г.

([193]) Вж. член 261, параграф 5 от ЗПР от 2016 г. и Кодекса за поведение относно масовото събиране на комуникационни данни, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, точка 2.9.

([194]) Кодекс за поведение относно намесата в оборудването, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, точка 2.2.

([195]) Със заповедта за взаимопомощ орган на Обединеното кралство се оправомощава да съдейства на орган извън територията на Обединеното кралство за прихващане и разкриване на прихванатите материали на този орган в съответствие с международен инструмент за взаимопомощ (член 15, параграф 4 от ЗПР от 2016 г.).

([196]) Законът за правомощията за разследване от 2016 г. (вж.: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) замени различни закони относно прихващането на комуникация, намесата в оборудването и събирането на комуникационни данни, по-специално част I от ЗУПР от 2000 г., в която се съдържаше предишната обща нормативна уредба за упражняването на правомощия за разследване от органите на реда и националната сигурност.

([197]) Член 138, параграф 1, член 158, параграф 1, член 178, параграф 1, член 199, параграф 1 от ЗПР от 2016 г.

(141) За да упражнят тези правомощия, органите трябва да получат заповед ([198]), издадена от компетентен орган ([199]) и одобрена от независим съдебен комисар ([200]) (по така наречената „процедура с двойна защита“). Получаването на такава заповед подлежи на проверка на необходимостта и пропорционалността ([201]). Тъй като целевите правомощия за разследване, предоставени съгласно ЗПР от 2016 г., са същите като тези, с които службите за национална сигурност разполагат, условията, ограниченията и гаранциите, приложими за такива правомощия, са разгледани подробно в раздела относно достъпа и използването на лични данни от публичните органи на Обединеното кралство за целите на националната сигурност (вж. съображение 177 и сл.).

3.2.2. *По-нататъшно използване на събраната информация*

(142) Споделянето на данни от правоприлагащ орган с друг орган за цели, различни от тези, за които те са били първоначално събрани (т.нар. „последващо споделяне“), се извършва при определени условия.

(143) 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 за тази цел ([202]). В този случай всички гаранции, предвидени в част 3 от ЗЗД от 2018 г., посочени в съображения 122 и 124, се прилагат за обработването, извършвано от получаващия орган.

(144) В правния ред на Обединеното кралство различни закони изрично позволяват такова 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 публични органи ([203]) или в случай на дълг към публичен орган или към Короната ([204]); ii) Законът за престъпленията и съдилищата от 2013 г., който позволява споделянето на информация с Националната агенция по престъпността (NCA) ([205]) с цел борба, разследване и наказателно преследване на тежката и организираната престъпност; iii) Законът за тежките престъпления от 2007 г., който позволява на публичните органи да разкриват информация на организации за борба с измамите с цел предотвратяване на измами ([206]).

(145) В тези закони изрично се предвижда, че споделянето на информация следва да става в съответствие с принципи, предвидени в ЗЗД от 2018 г. Освен това Полицейският колеж издаде Разрешена професионална практика относно споделянето на информация ([207]), за да помогне на полицията да изпълнява задълженията си за защита

([198]) В част 2, глава 2 от ЗПР от 2016 г. са предвидени ограничен брой случаи, при които прихващането може да се извършва без заповед. Това включва: прихващане със съгласието на подателя или получателя, прихващане за административни цели или за целите на принудителното изпълнение, прихващане, извършвано в определени институции (затвори, психиатрични болници и места за задържане на имигранти), както и прихващане, извършвано в съответствие с приложимо международно споразумение.

([199]) В повечето случаи органът, който издава заповедите съгласно ЗПР от 2016 г., е министърът (*Secretary of State*) на Обединеното кралство, а шотландските министри са оправомощени да издават заповеди за целево прихващане, заповеди за взаимопомощ и заповеди за целеви намеса в оборудването, когато лицата или помещенията, за които се отнася прихващането, и оборудването, в което се осъществява намесата, се намират в Шотландия (вж. членове 22 и 103 от ЗПР от 2016 г.). В случай на целева намеса в оборудването заповедта може да бъде издадена от ръководител на правоприлагащ орган (упоменат в част 1 и част 2 от приложение 6 към ЗПР от 2016 г.) при спазване на условията, предвидени в член 106 от ЗПР от 2016 г.

([200]) Съдебните комисари подпомагат комисаря по правомощията за разследване — независим орган, който упражнява надзорни функции над упражняването на правомощия за разследване от разузнавателните служби (за повече подробности вж. съображение 162 и сл.).

([201]) Вж. по-специално членове 19 и 23 от ЗПР от 2016 г.

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

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

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

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

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

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

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 ([208]).

(146) 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 ([209]).

(147) 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 служба (като например финансов или данъчен орган, орган за защита на конкуренцията, служба за закрила на младежта и др.); и 2) когато правоприлагащ орган в областта на наказателното право споделя данни с разузнавателна служба. 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. В съображения 12—111 Комисията оцени гаранциите, предвидени в ОРЗД на Обединеното кралство и в част 2 от ЗЗД от 2018 г., и стигна до заключението, че Обединеното кралство осигурява адекватно ниво на защита на личните данни, предавани в обхвата на Регламент (ЕС) 2016/679 от Европейския съюз на Обединеното кралство.

(148) Във втория случай, по отношение на споделянето на данни, събрани от правоприлагащ орган в областта на наказателното право, с разузнавателна служба за целите на националната сигурност, правното основание, което разрешава такова споделяне, е член 19 от Закона за борба с тероризма от 2008 г. (ЗБТ от 2008 г.) ([210]). Съгласно този закон всяко лице може да предоставя информация на всяка от разузнавателните служби с цел изпълнение на някоя от функциите на тази служба, включително „националната сигурност“.

(149) Що се отнася до условията, при които данните могат да бъдат споделяни за целите на националната сигурност, Законът за разузнавателните служби ([211]) и Законът за службите за сигурност ([212]) ограничават възможността на разузнавателните служби да получават данни до това, което е необходимо за изпълнение на техните законоустановени функции. Правоприлагащите органи, 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 ([213]). В член 20 от ЗБТ от 2008 г. се пояснява, че всяко споделяне на данни съгласно член 19 трябва да продължава да е в съответствие със законодателството за защита на данните. Това означава, че се прилагат всички ограничения и изисквания на част 3 от ЗЗД от 2018 г. Освен това, тъй като компетентните органи са публични органи за целите на Закона за правата на човека от 1998 г., те трябва да гарантират, че действат в съответствие с правата по Конвенцията, включително член 8 от ЕКПЧ. Тези ограничения гарантират, че всяко споделяне на данни между правоприлагащите органи и разузнавателните служби е в съответствие със законодателството за защита на данните и ЕКПЧ.

([208]) Вж. напр. дело *M, R/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 схеми 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 във връзка с 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.

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

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

([211]) Закон за разузнавателните служби от 1994 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1994/13/contents.

([212]) Закон за службите за сигурност от 1989 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/1989/5/contents.

([213]) В член 2, параграф 2 от Закона за разузнавателните служби от 1994 г. 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. 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“.

(150) Когато компетентен орган възнамерява да споделя лични данни, обработвани съгласно част 3 от ЗЗД от 2018 г., с правоприлагащи органи на трета държава, се прилагат специфични изисквания ([214]). По-специално предаването на такива данни може да се извършва въз основа на наредби относно адекватното ниво на защита, издадени от министъра, или, при липса на такива наредби, след осигуряването на подходящи гаранции. Съгласно член 75 от ЗЗД от 2018 г. подходящи гаранции са налице, когато са установени по силата на правен инструмент с обвързваща сила за предвидения получател или когато администраторът, след като е оценил всички обстоятелства, свързани с предаването на този тип лични данни на трета държава или на международна организация, е стигнал до заключението, че съществуват подходящи гаранции за защита на данните.

(151) Ако предаването не се основава на наредба относно адекватното ниво на защита или на подходящи гаранции, то може да се осъществи само при определени специфични обстоятелства, наричани „особени обстоятелства“ ([215]). 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 държава членка или 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). 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. Този набор от обстоятелства съответства на специфичните ситуации и условия, които се определят като „дерогации“ съгласно член 38 от Директива (ЕС) 2016/680.

(152) Освен това, когато материалите, получени от правоприлагащите органи въз основа на заповед, с която се разрешава прихващане или намеса в оборудването, се предават на трета държава, в ЗПР от 2016 г. са предвидени допълнителни гаранции. По-специално разкриването на такива данни, определено като „разкриване в чужбина“, е разрешено само ако издаващият орган счита, че са налице конкретни подходящи механизми, които ограничават броя на лицата, на които се разкриват данните, обема, в който материалите се разкриват или предоставят на разположение, както и степента, до която се копират, и броя на направените копия. Освен това издаващият орган може да прецени, че са необходими подходящи механизми, за да се гарантира, че всяко копие, направено от която и да е част от тези материали, се унищожава незабавно, след като вече не са налице подходящи основания за съхраняването му (ако не е унищожено по-рано) ([216]).

(153) И накрая, специфични форми на последващо предаване на данни от Обединеното кралство към Съединените щати биха могли да се осъществяват в бъдеще въз основа на Споразумението между правителството на Обединеното кралство Великобритания и Северна Ирландия и правителството на Съединените американски щати относно достъпа до електрони данни с цел противодействие на тежката престъпност („Споразумението между Обединеното кралство и САЩ“ или „Споразумението“) ([217]), сключено през октомври 2019 г. ([218]) Въпреки че Споразумението между Обединеното кралство и САЩ все още не е влязло в сила към момента на приемане на настоящото решение, очакваното му влизане в сила може да повлияе на последващото предаване към САЩ на данни, предадени най-напред на Обединеното кралство въз основа на настоящото решение. По-конкретно данните, предадени от ЕС на доставчици на услуги в Обединеното кралство, могат да бъдат обект на заповеди за предоставяне на електронни доказателства, издадени от компетентните правоприлагащи органи на САЩ, и приложими в Обединеното кралство по силата на Споразумението след влизането му в сила. Поради тези причини оценката на условията и гаранциите, при които може да се издават и изпълняват такива заповеди, е от значение за настоящото решение.

([214]) Вж. част 3, глава 5 от ЗЗД от 2018 г.

([215]) Член 76 от ЗЗД от 2018 г.

([216]) Членове 54 и 130 от ЗПР от 2016 г. Издаващите органи трябва да преценят необходимостта от въвеждане на специфични гаранции за материалите, предадени на чужди органи, за да се гарантира, че по отношение на съхраняването, унищожаването и разкриването на данните ще се прилагат гаранции, сходни на тези, които са въведени съгласно членове 53 и 129 от ЗПР от 2016 г.

([217]) Споразумение между правителството на Обединеното кралство Великобритания и Северна Ирландия и правителството на Съединените американски щати относно достъпа до електрони данни с цел противодействие на тежката престъпност, достъпно на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

([218]) Това е първото споразумение, сключено съгласно Закона за изясняване на законосъобразното използване на данни в чужбина (CLOUD) на САЩ. Законът CLOUD на САЩ е американски федерален закон, приет на 23 март 2018 г., в който чрез изменение на Закона за съхраняваните съобщения от 1986 г. се изяснява, че доставчиците на услуги в САЩ са задължени да спазват американските заповеди за разкриване на съдържание и на данни без съдържание, независимо къде се съхраняват тези данни. Съгласно Закона CLOUD се допуска също сключването на изпълнителни споразумения с чужди правителства, въз основа на които доставчиците на услуги в САЩ да могат да предоставят данни със съдържание директно на тези чуждестранни правителства (текстът на Закона CLOUD е достъпен на следния адрес: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf)

(154) В това отношение следва да се отбележи, че първо, що се отнася до неговия материален обхват, Споразумението е приложимо само за престъпления, които се наказват с лишаване от свобода с максимален срок от поне три години (определени като „тежки престъпления“) ([219]), включително за „терористична дейност“. Второ, данните, обработвани в друга юрисдикция, могат да бъдат получени съгласно Споразумението само след издаването на „[з]аповед […], подлежаща на преглед или надзор съгласно националното право на издаващата страна от съд, съдия, магистрат или друг независим орган преди или в рамките на производство, свързано с изпълнението на заповедта“ ([220]). Трето, всяка заповед трябва „да се основава на изисквания за разумна обосновка, основаваща се на обосновани и достоверни факти, конкретност, законност и сериозност по отношение на разследваното деяние“ ([221]) и „да бъде насочена към конкретни потребителски профили и в нея да се назовава конкретно лице, потребителски профил, адрес или лично устройство, или друг специфичен идентификатор“ ([222]). Четвърто, данните, получени по силата на Споразумението, се ползват от защита, равностойна на специфичните гаранции, предоставени съгласно така нареченото „Рамково споразумение между ЕС и САЩ“ ([223]) — всеобхватно споразумение за защита на личните данни, сключено през декември 2016 г. между ЕС и САЩ, в което са определени гаранциите и правата, приложими при предаването на данни в рамките на сътрудничеството в областта на правоприлагането — които са включени *mutatis mutandis* в Споразумението между Обединеното кралство и САЩ, най-вече за да бъде отразен специфичният характер на предаването на данни (т.е. предаване от частни оператори към правоприлагащи органи, а не между правоприлагащи органи) ([224]). В Споразумението между Обединеното кралство и САЩ изрично се предвижда, че защита, равностойна на тази, предоставена съгласно Рамковото споразумение между ЕС и САЩ, ще се прилага „за цялата лична информация, получена при изпълнението на заповеди, предмет на Споразумението, с цел да се осигури равностойна защита“ ([225]).

(155) Следователно данните, предавани на американските власти съгласно Споразумението между Обединеното кралство и САЩ, следва да се ползват от защитата, осигурена от правен инструмент на ЕС, с необходимите адаптации, за да бъде отразено естеството на въпросното предаване. Освен това органите на Обединеното кралство са потвърдили, че защитата, предвидена в Рамковото споразумение, ще се прилага за цялата лична информация, предоставена или съхранявана съгласно Споразумението между Обединеното кралство и САЩ, независимо от естеството или типа на органа, отправящ искането (т.е. както от федералните, така и от щатските правоприлагащи органи в САЩ), така че равностойна защита трябва да бъде осигурена във всички случаи. Органите на Обединеното кралство обаче са пояснили също, че подробностите относно конкретното прилагане на гаранциите за защита на данните все още са предмет на обсъждане между Обединеното кралство и САЩ. В контекста на разговорите със службите на Европейската комисия по настоящото решение органите на Обединеното кралство потвърдиха, че ще се съгласят Споразумението да влезе в сила едва след като се убедят, че прилагането му отговаря на предвидените в него законови задължения, включително яснота по отношение на спазването на стандартите за защита на личните данни за всички данни, поискани съгласно Споразумението. Тъй като евентуалното влизане в сила на Споразумението може да повлияе на нивото на защита, оценено в настоящото решение, всяка бъдеща информация и разяснения относно начина, по който САЩ ще изпълняват задълженията си по Споразумението, следва да бъдат изпратени от Обединеното кралство на Европейската комисия незабавно след получаването им и във всеки случаи преди влизането в сила на Споразумението, за да се осигури подходящо наблюдение на настоящото решение в съответствие с член 45, параграф 4 от Регламент (ЕС) 2016/679. Особено внимание ще бъде обърнато на прилагането и адаптирането на защитата, предвидена в Рамковото споразумение, към конкретния вид предаване на данни, обхванато от Споразумението между Обединеното кралство и САЩ.

(156) В по-общ план всички относими промени, свързани с влизането в сила и прилагането на Споразумението, ще бъдат надлежно взети предвид в контекста на постоянното наблюдение на настоящото решение, включително по отношение на необходимите последици, които трябва да се изведат при наличието на признаци, че вече не се осигурява по същество равностойно ниво на защита.

3.2.3. *Надзор*

(157) В зависимост от правомощията, упражнявани от компетентните органи при обработването на лични данни за целите на правоприлагането (независимо дали съгласно ЗЗД от 2018 г. или на ЗПР от 2016 г.), надзорът над упражняването на тези правомощия се осъществява от различни органи. По-специално Комисарят по информацията надзирава

([219]) Член 1, параграф 14 от Споразумението.

([220]) Член 5, параграф 2 от Споразумението.

([221]) Член 5, параграф 1 от Споразумението.

([222]) Член 4, параграф 5 от Споразумението. По отношение на прихващането в реално време се прилагат допълнителни и по-строги изисквания: заповедите трябва да бъдат с ограничен срок, който не трябва да бъде по-дълъг от разумно необходимия за изпълнение на целите на заповедта, и се издават само ако същата информация практически не може да бъде получена със средства, които предполагат по-малка намеса (член 5, параграф 3 от Споразумението).

([223]) Споразумение между Съединените американски щати и Европейския съюз относно защитата на личната информация във връзка с предотвратяването, разследването, разкриването и наказателното преследване на престъпления, ОВ L 336, 10.12.2016 г., стр. 3, достъпно на следния адрес: https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:22016A1210(01)

([224]) Член 9, параграф 1 от Споразумението.

([225]) Член 9, параграф 1 от Споразумението.

обработването на лични данни, които попадат в обхвата на част 3 от ЗЗД от 2018 г. ([226]). Независим и съдебен надзор върху упражняването на правомощията за разследване съгласно ЗПР от 2016 г. се осъществява от службата на комисаря по правомощията за разследване (IPCO) ([227]) (този аспект е разгледан в съображения 250—255). Допълнителен надзор се осигурява също от Парламента и от други органи.

3.2.3.1. Надзор по отношение на част 3 от ЗЗД от 2018 г.

(158) Общите функции на комисаря по информацията, чиято независимост и организация са обяснени в съображение 87, 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. Основните задачи на комисаря по информацията са осъществяване на наблюдение и привеждане в изпълнение на част 3 от ЗЗД от 2018 г., както и повишаване на обществената осведоменост и предоставяне на консултации на Парламента, правителството и други институции и органи. 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. При тези обстоятелства надзорните функции се упражняват от други органи, както е обяснено в съображения 99—103.

(159) 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. По-специално комисарят има правомощия да уведомява администратора или обработващия лични данни за предполагаемо нарушение на част 3 от ЗЗД от 2018 г., да отправя предупреждения до администратора или обработващия лични данни или да ги порицава, когато са нарушили разпоредбите на част 3 от закона, както и да дава становище, по своя инициатива или при поискване, на Парламента, на правителството или на други институции и органи, както и на обществеността, по всички въпроси, свързани със защитата на личните данни ([228]).

(160) Освен това комисарят има правомощия да издава информационни постановления ([229]), ревизионни постановления ([230]) и изпълнителни постановления ([231]), както и правомощия за достъп до документи на администратори и обработващи данни и до техните помещения ([232]) и за налагане на административни наказания „глоба“ или „имуществена санкция“ под формата на наказателни постановления ([233]). В политиката на комисаря по информацията за регулаторните действия се определят обстоятелствата, при които комисарят издава съответно информационно, ревизионно, изпълнително и наказателно постановление ([234]) (вж. също съображение 93 и Директива (ЕС) 2016/680, съображения 101—102 във връзка с решенията относно адекватното ниво на защита).

(161) Според последните си годишни доклади (2018—2019 г. ([235]), 2019—2020 г. ([236])) комисарят по информацията проведе редица разследвания и предприе принудителни мерки във връзка с обработването на данни от правоприлагащи органи. Например комисарят проведе разследване и през октомври 2019 г. публикува Становище относно използването в правоприлагането 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 по информацията разследва матрицата за бандите (Gangs matrix) ([237]) 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. През ноември 2018 г. комисарят по информацията издаде изпълнително постановление и впоследствие MPS предприе необходимите действия за повишаване

([226]) Член 116 от ЗЗД от 2018 г.
([227]) Вж. ЗПР от 2016 г. и по-специално част 8, глава 1.
([228]) Точка 2 от приложение 13 към ЗЗД от 2018 г.
([229]) Да разпорежда на администратора и на обработващия лични данни (и при определени обстоятелства на всяко друго лице) да предоставят необходимата информация (член 142 от ЗЗД от 2018 г.).
([230]) Да разрешава извършването на разследвания и одити, при което администраторът или обработващият лични данни може да бъде 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 (член 146 от ЗЗД от 2018 г.).
([231]) Да дава разрешение за упражняването на корективни правомощия, за които може да се изисква администраторите/обработващите лични да предприемат или да се въздържат от предприемането на конкретни действия (член 149 от ЗЗД от 2018 г.).
([232]) Член 154 от ЗЗД от 2018 г.
([233]) Член 155 от ЗЗД от 2018 г.
([234]) Политика за регулаторните действия, вж. бележка под линия 96.
([235]) Годишен доклад и годишни финансови отчети на комисаря по информацията за 2018—2019 г., вж. бележка под линия 101.
([236]) Годишен доклад и годишни финансови отчети на комисаря по информацията за 2019—2020 г., вж. бележка под линия 82.
([237]) База данни, в която са записани разузнавателни данни, свързани с предполагаеми членове на банди и жертви на престъпления, свързани с банди.

на сигурността и отчетността и за гарантиране на пропорционалното използване на данните. Друг пример за скорошно изпълнително действие в тази област 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. Освен това понастоящем комисарят разследва случай, свързан с достъпа на правоприлагащите органи до данни, съхранявани от частноправен субект, Clearview AI Inc ([238]).

(162) Освен правомощията за привеждане в изпълнение на комисаря по информацията, описани в съображения 160 и 161, някои нарушения на законодателството за защита на личните данни 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, разкриването или съхраняването на лични данни без съгласието на администратора и за предоставянето на разкритите лични данни на друго лице без съгласието на администратора ([239]); реидентифицирането на информация, която представлява деидентифицирани лични данни, без съгласието на администратора, отговарящ за деидентифицирането на личните данни ([240]); умишленото възпрепятстване на комисаря да упражнява правомощията си за проверката на лични данни в съответствие с международни задължения ([241]), представянето на неверни данни в отговор на информационно постановление или унищожаването на информация във връзка с информационни и ревизионни постановления ([242]).

3.2.3.2. Други органи, осъществяващи надзор на правоприлагането в областта на наказателното право

(163) Освен комисаря по информацията, в областта на наказателното правоприлагане има няколко надзорни органа с конкретни правомощия, свързани с въпросите за защита на личните данни. Сред тях са например комисарят по въпросите на съхранението и използването на биометричен материал („комисарят по биометричните въпроси“) ([243]) и комисарят относно камерите за наблюдение ([244]).

3.2.3.3. Парламентарен надзор на правоприлагането в областта на наказателното право

(164) Специалната комисия по вътрешните работи осъществява парламентарен надзор в областта на правоприлагането. Тази комисия се състои от 11 членове на парламента от трите най-големи политически партии. Комисията има за задача да извършва преглед на разходите, управлението и политиката на Министерството на вътрешните работи и свързаните с него публични органи, т.е. включително на полицията и на Националната агенция по престъпността, чиято работа комисията може да проверява задълбочено ([245]).

([238]) Вж. изявление на комисаря по информацията, достъпно на следния адрес: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/

([239]) Член 170 от ЗЗД от 2018 г.

([240]) Член 171 от ЗЗД от 2018 г.

([241]) Член 119, параграф 6 от ЗЗД от 2018 г.

([242]) През финансовата година, обхващаща периода от 1 април 2019 г. до 31 март 2020 г., в резултат на разследванията на комисаря по информацията са издадени четири предупреждения и са заведени осем наказателни дела. Тези дела са заведени съгласно член 55 от Закона за защита на данните от 1998 г., член 77 от Закона за свобода на информацията от 2000 г. и член 170 от Закона за защита на данните от 2018 г. В 75 % от случаите обвиняемите са се признали за виновни, отказвайки се от воденето на продължителни съдебни процеси със свързаните с това разходи. (Годишен доклад и годишни финансови отчети на комисаря по информацията за 2019—2020 г. (вж. бележка под линия 87, стр. 40).

([243]) Длъжността „комисар по биометричните въпроси“ е създадена със Закона за защита на свободите от 2012 г. (вж.: https://www.legislation.gov.uk/ukpga/2012/9/contents). 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 свободата от 2012 г.). Комисарят по биометрични въпроси се назначава съгласно Кодекса за публичните назначения (Кодексът е достъпен на следния адрес: Https://www.gov.uk/government/publications/governance-code-for-public-appointments) и от условията за неговото назначаване става ясно, 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 за срок от три месеца, осъждане за извършено престъпление или неспазване на условията за назначаване.

([244]) Длъжността „комисар относно камерите за наблюдение“ е създадена със Закона за защита на свободите от 2012 г. със задача да насърчава спазването на Кодекса за поведение относно използването на камери за наблюдение; да извършва преглед на действието на този кодекс; и да дава становище на министрите дали този кодекс се нуждае от изменение. Комисарят се назначава съгласно същите правила като комисаря по биометричните въпроси и разполага със сходни правомощия, ресурси и защита срещу отстраняване.

([245]) Виж https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency-scrutinised/

(165) Комисията може да избере обекта на своите проверки в рамките на правомощията си, включително да проверява конкретни случаи, стига въпросът да не е предмет на съдебно производство. Комисията може също така да иска писмени доказателства и свидетелски показания от широк кръг групи и лица. Тя изготвя доклади за своите констатации и издава препоръки на правителството ([246]). Правителството трябва да отговори на всяка от препоръките в доклада в рамките на 60 дни ([247]).

(166) В областта на наблюдението комисията е изготвила и доклад относно Закона за уреждане на правомощията за разследване от 2000 г. (ЗУПР от 2000 г.) ([248]), в който заключава, че ЗУПР от 2000 г. не е подходящ за целта. Докладът е взет предвид при замяната на значителни части от ЗРРП от 2000 г. със ЗРП от 2016 г. Пълен списък на проверките може да бъде намерен на уебсайта на комисията ([249]).

(167) Задачите на Специалната комисия по вътрешните работи се изпълняват в Шотландия от Подкомисията по правосъдие и обществен ред и в Северна Ирландия от Комисията по правосъдие ([250]).

3.2.4. *Средства за правна защита*

(168) Що се отнася до обработването на данни от правоприлагащите органи, механизми за правна защита се предоставят съгласно част 3 от ЗЗД от 2018 г., съгласно ЗПР от 2016 г., както и съгласно Закона за правата на човека от 1998 г.

(169) Тези механизми осигуряват на субектите на данни ефективни административни и съдебни средства за правна защита, като им дават възможност по-специално да защитят правата си, включително правото на достъп до личните им данни или правото на коригиране или заличаване на такива данни.

(170) Първо, съгласно член 165 от ЗЗД от 2018 г. 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. ([251]). Комисарят по информацията има правомощието да преценява спазването на ЗЗД от 2018 г. от администратора и обработващия лични данни, да ги задължава да предприемат необходимите действия в случай на неспазване и да налага санкции.

([246]) Специалните комисии, включително Специалната комисия по вътрешните работи, трябва да спазват Правилника за вътрешния ред на Камарата на общините. В Правилника за вътрешния ред се съдържат правилата, приети от Камарата на общините, които уреждат работата на Парламента. Правомощията на специалните комисии са широки, като съгласно правило 152, параграф 1 „[с]пециалните комисии се назначават, за да извършват преглед на разходите, управлението и политиката на основните правителствени ведомства, както е посочено в параграф 2 от това правило, и на свързаните с тях публични органи.“ Това дава право на Специалната комисия по вътрешните работи да извърши преглед на всяка политика на Министерството на вътрешните работи, в която се съдържат политики (и свързаното с тях законодателство) относно правомощията за разследване. Освен това от правило 152, параграф 4 става ясно, че комисиите имат различни правомощия, включително да изискват от физически лица да дават показания или да предоставят документи по определен въпрос, както и да изготвят доклади. Текущите и предишните проверки на комисията са достъпни на следния адрес: https://committees.parliament.uk/committee/83/home-affairs-committee/.

([247]) Правомощията на Специалната комисията по вътрешните работи в Англия и Уелс са определени в Правилника за вътрешния ред на Камарата на общините, достъпен на следния адрес: https://www.parliament.uk/business/publications/commons/standing-orders-public11/.

([248]) Достъпен на следния адрес: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm.

([249]) Достъпен на следния адрес: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) Правилникът на Подкомисията по правосъдие и обществен ред в Шотландия е достъпен на следния адрес:https://www.parliament.scot/parliamentarybusiness/CurrentCommittees/justice-committee.aspx, а правилникът на Комисията по правосъдие в Северна Ирландия може да бъде намерен на следния адрес: http://www.niassembly.gov.uk/assembly-business/standing-orders/]

([251]) В последния годишен доклад на комисаря по информацията е дадена разбивка на естеството на получените и приключените жалби. По-специално броят на получените жалби, свързани с „дейности на полицията и регистри за съдимост“ възлиза на 6 % от общия брой на получените жалби (като бележи ръст от 1 % в сравнение с предходната финансова година). От годишния доклад става ясно също, че най-голям е броят на жалбите, свързани с искания за достъп на субекти на данни (46 % от общия брой жалби, което представлява ръст от 8 % в сравнение с предходната финансова година) (Годишен доклад на комисаря по информацията за 2019—2020 г., стр. 55; вж. бележка под линия 88.

(171) Второ, в ЗЗД от 2018 г. се предвижда право на средства за правна защита срещу комисаря по информацията, в случай че той не разгледа по подходящ начин жалба, внесена от субекта на данни. По-конкретно, ако комисарят не постигне „напредък“ ([252]) 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 ([253]) да разпореди на комисаря да предприеме подходящи действия, за да отговори на жалбата, или да информира жалбоподателя за напредъка по жалбата ([254]). 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 ([255]).

(172) Трето, физическите лица могат да получат съдебна защита срещу администраторите и обработващите лични данни пряко пред съдилищата. По-специално съгласно член 167 от ЗЗД от 2018 г. субектът на данни може да подаде жалба пред съда за нарушаване на негово право съгласно законодателството за защита на данните и съдът може чрез определение да задължи администратора да предприеме (или да се въздържи от предприемането на) действия по отношение на обработването, така че да бъде спазен ЗЗД от 2018 г. 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.

(173) И накрая, всяко лице, което счита, че неговите права, включително правото на неприкосновеност на личния живот и на защита на личните данни, са нарушени от публични органи, може да получи правна защита пред съдилищата на Обединеното кралство съгласно Закона за правата на човека от 1998 г. ([256]), а 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 съгласно Европейската конвенция за правата на човека ([257]) (вж. съображение 111).

3.2.4.1. Механизми за правна защита, налични съгласно ЗПР от 2016 г.

(174) Физическите лица могат да получат правна защита във връзка с нарушения на ЗПР от 2016 г. от Трибунала за правомощията за разследване. Възможностите за правна защита, налични съгласно ЗПР от 2016 г., са описани в съображения 263—269 по-долу.

([252]) 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.

([253]) 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.

([254]) Член 166 от ЗЗД от 2018 г. Сред примерите за успешни дела срещу комисаря по информацията, заведени пред трибунала, са случай, при който комисарят по информацията е потвърдил получаването на жалба от субект на данни, но не е посочил действията, които възнамерява да предприеме, и поради това му е разпоредено да потвърди в рамките на 21 календарни дни дали ще разследва жалбата и, ако е така, да информира жалбоподателя за хода на разследването не по-рядко от всеки 21 календарни дни след това (решението все още не е публикувано), както и случай, при който трибуналът от първа инстанция е счел, че не е ясно дали отговорът, предоставен от комисаря по информацията на жалбоподателя, отразява правилно „резултата“ от жалбата (вж. решението по делото Susan Milne/The Information Commissioner [2020], достъпно на следния адрес: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf)

([255]) Членове 162 и 163 от ЗЗД от 2018 г.

([256]) Вж. например делото Brown/Commissioner of Police of the Metropolis & Anor [2019] EWCA Civ 1724, в което е присъдено обезщетение от 9 000 британски лири съгласно ЗЗД от 1998 г. и съгласно Закона за правата на човека от 1998 г. за незаконно получаване на лична информация и злоупотреба с нея, и делотоR (с ищец Bridges)/Chief Constable of South Wales [2020] EWCA Civ 1058, в което Апелативният съд е обявил за незаконно внедряването на система за лицево разпознаване от полицията на Уелс, тъй като е в нарушение на член 8 от ЕКПЧ, и оценката на въздействието върху защитата на личните данни, изготвена от администратора, не съответства на ЗЗД от 2018 г.

([257]) Член 34 от Европейската конвенция за правата на човека гласи: „Съдът може да бъде сезиран с жалба от всяко лице, неправителствена организация или група лица, които твърдят, че са жертва на нарушение от страна на някоя от Високодоговарящите страни на правата, провъзгласени в Конвенцията или в Протоколите към нея. Високодоговарящите страни са длъжни да не създават по никакъв начин пречки за ефективното упражняване на това право“.

3.3. **Достъп и използване от публични органи на Обединеното кралство за целите на националната сигурност**

(175) В правния ред на Обединеното кралство разузнавателните служби, оправомощени да събират електронна информация, съхранявана от администратори или обработващи лични данни, от съображения за национална сигурност, при обстоятелства, които са от значение за адекватното ниво на защита, са Службата за сигурност (MI5) ([258]), Службата за тайно разузнаване (SIS ([259])) и Правителствената централа за комуникации ([260]) (GCHQ) ([261]).

3.3.1. *Правни основания, ограничения и гаранции*

(176) В Обединеното кралство правомощията на разузнавателните служби са определени в ЗПР от 2016 г. и в ЗУПР от 2000 г., в които, наред със ЗЗД от 2018 г., са предвидени материалния и личностния обхват на тези правомощия, както и ограниченията и гаранциите за упражняването им. Тези правомощия, както и приложимите към тях ограничения и гаранции са подробно оценени в следващите раздели.

3.3.1.1. Правомощия за разследване, упражнявани в контекста на националната сигурност

(177) Правната уредба за упражняването на разследващи правомощия, т.е. на правомощия за прихващане на комуникационни данни, достъп до тях и за намеса в оборудването, се съдържа в ЗПР от 2016 г. Със ЗПР от 2016 г. е въведена обща забрана на използването на техники за достъп до съдържанието на съобщенията, достъп до данни за съобщенията или намеса в оборудването без законно разрешение и тези дейности са криминализирани ([262]) . Това намира отражение във факта, че упражняването на тези правомощия за разследване е законно само когато се извършва въз основа на заповед или разрешение ([263]).

(178) В ЗПР от 2016 г. се определят подробни правила, уреждащи обхвата и прилагането на правомощията за разследване, както и техните специфични ограничения и гаранции. В зависимост от вида на правомощията за разследване (прихващане на комуникации, получаване и събиране и съхраняване на комуникационни данни и

([258]) MI5 е на подчинение на министъра на вътрешните работи. Функциите на MI5 са описани в Закона за службите за сигурност от 1989 г: защита на националната сигурност (включително защита срещу заплахи от шпионаж, тероризъм и саботаж, от дейности на агенти на чужди сили и от действия, насочени към отхвърляне или подриване на парламентарната демокрация с политически, индустриални или насилствени средства), защита на икономическото благосъстояние на Обединеното кралство от външни заплахи и подкрепа на дейностите на полицейските служби и на други правоприлагащи органи за предотвратяването и разкриването на тежки престъпления.

([259]) Правителствената централа за комуникации е на подчинение на министъра на външните работи и нейните функции са описани в Закона за разузнавателните служби от 1994 г. Функциите ѝ включват получаването и предоставянето на информация, свързана с действията или намеренията на лица извън Британските острови, и изпълнението на други задачи, свързани с действията или намеренията на такива лица. Тези функции могат да се упражняват само в интерес на националната сигурност, в интерес на икономическото благосъстояние на Обединеното кралство или в подкрепа на предотвратяването или разкриването на тежки престъпления.

([260]) Правителствената централа за комуникации е на подчинение на министъра на външните работи и нейните функции са описани в Закона за разузнавателните служби от 1994 г. Те са а) наблюдение, използване или намеса в електромагнитни и други емисии и в оборудване, произвеждащо такива емисии, получаване и предоставяне на информация, извлечена от такива емисии или оборудване, или свързана с тях, както и от криптирани материали; б) предоставяне на консултантска помощ и съдействие по езикови въпроси, включително във връзка с техническа терминология и криптография и с други въпроси, свързани със защитата на информацията, на въоръжените сили, на правителството или на други организации или лица, които се считат за уместни. Тези функции може да се упражняват само в интерес на националната сигурност, в интерес на икономическото благосъстояние на Обединеното кралство във връзка с действията или намеренията на лица извън Британските острови или в подкрепа на предотвратяването или разкриването на тежки престъпления.

([261]) Други публични органи, упражняващи функции, свързани с националната сигурност, са Военното разузнаване, Съветът и Секретариатът за национална сигурност, Съвместната организация за разузнаване и Съвместният разузнавателен комитет. Нито Съвместният разузнавателен комитет, нито Съвместната организация за разузнаване обаче се ползват с правомощия за разследване съгласно ЗПР от 2016 г., а обхватът на правомощията на Военното разузнаване е ограничен.

([262]) Забраната се прилага както за обществени, така и за частни комуникационни мрежи, както и за обществените пощенски служби, когато прихващането се извършва в Обединеното кралство. Забраната не се прилага за администратора на частна мрежа, ако той е дал изрично или мълчаливо съгласие за извършване на прихващането (член 3 от ЗПР от 2016 г.).

([263]) В конкретни ограничени случаи е възможно прихващането да се извършва без заповед, тоест когато се осъществява със съгласието на подателя или получателя (член 44 от ЗПР от 2016 г.), когато се осъществява за административни цели или за целите на привеждането в изпълнение (членове 45—48 от ЗПР от 2016 г.), в някои специализирани институции (членове 49—51 от ЗПР от 2016 г.) и в съответствие с искания на чужди държави (член 52 от ЗПР от 2016 г.).

намеса в оборудването) ([264]), както и от това дали правомощието се упражнява за конкретна цел или масово, се прилагат различни правила. Подробности относно обхвата, гаранциите и ограниченията на всяка мярка, предоставена от ЗПР от 2016 г., са описани в специалния раздел по-долу.

(179) ЗПР от 2016 г. е допълнен с редица нормативно приети кодекси за поведение, издадени от министъра, одобрени от двете камари на Парламента ([265]) и приложими на територията на цялата държава, в които се дават насоки за упражняването на тези правомощия ([266]). Субектите на данни могат да разчитат пряко на разпоредбите на ЗПР от 2016 г., за да упражняват правата си, а точка 5 от приложение 7 към ЗПР от 2016 г. уточнява, че кодексите за поведение са допустими като доказателство в граждански и наказателни производства, а съдът, трибуналът или надзорният орган могат да вземат предвид всяко неспазване на кодексите при решаването на свързан с тях въпрос в съдебното производство ([267]). В контекста на своята оценка на „качеството на законодателството“ на предишното законодателство на Обединеното кралство в областта на наблюдението, ЗУПР от 2000 г., големият състав на Европейския съд по правата на човека изрично призна значението на кодексите за поведение на Обединеното кралство и прие, че техните разпоредби могат да бъдат взети предвид при оценката на предвидимостта на законодателството, позволяващо наблюдението ([268]).

(180) Следва също така да се отбележи, че службите за национална сигурност и някои правоприлагащи органи имат целеви правомощия (за целево прихващане ([269]), събиране на комуникационни данни ([270]), съхраняване на комуникационни данни ([271]) и целева намеса в оборудването ([272])), докато само разузнавателните служби ([273]) може да упражняват правомощия, свързани с масиви от данни (т.е. масово прихващане ([274]), масово събиране на комуникационни данни ([275]), масова намеса в оборудването ([276]) и големи масиви от лични данни ([277])).

(181) Когато взема решение кое разследващо правомощие следва да бъде упражнено, разузнавателната служба трябва да се съобразява с „общите задължения във връзка с неприкосновеността на личния живот“, изброени в член 2, параграф 2, буква а) от ЗПР от 2016 г., които включват проверка за необходимост и пропорционалност. По-конкретно по смисъла на тази разпоредба публичен орган, който възнамерява да упражнява правомощие за разследване, трябва да прецени i) дали това, което се цели да бъде постигнато със заповедта, разрешението или

([264]) Що се отнася например до обхвата на тези мерки, в част 3 и част 4 (съхраняване и събиране на комуникационни данни), обхватът на мярката е тясно свързан с определението за „телекомуникационни оператори“, чиито данни на потребителите са предмет на мярката. Друг пример може да бъде даден във връзка с използването на „масови“ правомощия. В този случай обхватът на тези правомощия е ограничен до „комуникации, изпращани или получавани от лица извън Британските острови“.

([265]) В приложение 7 към ЗПР от 2016 г. са определени обхватът на кодексите, процедурата, която трябва да се следва при издаването им, правилата за тяхното преразглеждане и правните последици от кодексите.

([266]) Кодексите за поведение съгласно ЗПР от 2016 г. са достъпни на следния адрес: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) Съдилищата и трибуналите използват кодексите за поведение при оценка на законосъобразността на действията на органите. Вж. например: делото Dias/Cleveland Police, [2017] UKIPTrib15_586-CH, в което Трибуналът за правомощията за разследване се позовава на конкретни извадки от Кодекса за поведение относно комуникационните данни, за да изясни определението на основанието „за предотвратяване или разкриване на престъпления или за предотвратяване на безредици“, използвано в искания за събиране на комуникационни данни. Кодексът е включен в мотивите на решението, в което се заключава, че това основание е използвано неправилно. Въз основа на това съдът постановява, че оспорените действия са незаконни. Съдилищата също така са оценили нивото на гаранциите, предвидени в кодексите, вж. например решението по делото Just for Law Kids/Secretary of State for the Home Department [2019] EWHC 1772 (Admin), в което Върховният съд се произнася, че първичното и вторичното законодателство, заедно с вътрешните насоки, осигуряват достатъчни гаранции; или решението по делото R (National Council for Civil Liberties)/Secretary of State for the Home Department и други [2019] EWHC 2057 (Admin), в което съдът се произнася, че както ЗПР от 2016 г., така и Кодексът за поведение относно намесата в оборудването съдържат достатъчно разпоредби, свързани с необходимостта заповедите да бъдат конкретни.

([268]) По делото Big Brother Watch големият състав на Европейския съд по правата на човека отбелязва, че „[т]ъй като Кодексът за поведение относно прихващането на съобщения е публичен документ, който се одобрява и от двете камари на Парламента и се публикува онлайн и на хартия от правителството, той трябва да се зачита както от лицата, изпълняващи функции по прихващане, така и от съдилищата (вж. точки 93—94 по-горе). Вследствие на това Съдът прие, че неговите разпоредби могат да бъдат взети предвид при оценката на предвидимостта на ЗУПР (вж. решение по дело Kennedy, цитирано по-горе, § 157). Съответно Съдът би приел, че вътрешното право е било „достъпно“ по адекватен начин.“ (Вж. Европейски съд по правата на човека (голям състав), Big Brother Watch и др./Обединено кралство, жалби № 58170/13, 62322/14 и 24960/15 („Big Brother Watch и др.“) от 25 май 2021 г., т. 366).

([269]) Част 2 от ЗПР от 2016 г.

([270]) Част 3 от ЗПР от 2016 г.

([271]) Част 4 от ЗПР от 2016 г.

([272]) Част 5 от ЗПР от 2016 г.

([273]) За списъка на съответните правоприлагащи органи, които могат да упражняват целеви правомощия по разследване съгласно ЗПР от 2016 г., вж. предишната бележка под линия (139).

([274]) Член 136 от ЗПР от 2016 г.

([275]) Член 158 от ЗПР от 2016 г.

([276]) Член 176 от ЗПР от 2016 г.

([277]) Член 199 от ЗПР от 2016 г.

постановлението, е практически възможно да бъде постигнато с други средства, които предполагат по-малка намеса; ii) дали нивото на защита, което трябва да се прилага във връзка с всяко получаване на информация по силата на заповедта, разрешението или постановлението, е по-високо поради особената чувствителност на тази информация; iii) обществения интерес от целостта и сигурността на далекосъобщителните системи и на пощенските услуги, и iv) всички други аспекти на обществения интерес от защитата на правото на неприкосновеност на личния живот ([278]).

(182) Начинът, по който следва да се прилагат тези критерии, както и начинът, по който се оценява тяхното съответствие като част от разрешението за упражняване на такива правомощия от министъра и от независимите съдебни комисари, са допълнително уточнени в съответните кодекси за поведение. По-специално упражняването на всяко от тези разследващи правомощия трябва винаги да бъде „пропорционално на това, което се цели да бъде постигнато, [което] предполага да се намери баланс между сериозността на намесата в личния живот (и другите съображения, посочени в член 2, параграф 2) и необходимостта от дейността от гледна точка на разследването, оперативната дейност или способностите“. Това означава по-специално, че упражняването на правомощието „следва да предлага реална възможност за постигане на очакваната полза и не следва да е непропорционално или произволно“, както и че „намесата в личния живот не следва да се счита за пропорционална, ако търсената информация е практически възможно да бъде получена с други средства, които предполагат по-малка намеса“ ([279]). По-конкретно спазването на принципа на пропорционалност трябва да се оценява, като се вземат предвид следните критерии: „i) обема на предложената намеса в личния живот спрямо това, което се цели да бъде постигнато; ii) как и защо методите, които ще бъдат възприети, ще доведат до възможно най-малка намеса по отношение на лицето и на други лица; iii) дали дейността представлява подходящо използване на закона и разумен начин за постигане на това, което се цели да бъде постигнато, като се вземат предвид всички разумни алтернативи; iv) какви други методи, според случая, са или не са били приложени, или са били използвани, но са оценени като недостатъчни за постигане на оперативните цели без упражняване на предложеното правомощие за разследване“ ([280]).

(183) На практика, както е обяснено от органите на Обединеното кралство, това гарантира, че дадена разузнавателна служба първо определя оперативната цел (като по този начин ограничава събирането, напр. за цел, свързана с борбата с международния тероризъм в определен географски район) и след това, въз основа на тази оперативна цел, трябва да прецени коя техническа възможност (напр. целево прихващане или масово прихващане, намеса в оборудването, събиране на комуникационни данни) е най-пропорционална (т.е. води до най-малка намеса в личния живот; вж. член 2, параграф 2 от ЗПР) на това, което се цели да бъде постигнато, и следователно може да бъде разрешена на едно от съществуващите законови основания.

(184) Струва си да се отбележи, че това стъпване на стандартите за необходимост и пропорционалност е отбелязано и приветствано и от специалния докладчик на ООН за правото на неприкосновеност на личния живот Джоузеф Канатаци, който заявява във връзка със системата, създадена със ЗПР от 2016 г., че „въведените както в разузнавателните служби, така и в правоприлагащите органи процедури, изглежда, систематично изискват разглеждане на необходимостта и пропорционалността на дадена мярка за наблюдение или операция, преди тя да бъде препоръчана за одобрение, както и проверка на мярката или дейността на същото основание“ ([281]). Той също така отбелязва, че при срещата си с представители на правоприлагащите органи и службите за национална сигурност „е получил единодушното мнение, че правото на неприкосновеност на личния живот трябва да бъде първостепенно съображение при всяко решение относно мерки за наблюдение. Всички те разбират и оценяват необходимостта и пропорционалността като основни принципи, които трябва да се вземат под внимание“.

([278]) В Кодекса за поведение относно прихващането на комуникация се посочва, че другите елементи на проверката за пропорционалност включват: „i) обема на предложената намеса в личния живот спрямо това, което се цели да бъде постигнато; ii) как и защо методите, които ще бъдат възприети, ще доведат до възможно най-малка намеса по отношение на лицето и на други лица; iii) дали дейността представлява подходящо използване на закона и разумен начин за постигане на това, което се цели да бъде постигнато, като се вземат предвид всички разумни алтернативи; iv) какви други методи, според случая, са или не са били приложени, или са били използвани, но са оценени като недостатъчни за постигане на оперативните цели без упражняване на предложеното правомощие за разследване“. Параграф 4.16 от Кодекса за поведение относно прихващането на комуникация, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([279]) Вж. параграфи 4.12 и 4.15 от Кодекса за поведение относно прихващането на комуникация, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([280]) Вж. параграф 4.16 от Кодекса за поведение относно прихващането на комуникация.

([281]) Заключително изявление на специалния докладчик за правото на неприкосновеност на личния живот в края на неговата мисия в Обединеното кралство Великобритания и Северна Ирландия, достъпно на следния адрес: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, para 1.a.

(185) Конкретните критерии за издаване на различните заповеди, както и ограниченията и гаранциите, предвидени в ЗПР от 2016 г. по отношение на всяко правомощие за разследване, са подробно описани в съображения 186—243.

3.3.1.1.1. Целево прихващане и преглед

(186) Съществуват три вида заповеди за целево прихващане: заповед за целево прихващане ([282]), заповед за целеви преглед и заповед за взаимопомощ ([283]). Условията за тяхното получаване и съответните гаранции са посочени в част 2, глава 1 от ЗПР от 2016 г.

(187) Със заповедта за целево прихващане се разрешава прихващането на комуникациите, описани в заповедта, в процеса на тяхното предаване, както и получаването на други данни, свързани с тези комуникации ([284]), включително вторични данни ([285]). Със заповедта за целеви преглед се упълномощава определено лице да извърши подбор на прихванато съдържание, получено по заповед за масово прихващане, за целите на прегледа ([286]).

(188) Всяка заповед по смисъла на част 2 от ЗПР от 2016 г. може да бъде издадена от министъра ([287]) и одобрена от съдебен комисар ([288]). Във всички случаи срокът на действие на всякакъв вид заповеди за целево действие е ограничен до 6 месеца ([289]), а по отношение на изменението ([290]) и подновяването на заповедта ([291]) се прилагат конкретни правила.

(189) Преди да издаде заповедта министърът на Обединеното кралство трябва да извърши оценка на необходимостта и пропорционалността. ([292]). По-специално по отношение на заповед за целево прихващане и заповед за целеви преглед министърът следва да провери дали мярката е необходима на едно от следните основания: тя е в интерес на националната сигурност; прилага се за предотвратяване или разкриване на тежко престъпление; или в интерес на икономическото благосъстояние на Обединеното кралство ([293]), доколкото този интерес е от значение и за интересите на националната сигурност ([294]). От друга страна, заповед за взаимопомощ (вж. съображение 139 по-горе) може да бъде издадена само ако министърът прецени, че съществуват обстоятелства, равностойни на тези, при които би издал заповед с цел предотвратяване и/или разкриване на тежко престъпление ([295]).

(190) Освен това министърът следва да прецени дали мярката е пропорционална на това, което се цели да бъде постигнато ([296]). Когато се оценява пропорционалността на исканите мерки, трябва да се вземат предвид общите задължения по отношение на неприкосновеността на личния живот, изложени в член 2, параграф 2 от ЗПР от 2016 г., по-специално необходимостта да се оцени дали това, което се цели да бъде постигнато със заповедта,

([282]) Член 15, параграф 2 от ЗПР от 2016 г.

([283]) Член 15, параграф 4 от ЗПР от 2016 г.

([284]) Член 15, параграф 2 от ЗПР от 2016 г.

([285]) Вторичните данни са данни, които се добавят към или са логически свързани с прихванатата комуникация, могат да бъдат логически отделени от нея и, ако се отделят по този начин, не биха разкрили нищо от това, което би могло разумно да се счита за смисъл (ако има такъв) на комуникацията. Някои примери за вторични данни включват конфигурации на рутера или защитни стени, или периода от време, в който рутерът е бил активен в мрежата, когато те са част от прихванатата комуникация, добавят се към нея или са логично свързани с нея. За повече подробности вж. определението в член 16 от ЗПР от 2016 г. и параграф 2.19 от Кодекса за поведение относно прихващането на комуникация, вж. бележка под линия 278.

([286]) Този преглед се извършва като изключение от член 152, параграф 4 от ЗПР от 2016 г., в който е предвидена забрана на опитите за идентифициране на комуникацията на лица, които се намират на Британските острови. Вж. съображение 229.

([287]) Шотландският министър одобрява заповедта, когато се отнася за тежка престъпна дейност в Шотландия (вж. член 21 и член 22 от ЗПР от 2016 г.), а министърът на Обединеното кралство може да определи висш служител, който да издава заповеди за взаимопомощ, когато има вероятност прихващането да бъде свързано с лице или с помещения, намиращи се извън Обединеното кралство (член 40 от ЗПР от 2016 г.).

([288]) Член 19 и член 23 от ЗПР от 2016 г.

([289]) Член 32 от ЗПР от 2016 г.

([290]) Член 39 от ЗПР от 2016 г. Ограничени изменения на заповедите могат да се правят от точно определени лица при условията, определени в ЗПР от 2016 г. Лицето, издало заповедта, може да я отмени по всяко време. То трябва да отмени заповедта, ако тя вече не е необходима на каквото и да е подходящо основание или ако деянието, разрешено със заповедта, вече не е пропорционално на това, което се цели да бъде постигнато.

([291]) Член 33 от ЗПР от 2016 г. Решението за подновяване на заповедта трябва да бъде одобрено от съдебен комисар.

([292]) Член 19 от ЗПР от 2016 г.

([293]) По отношение на понятието „в интерес на икономическото благосъстояние, когато този интерес е от значение и за националната сигурност“ Европейският съд по правата на човека (голям състав) установи в т. 371 на решението си по дело Big Brother Watch and others/United Kingdom (вж. бележка под линия 268 по-горе), че това понятие е достатъчно фокусирано върху националната сигурност. Въпреки че констатацията на Съда по това дело е свързана с използването на понятието в ЗРРП от 2000 г., същото понятие се използва и в ЗПР от 2016 г.

([294]) Член 20, параграф 2 от ЗПР от 2016 г.

([295]) Член 20, параграф 3 от ЗПР от 2016 г.

([296]) Член 19, параграф 1, буква б), член 19, параграф 2, буква б) и член 19, параграф 3, буква б) от ЗПР от 2016 г.

разрешението или постановлението, е практически възможно да бъде постигнато с други средства, които предполагат по-малка намеса, и дали нивото на защита, което трябва да се прилага във връзка с всяко получаване на информация по силата на заповедта, разрешението или постановлението, е по-високо поради особената чувствителност на тази информация (вж. съображение 181 по-горе).

(191) За тази цел ще се наложи министърът да вземе предвид всички елементи на заявлението, представено от подалия искането орган, по-специално свързаните с лицата, които трябва да бъдат прихванати, и със значението на мярката за разследването. Такива елементи са посочени в Кодекса за поведение относно прихващането на комуникация и трябва да бъдат описани с определена степен на конкретност ([297]). Освен това съгласно член 17 от ЗПР от 2016 г. във всяка заповед, издадена съгласно глава 2 от него, трябва да се назовава или описва конкретното лице или група лица, организация или помещения, спрямо които ще се извършва прихващане (т.е. „обектът“). Когато заповедта е за целево прихващане или за целеви преглед, тя може да се отнася и до група лица, до повече от едно лице или една организация или до повече от една група помещения (наричана също „тематична заповед“) ([298]). В тези случаи в заповедта следва да бъде описана общата цел или дейност на групата лица или на операцията/разследванията и да се назоват или опишат колкото е възможно повече от тези лица/организации или групи от помещения, когато това е практически осъществимо ([299]). И накрая, във всички заповеди, издадени съгласно част 2 от ЗПР от 2016 г., трябва да се посочват адресите, номерата, апаратурата, факторите или комбинацията от фактори, които ще се използват за идентифициране на комуникациите ([300]). В това отношение в Кодекса за поведение относно прихващането на комуникация се уточнява, че в случай на заповед за целево прихващане и заповед за целеви преглед „в заповедта трябва да се посочват (или описват) факторите или комбинацията от фактори, които ще се използват за идентифициране на комуникациите. Когато комуникациите ще се идентифицират чрез позоваване (например) на телефонен номер, номерът трябва да бъде посочен в неговата цялост. Когато обаче за идентифициране на комуникациите ще се използват много сложни или непрекъснато променящи се интернет превключватели, те следва да бъдат описани, доколкото е възможно“ ([301]).

(192) Важна гаранция в този контекст е, че оценката, извършена от министъра за целите на издаването на заповед, трябва да бъде одобрена от независим съдебен комисар ([302]), който проверява по-специално дали решението за издаване на заповедта отговаря на принципите на необходимост и пропорционалност ([303]) (във връзка със статута и ролята на съдебните комисари вж. съображения 251—256 по-долу). В ЗПР от 2016 г. също така е пояснено, че при извършване на такава проверка съдебният комисар трябва да прилага същите принципи, каквито биха били приложени от съда във връзка с молба за съдебен контрол ([304]). По този начин се гарантира, че във всеки отделен случай и преди да се осъществи достъп до данните, спазването на принципа на необходимост и пропорционалност се проверява систематично от независим орган.

(193) В ЗПР от 2016 г. се предвиждат малко конкретни и ограничени изключения за извършване на целенасочени прихващания без заповед. Тези ограничени случаи са подробно описани в закона ([305]) и, с изключение на случаите, които се основават на „съгласие“ на изпращача/получателя, те се извършват от лица (физически лица или публични органи), различни от службите за национална сигурност. Освен това този вид прихващане се извършва за цели, различни от събирането на „разузнавателна информация“ ([306]), и в някои случаи е много малко вероятно събирането да се извърши в контекста на сценарий на „предаване“ (например в случай на прихващане, извършено в психиатрична

([297]) Исканата информация включва подробности за ситуацията (описание на лицата/организациите/помещенията, комуникацията, която ще бъде прихваната) и как получаването на тази информация ще бъде от полза за разследването, както и описание на действията, за които се иска разрешение. В случай че не е възможно да се опишат лицата/организацията/помещенията, трябва да се включи обяснение защо това не е било възможно или защо е направено само общо описание (параграфи 5.32 и 5.34 от Кодекса за поведение относно прихващането на комуникация, вж. бележка под линия 278).

([298]) Член 17, параграф 2 от ЗПР от 2016 г. Вж. също параграф 5.11 и сл. от Кодекса за поведение относно прихващането на съобщения, вж. бележка под линия 278.

([299]) Член 31, параграфи 4 и 5 от ЗПР от 2016 г.

([300]) Член 31, параграф 8 от ЗПР от 2016 г.

([301]) Параграфи 5.37 и 5.38 от Кодекса за поведение относно прихващането на комуникация, вж. бележка под линия 278.

([302]) Одобрението от съдебен комисар не се изисква, когато министърът прецени, че има спешна необходимост от издаване на заповедта (член 19, параграф 1 от ЗПР). Съдебният комисар обаче трябва да бъде информиран в кратък срок и трябва да реши дали да одобри заповедта или не. Ако заповедта не бъде одобрена, тя престава да действа (член 24 и член 25 от ЗПР от 2016 г.).

([303]) Член 23, параграф 1 от ЗПР от 2016 г.

([304]) Член 23, параграф 2 от ЗПР от 2016 г.

([305]) Вж. членове 44—51 от ЗПР от 2016 г. и член 12 от Кодекса за поведение относно прихващането на комуникация (вж. бележка под линия 278).

([306]) Такъв е случаят например, когато е необходимо прихващане в затвор или в психиатрична болница (за да се провери поведението на задържано лице или пациент) или от пощенски или телекомуникационни оператор, например за откриване на съдържание, представляващо злоупотреба.

болница или в затвор). Като се има предвид естеството на органа, за който се отнасят тези специфични случаи (различен от службите за национална сигурност), ще се прилагат всички гаранции, предвидени в част 2 от ЗЗД от 2018 г. и ОРЗД на Обединеното кралство, включително надзора на комисаря по информацията и наличните механизми за правна защита. Освен това в допълнение към гаранциите, предоставени от ЗЗД от 2018 г., в някои случаи ЗПР от 2016 г. предвижда и последващ надзор от страна на IPCO ([307]).

(194) Когато се извършва прихващане, се прилагат допълнителни ограничения и гаранции с оглед на специфичния статут на засегнатото(ите) лице(а) ([308]). Например, прихващането на отделни съобщения, които са обект на адвокатска тайна, се разрешава само при извънредни и наложителни обстоятелства, а лицето, което издава заповедта, трябва да вземе предвид обществения интерес от поверителността на пратките, които са обект на адвокатска тайна, и специфичните изисквания по отношение на обработването, съхраняването и разкриването на такива материали ([309]).

(195) Освен това в ЗПР от 2016 г. са предвидени специфични гаранции, свързани със сигурността, съхраняването и разкриването, които министърът следва да вземе предвид, преди да издаде заповед за целево действие ([310]). По-специално съгласно член 53, параграф 5 от ЗПР от 2016 г. всяко направено копие на който и да е от материалите, събрани по силата на заповедта, трябва да се съхранява по сигурен начин и да бъде унищожено веднага след отпадането на съответните основания за съхраняването му, а съгласно член 53, параграф 2 от ЗПР от 2016 г. броят на лицата, на които се разкрива материалът, и степента на разкриването, предоставянето или копирането на материала трябва да бъдат ограничени до необходимия минимум за постигането на законоустановените цели.

(196) И накрая, когато материалът, който е прихванат въз основа на заповед за целево прихващане или на заповед за взаимопомощ, трябва да бъде предаден на трета държава („разкриване в чужбина“), в ЗПР от 2016 г. се предвижда, че министърът трябва да се увери, че са налице подходящи договорености, които да гарантират, че в тази трета държава съществуват подобни гаранции за сигурност, съхраняване и разкриване ([311]). В допълнение член 109, параграф 2 от ЗЗД от 2018 г. предвижда, че разузнавателните служби могат да предават лични данни извън територията на Обединеното кралство само ако предаването е необходима и пропорционална мярка за целите на законоустановените функции на администратора или за други цели, предвидени в член 2, параграф 2, буква а) от Закона за службите за сигурност от 1989 г. или в член 2, параграф 2, буква а) и член 4, параграф 2, буква а) от Закона за разузнавателните служби от 1994 г. ([312]) Важно е да се отбележи, че тези изисквания се прилагат и в случаите, когато се прави позоваване на изключението във връзка с националната сигурност съгласно член 110 от ЗЗД от 2018 г., тъй като в него не е посочен член 109 от ЗЗД от 2018 г. като една от разпоредбите, която може да не се прилага, ако се изисква освобождаване от определени разпоредби с цел опазване на националната сигурност.

3.3.1.1.2. Целево събиране и съхраняване на комуникационни данни

(197) ЗПР от 2016 г. позволява на министъра да изисква от операторите на далекосъобщителни мрежи да съхраняват комуникационни данни с оглед осъществяването на целеви достъп от страна на редица публични органи, включително правоприлагащи органи и разузнавателни служби. В част 4 от ЗПР от 2016 г. е уредено съхраняването на комуникационни данни, а в част 3 се съдържат разпоредби относно целевото събиране на комуникационни данни. В част 3 и част 4 от ЗПР от 2016 г. са определени също специфични ограничения за упражняването на тези правомощия и са предвидени специфични гаранции.

([307]) Вж. обратния случай в член 229, параграф 4 от ЗПР.

([308]) С членове 26—29 от ЗПР от 2016 г. се въвеждат ограничения за издаване на заповеди за целево прихващане и целеви преглед във връзка с прихващане на комуникации, изпратени или предназначени за лице, което е член на Парламента (всеки парламент на Обединеното кралство), прихващане на вещи, които са обект на адвокатска тайна, прихващане на комуникации, за които прихващащият орган смята, че съдържат поверителни журналистически материали, и когато целта на заповедта е да се идентифицира или потвърди източник на журналистическа информация.

([309]) Член 26 от ЗПР от 2016 г.

([310]) Член 19, параграф 1 от ЗПР от 2016 г.

([311]) Член 54 от ЗПР от 2016 г. Гаранциите, свързани с разкриването на материали пред чуждестранни органи, са допълнително уточнени в кодексите за поведение: вж. по-специално точка 9.26 и сл. и точка 9.87 от Кодекса за поведение относно прихващането на съобщения, както и точка 9.33 и сл. и точка 9.41 от Кодекса за поведение относно намесата в оборудването (вж. бележка под линия 278).

([312]) Тези цели са: по отношение на службата за сигурност: предотвратяване или разкриване на тежки престъпления или наказателно производство (член 2, параграф 2, буква а) от Закона за службите за сигурност от 1989 г.); по отношение на разузнавателната служба: интересите на националната сигурност, предотвратяването или разкриването на тежко престъпление или наказателно производство (член 2, параграф 2, буква а) от Закона за разузнавателните служби от 1994 г.); и по отношение на Правителствената централа за комуникации: наказателно производство (член 4, параграф 2, буква а) от Закона за разузнавателните служби от 1994 г.). Вж. също обяснителните бележки относно ЗЗД от 2018 г., които могат да бъдат намерени на следния адрес: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted.

(198) Терминът „комуникационни данни“ обхваща кой, кога, къде и как е осъществил комуникацията, но не и нейното съдържание, т.е. какво е казано или написано. За разлика от прихващането, получаването и съхраняването на данни за съобщенията не е насочено към получаване на съдържанието на съобщението, а към получаване на информация например за абоната на телефонна услуга или подробна фактура. Това може да включва времето и продължителността на съобщението, номера или адреса на електронната поща на изпращача и получателя, а понякога и местоположението на устройствата, от които са осъществени електронните съобщения ([313]).

(199) Следва да се отбележи, че съхраняването и събирането на комуникационни данни обикновено не засяга лични данни на субекти на данни от ЕС, предадени съгласно настоящото решение на Обединеното кралство. Задължението за съхраняване или разкриване на комуникационни данни съгласно части 3 и 4 от ЗПР от 2016 г. обхваща данни, които се събират от оператори на далекосъобщителни мрежи в Обединеното кралство директно от потребителите на далекосъобщителна услуга ([314]). Този тип „насочено към потребителя“ обработване обикновено не включва предаване въз основа на настоящото решение, т.е. предаване от администратор/обработващ в ЕС към администратор/обработващ в Обединеното кралство.

(200) За целите на изчерпателността обаче условията и гаранциите, уреждащи тези режими на събиране и съхраняване, са описани по-долу.

(201) Като предпоставка трябва да се отбележи, че съхраняването и целевото събиране на комуникационни данни е на разположение както на националните агенции за сигурност, така и на някои правоприлагащи органи ([315]). Условията за изискване на запазването и/или събирането на комуникационни данни могат да варират в зависимост от основанието за искане на мярката, а именно национална сигурност или цел на правоприлагането.

(202) По-специално, въпреки че новият режим въведе общото изискване за предварително разрешение от независим орган, което ще се прилага във всички случаи, когато комуникационни данни се запазват и/или придобиват (за целите на правоприлагането или за целите на националната сигурност), съгласно решението на Съда на Европейския съюз по делото Tele2/Watson ([316]) са въведени специфични гаранции, когато мярката е поискана за целите на правоприлагането. По-специално, когато запазването или придобиването на комуникационни данни се изисква за целите на правоприлагането, предварителното разрешение винаги трябва да се дава от комисаря по правомощията за разследване. Това не винаги е така, когато мярката е поискана за целите на националната сигурност, тъй като, както е описано по-долу, в някои случаи такъв вид мерки могат да бъдат разрешени от друго „разрешаващо лице“. Освен това новият режим повиши прага, за който може да бъде разрешено съхраняването и придобиването на комуникационни данни до „тежки престъпления“ ([317]).

([313]) Определение на „данни за съобщенията“ се съдържа в член 261, параграф 5 от ЗПР от 2016 г. Данните за съобщенията са разделени на „данни за събития“ (всякакви данни, с които се идентифицира или описва събитие, независимо дали по отношение на местоположението му или не, във или чрез далекосъобщителна система, когато събитието представлява извършване на определена дейност в определен момент от един или повече субекти) и „данни за субекта“ (всякакви данни, които а) са свързани със i) субект, ii) връзка между далекосъобщителна услуга и субект или iii) връзка между която и да е част от далекосъобщителна система и субект, б) се състоят от или включват данни, които идентифицират или описват субекта (независимо дали по отношение на неговото местоположение или не), и в) не са данни за събития).

([314]) Това следва от определението за комуникационни данни в член 261, параграф 5 от ЗПР от 2016 г., съгласно което комуникационните данни се съхраняват или получават от оператор на далекосъобщителна мрежа и или се отнасят до потребителя на далекосъобщителна услуга и са свързани с предоставянето на тази услуга, или се съдържат в дадена комуникация, представляват част от нея, добавени са към нея или са свързани логически с нея (вж. също Кодекса за поведение относно комуникационните данни, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf, параграфи 2.22—2.33). Освен това съгласно определението за „оператор на далекосъобщителна мрежа“ в член 261, параграф 10 от ЗПР от 2016 г. операторът на далекосъобщителната мрежа трябва да е лице, което предлага или предоставя далекосъобщителна услуга на лица в Обединеното кралство, или лице, което контролира или предоставя далекосъобщителна система, която (изцяло или частично) се намира в Обединеното кралство или се контролира от Обединеното кралство. От тези определения става ясно, че не могат да бъдат налагани задължения съгласно ЗПР от 2016 г. на оператори на далекосъобщителни мрежи, чието оборудване не се намира в Обединеното кралство и не се контролира от него и които не предлагат или не предоставят услуги на лица в Обединеното кралство (вж. също Кодекса за поведение относно комуникационните данни, параграф 2.1). Ако абонати от ЕС (независимо дали се намират в ЕС или в Обединеното кралство) използват услуги в Обединеното кралство, всички комуникации във връзка с предоставянето на тези услуги ще се събират директно от доставчика на услуги в Обединеното кралство, а няма да подлежат на предаване от ЕС.

([315]) Тези органи са изброени в приложение 4 към ЗПР от 2016 г. и включват полицейските служби, разузнавателните служби, някои министерства и ведомства, Националната агенция по престъпността, Кралската данъчна и митническа служба, Органа за защита на конкуренцията и пазарите, комисаря по информацията, службите за бърза помощ, противопожарните и спасителните служби и органи например в областта на здравето и безопасността на храните.

([316]) Съединени дела C-203/15 и C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

([317]) Вж. член 61.7, буква б) относно придобиването на комуникационни данни и член 87.10A относно съхраняването на комуникационни данни.

i) *Разрешение за получаване на комуникационни данни*

(203) Съгласно част 3 от ЗПР от 2016 г. на съответните публични органи се разрешава да получават комуникационни данни от оператор на далекосъобщителна мрежа или от всяко лице, способно да получава и разкрива такива данни. С разрешението не може да се позволява прихващане на съдържанието на комуникациите ([318]) и то престава да действа след период от един месец ([319]), като има възможност да се поднови с допълнително разрешение ([320]). За придобиването на комуникационни данни се изисква разрешение от комисаря по правомощията за разследване (IPC) ([321]) (относно статута и правомощията на IPC вж. съображения 250—251 по-долу). Такъв е винаги случаят, когато получаването на комуникационни данни се изисква от съответния правоприлагащ орган. В член 61 от ЗПР от 2016 г. обаче се предвижда, че когато данните се придобиват в интерес на националната сигурност или на икономическото благосъстояние на Обединеното кралство, стига това да е от значение за националната сигурност, или когато служител на разузнавателна служба е подал искане съгласно член 61, параграф 7, буква б) ([322]), придобиването може алтернативно ([323]) да бъде разрешено от IPC или от определен за това висш служител ([324]). Определеният служител трябва да бъде независим от съответното разследване или операция и да има познания на работно равнище за принципите и законодателството в областта на правата на човека, особено за принципите на необходимост и пропорционалност ([325]). Решението, взето от определения служител, се подлага на последващ контрол от страна на IPC (вж. съображение 254 по-долу за повече подробности относно функциите на IPC за последващ контрол).

(204) Разрешението за получаване на комуникационни данни се основава на оценка на необходимостта и пропорционалността на мярката. По-конкретно необходимостта на мярката се оценява с оглед на основанията, изброени в законодателството ([326]). Предвид целевия характер на тази мярка, тя трябва също така да бъде необходима за конкретно разследване или операция ([327]). Допълнителни изисквания за оценка на необходимостта от мерките се съдържат в Кодекса за поведение относно комуникационните данни ([328]). По-специално в този кодекс се предвижда, че в искането, внесено от подаващия орган, следва да бъдат посочени най-малко три елемента, с които да се обоснове необходимостта от искането: i) разследваното събитие, например престъпление или местонахождение на уязвимо изчезнало лице; ii) лицето, за което се търсят данни, като заподозрян, свидетел или изчезнало лице, и как то е свързано със събитието; и iii) търсените комуникационни данни, като телефонен номер или IP адрес, и как тези данни са свързани с лицето и събитието ([329]).

(205) Освен това събирането на комуникационни данни трябва да бъде пропорционално на това, което се цели да бъде постигнато ([330]). В Кодекса за поведение относно комуникационните данни се пояснява, че когато извършва такава оценка, даващото разрешението лице следва да намери баланс между „степента на намеса в правата и свободите на дадено лице и конкретната полза за разследването или операцията, предприети от подходящ публичен орган в обществен интерес“, както и че като се вземат предвид всички факти и обстоятелства по конкретния случай, „намеса в

([318]) Член 60A, параграф 6 от ЗПР от 2016 г.

([319]) Този период се намалява на три дни, когато разрешението се дава по неотложни причини (член 65, параграф 3, A от ЗПР от 2016 г.).

([320]) Съгласно член 65 от ЗПР от 2016 г. подновеното разрешение е валидно един месец от датата на изтичане на съществуващото разрешение. Лицето, издало разрешението, може да го отмени по всяко време, ако прецени, че то вече не отговаря на изискванията.

([321]) Член 60A, параграф 1 от ЗПР от 2016 г. Службата за разрешения за комуникационни данни (OCDA) изпълнява тази функция от името на IPC (вж. Кодекс на добрите практики за комуникационните данни, параграф 5.6)

([322]) Искането съгласно член 61, параграф 7, буква б) от ЗПР от 2016 г. се подава за „приложима цел, свързана с престъпление“, което съгласно член 61, параграф 7, A от ЗПР от 2016 г. означава: „за целите на предотвратяването или разкриването на тежко престъпление, когато комуникационните данни са изцяло или частично данни за събития; за целите на предотвратяването или разкриването на престъпление или за предотвратяването на безредици —във всички други случаи“.

([323]) В Кодекса за поведение относно комуникационните данни се посочва, че „когато искане, свързано с националната сигурност, може да бъде подадено, както съгласно член 60A, така и съгласно член 61, решението за това коя процедура за получаване на разрешение е най-подходяща във всеки отделен случай се взема от отделните публични органи. Публичните органи, които желаят да използват процедурата с определения висш служител, следва да имат ясни насоки за това кога тази процедура за получаване на разрешение е подходяща“ (параграф 5.19 от Кодекса за поведение относно комуникационните данни, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf).

([324]) В член 70, параграф 3 от ЗПР от 2016 г. е дадено определението на „определен служител“, което е различно в зависимост от съответния публичен орган (както е посочено в приложение 4 към ЗПР от 2016 г.).

([325]) Подробна информация за независимостта на определения висш служител са предоставени в Кодекса за поведение относно комуникационните данни (Кодекс за поведение относно комуникационните данни, параграфи 4.12—4.17, вж. бележка под линия 323).

([326]) Основанията са: i) национална сигурност; ii) предотвратяване или разкриване на престъпление или предотвратяване на безредици (в случай на „данни за събития“ — само тежко престъпление); iii) в интерес на икономическото благосъстояние на Обединеното кралство, доколкото този интерес е от значение и за интересите на националната сигурност; iv) в интерес на обществената безопасност; v) за предотвратяване на смърт или нараняване, или на каквито и да било увреждания на физическото или психичното здраве на дадено лице, или за ограничаване на наранявания или увреждания на физическото или психичното здраве на дадено лице; vi) за подпомагане на разследването на предполагаеми съдебни грешки или vii) за установяване на самоличността на мъртво лице или на лице, което не може да удостовери самоличността си поради определено състояние (член 61, параграф 7 от ЗПР от 2016 г.).

([327]) Член 60A, параграф 1, буква б) от ЗПР от 2016 г.

([328]) Параграф 3.3 и сл. от Кодекса за поведение относно комуникационните данни, вж. бележка под линия 323.

([329]) Параграф 3.13 от Кодекса за поведение относно комуникационните данни, вж. бележка под линия 323.

([330]) Член 60, параграф 1, буква c) от ЗПР от 2016 г.

правата на дадено лице все пак може да не е оправдана, тъй като неблагоприятното въздействие върху правата на друго лице или група лица е твърде сериозно“. Освен това, за да се оцени конкретно пропорционалността на мярката, в кодекса са изброени редица елементи, които следва да бъдат включени в подадената от органа молба ([331]). Освен това трябва да се обърне специално внимание на типа комуникационни данни (данни за „субект“ или за „събитие“ ([332])), които ще бъдат получени, и трябва да се даде предпочитание на използването на категория данни, която предполага по-малка намеса ([333]). Кодексът за поведение относно комуникационните данни съдържа също така конкретни инструкции във връзка с разрешенията, свързани с комуникационни данни на лица от определени професии (като лекари, адвокати, журналисти, членове на Парламента или свещенослужители) ([334]), по отношение на които се прилагат допълнителни гаранции ([335]).

ii) *Постановление за съхраняване на комуникационни данни*

(206) В част 4 от ЗПР от 2016 г. са определени правилата за съхраняване на комуникационни данни, и по-специално критериите, въз основа на които министърът може да издаде постановление за съхраняване ([336]). Гаранциите, въведени от ЗПР, са същите, когато данните се съхраняват за целите на правоприлагането или в интерес на националната сигурност.

(207) Издаването на такива постановления за съхраняване има за цел да се гарантира, че операторите на далекосъобщителни мрежи съхраняват за период от най-много 12 месеца подходящи комуникационни данни, които иначе биха били изтрити, след като вече не са необходими за стопански цели ([337]). Съхранените данни трябва да останат на разположение за необходимия период, в случай че впоследствие възникне необходимост публичен орган да ги получи съгласно разрешение за целево събиране на комуникационни данни, предвидено в част 3 от ЗПР от 2016 г. и описано в съображения 203—205.

(208) За упражняването на това правомощие съществуват редица ограничения и гаранции. Министърът може да издаде постановление за съхраняване на един или няколко оператора ([338]) само когато смята, че изискването за съхраняването на данните е необходимо поради едно от законоустановените цели ([339]) и е пропорционално на това, което се цели да бъде постигнато ([340]). За тази цел и както е изяснено в самия ЗПР

([331]) Информацията, която трябва да бъде включена, трябва да съдържа: i) кратко описание на начина, по който получаването на данните ще допринесе за разследването или операцията; ii) обосновка на периодите от време, за които се отнася искането, включително по отношение на тяхната пропорционалност на разследваното събитие; iii) обосновка на нивото на намеса, като се вземе предвид ползата от данните за разследването (тази обосновка следва да включва преценка дали за постигане на целта може да бъдат предприети разследвания, които предполагат по-малка намеса); iv) анализ на правата (по-специално на неприкосновеност на личния живот и когато е уместно — на свобода на изразяване) на лицето и постигане на баланс между тези права и ползата за разследването; v) подробности за това каква странична намеса може да настъпи и как периодите от време, за които се отнася искането, влияят върху страничната намеса (Кодекс за поведение относно комуникационните данни, параграфи 3.22—3.26, вж. бележка под линия 323).

([332]) Вж. бележка под линия 313.

([333]) Когато се искат комуникационни данни, които предполагат по-голяма намеса (напр. данни за събитие), в кодекса е посочено, че е по-подходящо първо да се получат данни за субекта или директно да се получат данни за събития в ограничени специфични случаи на неотложност (Кодекс за поведение относно комуникационните данни, параграфи 6.10—6.14, вж. бележка под линия 323).

([334]) Параграфи 8.8—8.44 от Кодекса за поведение относно комуникационните данни, вж. бележка под линия 323.

([335]) В Кодекса за поведение се посочва, че „даващото разрешение лице трябва да обърне специално внимание, когато разглежда такива искания, включително да прецени допълнително дали може да има неволни последици от тях и дали искането обслужва най-добре обществения интерес“ (Кодекс за поведение относно комуникационните данни, параграф 8.8). Освен това трябва да се водят регистри на този тип искания и при следващата проверка вниманието на IPC следва да бъде насочено към такива искания (Кодекс за поведение относно комуникационните данни, параграф 8.10, вж. бележка под линия 323).

([336]) Членове 87—89 от ЗПР от 2016 г.

([337]) Съгласно член 90 от ЗПР от 2016 г. оператор на далекосъобщителна мрежа, на когото е връчено постановление за съхраняване, може да поиска министърът, който го е издал, да го преразгледа.

([338]) Съгласно член 87, параграф 2, буква а) от ЗПР от 2016 г. постановлението за съхраняване може да се отнася до „определен оператор или описание на група оператори“.

([339]) Целите са: i) в интерес на националната сигурност; ii) приложима цел, свързана с престъпността (съгласно определението в член 87, параграф 10А от ЗПР от 2016 г.); iii) в интерес на икономическото благосъстояние на Обединеното кралство, доколкото този интерес е от значение и за интересите на националната сигурност; iv) в интерес на обществената безопасност; v) предотвратяване на смърт или нараняване, или на каквито и да било увреждания на физическото или психичното здраве на дадено лице, или ограничаване на наранявания или увреждания на физическото или психичното здраве на дадено лице; или vi) подпомагане на разследването на предполагаеми съдебни грешки (член 87 от ЗПР).

([340]) Член 87 от ЗПР от 2016 г. Освен това, съгласно съответния кодекс за поведение, за да се оцени пропорционалността на постановлението за съхраняване, се прилагат критериите, предвидени в член 2, параграф 2 от ЗПР от 2016 г., по-специално изискването за оценка дали това, което се цели да бъде постигнато с постановлението, е практически възможно да бъде постигнато с други средства, които предполагат по-малка намеса. Както във връзка с оценката на пропорционалността при събиране на комуникационни данни, в Кодекса за поведение относно комуникационните данни се пояснява, че такава оценка включва „постигането на баланс между степента на намеса в правото на зачитане на неприкосновеността на личния живот на физическото лице и конкретната полза за разследването“ (Кодекс за поведение относно комуникационните данни, параграф 16.3, вж. бележка под линия 323).

от 2016 г. ([341]), преди да издаде постановление за съхраняване, министърът трябва да вземе предвид: вероятните ползи от постановлението ([342]); описанието на далекосъобщителните услуги; целесъобразността на ограничаването на данните, които трябва да бъдат съхранени, чрез посочване на местоположението или чрез описания на лицата, на които се предоставят далекосъобщителните услуги ([343]); вероятния брой потребители (ако е известен) на всяка далекосъобщителна услуга, за която се отнася постановлението ([344]); техническата осъществимост на изпълнението на постановлението; вероятните разходи за изпълнение на постановлението и всички други последици от постановлението за оператора на далекосъобщителната мрежа (или описание на операторите), за когото се отнася ([345]). Както е подробно описано в глава 17 от Кодекса за поведение относно комуникационните данни, във всички постановления за съхраняване трябва да се посочи всеки вид данни, който ще бъде съхранен, и основанията, поради които той отговаря на необходимите стандарти за съхраняване.

(209) Във всички случаи (както за целите на националната сигурност, така и за целите на правоприлагането) решението на министъра да издаде постановление за съхраняване трябва да бъде одобрено от независим съдебен комисар в рамките на т.нар. „процедура с двойна защита“, който трябва да провери по-специално дали постановлението за съхраняване на съответните комуникационни данни е необходимо и пропорционално за една или повече от законоустановените цели ([346]).

3.3.1.1.3. Намеса в оборудването

(210) Намесата в оборудването се състои от набор от техники, използвани за получаване на разнообразни данни от оборудването ([347]), което включва компютри, таблети и смартфони, както и кабели, проводници и устройства за съхранение ([348]). Намесата в оборудването дава възможност да се получат както съдържанието на комуникациите, така и данни от оборудването ([349]).

(211) В съответствие с член 13, параграф 1 от ЗПР от 2016 г., за да осъществи дадена разузнавателна служба намеса в оборудването, е необходимо разрешение, което се издава чрез заповед по процедурата с „двойна защита“, установена със ЗПР от 2016 г., при условие че има „връзка с Британските острови“ ([350]). Според обясненията, предоставени от

([341]) Вж. член 88 от ЗПР от 2016 г.

([342]) Ползите могат да бъдат съществуващи или предвиждани и трябва да са свързани със законоустановените цели, за които могат да се съхраняват данните (Кодекс за поведение относно комуникационните данни, параграф 17.17, вж. бележка под линия 323).

([343]) Това включва да се определи дали пълният географски обхват на постановлението за съхраняване е необходим и пропорционален и дали е необходимо и пропорционално да се включат или изключат лица с някакви конкретни описания (Кодекс за поведение относно комуникационните данни, параграф 17.17, вж. бележка под линия 323).

([344]) Това ще помогне на министъра за прецени както нивото на намеса в личния живот на потребителите, така и вероятните ползи от данните, които трябва да бъдат съхранени (Кодекс за поведение относно комуникационните данни, параграф 17.17, вж. бележка под линия 323).

([345]) Член 88 от ЗПР от 2016 г.

([346]) Член 89 от ЗПР от 2016 г.

([347]) Съгласно член 135, параграф 1 и член 198, параграф 1 от ЗПР от 2016 г. понятието „оборудване“ включва оборудване, което създава електромагнитни, акустични или други емисии, и всяко устройство, което може да се използва във връзка с такова оборудване.

([348]) Кодекс за поведение относно намесата в оборудването, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf , т. 2.2.

([349]) Данните от оборудването са определени в член 100 от ЗПР от 2016 г. като системни данни и данни, които а) се съдържат в дадена комуникация, представляват част от нея, добавени са към нея или са свързани логически с нея (независимо дали от подателя или по друг начин) или с която и да е друга информация; б) е възможно да бъдат логически отделени от останалата част на комуникацията или от информацията и в) ако бъдат отделени по този начин, не биха разкрили нищо от това, което би могло разумно да се счита за смисъл (ако има такъв) на комуникацията.

([350]) За да бъде условието за наличие на заповед задължително, съгласно член 13, параграф 1 от ЗПР от 2016 г. действията на разузнавателната служба трябва да съставляват едно или повече престъпления съгласно членове 1—3А от Закона за злоупотребата с компютри от 1990 г., какъвто би бил случаят при преобладаващото мнозинство от обстоятелства, вж. Кодекса за поведение относно намесата в оборудването, параграфи 3.32 и 3.6—3.9). Съгласно член 13, параграф 2 от ЗПР от 2016 г. „връзка с Британските острови“ има, ако а) някое от действията би било извършено на Британските острови (независимо от местоположението на оборудването, в което би била или може да бъде осъществена намеса), б) разузнавателната служба смята, че което и да е оборудване, в което би била или би могло да бъде осъществена намеса, би се намирало или може да се намира на Британските острови в даден момент, докато се осъществява намесата, или в) целта на намесата е да се получат i) комуникации, изпратени от или на лице, което се намира или за което разузнавателната служба смята, че към момента се намира на Британските острови, ii) лична информация, свързана с лице, което се намира или за което разузнавателната служба смята, че към момента се намира на Британските острови, или iii) данни за оборудване, които са част от комуникации или лична информация, които попадат в обхвата на подточка i) или подточка ii), или са свързани с тях.

органите на Обединеното кралство, в случаите, когато данните се предават от Европейския съюз към Обединеното кралство в рамките на обхвата на настоящото решение, винаги ще има „връзка с Британските острови“ и поради това всяка намеса в оборудването, обхващаща такива данни, подлежи на задължителното условие за наличие на заповед по член 13, параграф 1 от ЗПР от 2016 г. ([351]).

(212) Правилата във връзка със заповедите за целева намеса в оборудването са определени в част 5 от ЗПР от 2016 г. Подобно на целевото прихващане, целевата намеса в оборудването трябва да се отнася за конкретен „обект“, който трябва да бъде посочен в заповедта ([352]). Подробностите за това как трябва да бъде идентифициран „обектът“ зависят от предмета на действията и от вида на оборудването, в което ще бъде осъществена намеса.. По-специално в член 115, параграф 3 от ЗПР са посочени елементите, които следва да бъдат включени в заповедта (напр. име на лицето или наименование на организацията, описание на местоположението), в зависимост например от това дали намесата се отнася до оборудване, което принадлежи на определено лице или организация, или група лица, използва се от тях или е в тяхно владение, намира се на определено място и т.н. ([353]). Целите, за които могат да бъдат издадени заповеди за целева намеса в оборудване, зависят от публичния орган, който я иска ([354]).

(213) Както при целевото прихващане, издаващият орган трябва да прецени дали мярката е необходима за постигане на конкретна цел и дали е пропорционална на това, което се цели да бъде постигнато ([355]). Освен това той следва също така да прецени дали съществуват гаранции по отношение на сигурността, съхраняването и разкриването, както и във връзка с „разкриването в чужбина“ ([356]) (вж. съображение 196).

(214) Заповедта трябва да бъде одобрена от съдебен комисар, освен на случай на неотложност ([357]). В последния случай съдебен комисар трябва да бъде уведомен за издаването на заповедта и трябва да я одобри в срок от три работни дни. В случай че съдебният комисар откаже да я одобри, заповедта престава да действа и не може да бъде подновявана ([358]). Освен това съдебният комисар има правомощието да изисква всички данни, получени по силата на заповедта, да бъдат заличени ([359]). Фактът, че дадена заповед е била издадена спешно не влияе на последващия контрол (вж. съображения 244—255) или на възможностите на лица да търсят правна защита (вж. съображения 260—270). Физическите лица могат да подадат жалба до ICO или да предявят иск относно всяко предполагаемо поведение пред Трибунала за правомощията за разследване по обичайния начин. Във всички случаи проверката, която се извършва от съдебния комисар, когато трябва да реши дали да одобри дадена заповед, е провераката за необходимостта и пропорционалността, както по отношение на исканията за целево прихващане ([360]) (вж. съображение 192 по-горе).

([351]) От съображения за пълнота следва да се отбележи, че дори в ситуации, в които няма „връзка с Британските острови“ и следователно осъществяването на намеса в оборудването не подлежи на задължителното условия за наличие на заповед по член 13, параграф 1 от ЗПР от 2016 г., разузнавателна служба, която възнамерява да осъществи дейност, за която може да получи заповед за масова намеса в оборудването, по принцип следва да получи такава заповед (вж. Кодекс за поведение относно намесата в оборудването, параграф 3.24). Дори когато заповедта за намеса в оборудването по ЗПР от 2016 г. нито се изисква по закон, нито е получена на принципна основа, действията на разузнавателните служби подлежат на редица условия и ограничения съгласно член 7 от Закона за разузнавателните служби от 1994 г. Това включва по-специално изискването за разрешение от министъра, който трябва да се увери, че нито едно действие не надхвърля необходимото за правилното изпълнение на функциите на разузнавателната служба.

([352]) Съдържанието на заповедта е регламентирано в член 115 от ЗПР от 2016 г., където е уточнено, че в нея трябва да бъдат посочени имената на лицата или наименованията на организациите, или тяхно описание, местоположението или групата лица, които се явяват „обект“, описание на естеството на разследването и описание на дейностите, за които се използва оборудването. В нея също така трябва да бъде описан видът на оборудването и действията, които са разрешени на лицето, до което е адресирана заповедта.

([353]) Вж. също Кодекс за поведение относно намесата в оборудването, параграф 5.7, вж. бележка под линия 348.

([354]) Службите за национална сигурност могат да подават искания за заповед за намеса в оборудването, когато това е необходимо за целите на националната сигурност, за разкриване на тежки престъпления и/или в интерес на икономическото благосъстояние на Обединеното кралство, доколкото този интерес е от значение и за интересите на националната сигурност (член 102 и член 103 от ЗПР от 2016 г.). В зависимост от органа заповед за намеса в оборудването може да се иска за целите на правоприлагането, когато това е необходимо за разкриване или предотвратяване на тежко престъпление, или за предотвратяване на смърт или нараняване или на увреждане на физическото или психичното здраве на дадено лице, или за ограничаване на наранявания или увреждания на физическото или психичното здраве на дадено лице (вж. член 106, параграф 1 и член 106, параграф 3 от ЗПР от 2016 г.).

([355]) Член 102, параграф 1 от ЗПР от 2016 г.

([356]) Членове 129—131 от ЗПР от 2016 г.

([357]) Член 109 от ЗПР от 2016 г.

([358]) Член 109, параграф 4 от ЗПР от 2016 г.

([359]) Член 110, параграф 3, буква b) от ЗПР от 2016 г. Съгласно параграф 5.67 от Кодекса за поведение относно намесата в оборудването спешността се определя от това дали би било разумно осъществимо да се поиска одобрението на съдебния комисар да издаде заповедта в рамките на наличното време, за да се отговори на оперативна или следствена нужда. Спешните заповеди следва да попадат в едната или и в двете от следните категории: i) непосредствена заплаха за живота или заплаха от тежки посегателства – например ако дадено лице е било отвлечено и се преценява, че животът му е в непосредствена опасност; или ii) възможност за събиране на разузнавателна информация или за разследване с ограничено време за действие – например пратка наркотици от клас A предстои да влезе в Обединеното кралство, а правоприлагащите органи искат да бъдат обхванати извършителите на тежки престъпления, за да извършат арести. Вж. бележка под линия 348.

([360]) Член 108 от ЗПР от 2016 г.

(215) И накрая, специфичните гаранции, приложими по отношение на целевото прихващане, що се отнася до срока на валидност, подновяването и изменянето на заповедта, както и прихващането на членове на Парламента, на пратки, които са обект на адвокатска тайна, и на журналистически материали (за повече подробности вж. съображение 193), се прилагат и по отношение на намесата в оборудването.

3.3.1.1.4. Упражняване на правомощия, свързани с масиви от данни

(216) Правомощията, свързани с масиви от данни, са уредени в част 6 от ЗПР от 2016 г. Освен това в кодексите за поведение се съдържат по-подробни разпоредби относно упражняването на правомощия, свързани с масиви от данни. Въпреки че в законодателството на Обединеното кралство няма определение на „правомощие, свързано с масиви от данни“, в контекста на ЗПР от 2016 г. то е описано като събиране и съхраняване на големи количества данни, получени от правителството чрез различни средства (т.е. правомощията за масово прихващане, масово събиране на данни, масова намеса в оборудването и масиви от лични данни), до които впоследствие органите могат да осъществят достъп. Това описание е пояснено, като е уточнено какво не е „правомощие, свързано с масиви от данни“: то не е равносилно на така нареченото „масово наблюдение“ без ограничения или гаранции. Напротив, както е обяснено по-долу, то подлежи на ограничения и гаранции, чиято цел е да се гарантира, че достъпът до данни не се предоставя неизбирателно или необосновано ([361]). По-специално правомощията, свързани с масиви от данни, може да се упражняват само ако се установи връзка между техническата мярка, която дадена национална разузнавателна служба възнамерява да приложи, и оперативната цел, за която се иска такава мярка.

(217) Освен това правомощия, свързани с масиви от данни, имат само разузнавателните служби и за упражняването им винаги се изисква заповед, издадена от министъра и одобрена от съдебен комисар. При избора на средства за събиране на разузнавателни данни трябва да се има предвид дали въпросната цел може да се преследва със „средства, които предполагат по-малка намеса“ ([362]). Този подход произтича от правната уредба, която се основава на принципа на пропорционалност и следователно дава приоритет на целевото събиране пред масовото събиране на данни.

3.3.1.1.4.1. Масово прихващане и масова намеса в оборудването

(218) Режимът за масово прихващане е уреден в част 6, глава 1 от ЗПР от 2016 г., а в глава 3 от същата част е уредена масовата намеса в оборудването. Тези режими са по същество еднакви и поради това условията и допълнителните гаранции, приложими по отношение на такива заповеди, се анализират заедно.

i) *Условия и критерии за издаването на заповед*

(219) Заповедта за масово прихващане е ограничена до прихващането на комуникация, изпратена или получена от лица, които са извън Британските острови ([363]) (така наречената „свързана с чужбина комуникация“ ([364])), в процеса на тяхното предаване, както и до прихващането на други подходящи данни, и до последващия подбор

([361]) Според доклада относно правомощията, свързани с масиви от данни, представен преди одобряването на ЗПР от 2016 г. от лорд Дейвид Андерсън, независим оценител на законодателството за борба с тероризма, *„трябва да е ясно, че събирането и съхраняването на масиви от данни не е равносилно на така нареченото „масово наблюдение“. Всяка уважаваща себе си правна система ще предвиди ограничения и гаранции, чиято цел е именно да се гарантира, че достъпът до големи количества чувствителни данни (...) не се предоставя неизбирателно или необосновано. Такива ограничения и гаранции със сигурност съществуват в законопроекта.*. Лорд Дейвид Андерсън, Доклад относно правомощията, свързани с масиви от данни, август 2016 г., параграф 1.9 (подчертаването е добавено), достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

([362]) Член 2,2 от ЗПР от 2016 г. Вж. например параграф 4.11 от Кодекса за поведение относно масовото събиране на комуникационни данни, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) „Британските острови“ се състоят от Обединеното кралство, Англо-нормандски острови и остров Ман и са определени в приложение 1 към Закона за тълкуването от 1978 г., достъпно на следния адрес: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1.

([364]) Съгласно член 136 от ЗПР от 2016 г. „свързана с чужбина комуникация“ означава: i) комуникация, изпратена от физически лица, които са извън Британските острови, или ii) комуникация, получена от физически лица, които са извън Британските острови. Този режим, както е потвърдено от органите на Обединеното кралство, обхваща и комуникацията между две лица, и двете от които са извън Британските острови. Големият състав на Европейския съд по правата на човека по дело Big Brother Watch и др./Обединено кралство (вж. бележка под линия 279 по-горе), точка 376, приема по отношение на сходно ограничение (отнасящо се до „външните комуникации“) на комуникациите, които могат да бъдат засечени чрез масово прихващане съгласно ЗУПР от 2000 г, че то е било достатъчно ограничено и предвидимо.

на прихванатите материали ([365]) за целите на прегледа. Със заповедта за масова намеса в оборудването ([366]) на адресата се разрешава да осъществи намеса във всяко оборудване с цел да се получи свързана с чужбина комуникация (в това число всичко, което включва реч, музика, звуци, визуални изображения или данни от всякакво естество), данни от оборудването (данни, които позволяват или улесняват работата на пощенска служба; далекосъобщителна система; далекосъобщителна услуга) или друга информация. далекосъобщителна система; далекосъобщителна услуга) или друга информация ([367]).

(220) Министърът може да издаде заповед във връзка с масиви от данни само по молба, подадено от ръководител на разузнавателна служба ([368]). Заповед, с която се разрешава масово прихващане или масова намеса в оборудването, трябва да се издава само ако е необходима в интерес на националната сигурност и за допълнителна цел, свързана с предотвратяването или разкриването на тежко престъпление, или в интерес на икономическото благосъстояние на Обединеното кралство, когато е от значение за националната сигурност ([369]). Освен това съгласно член 142, параграф 7 от ЗПР от 2016 г. заповедта за масово прихващане трябва да съдържа повече подробности, а не само позоваване на „интересите на националната сигурност“, „икономическото благосъстояние на Обединеното кралство“ и „предотвратяването и борбата с тежките престъпления“, и в нея трябва да бъде установена връзка между мярката, която се иска, и една или повече оперативни цели, които трябва да бъдат включени в заповедта.

(221) Изборът на оперативната цел е резултат от многопластов процес. В член 142, параграф 4 е предвидено, че оперативните цели, посочени в заповедта, трябва да бъдат упоменати в списък, поддържан от ръководителите на разузнавателните служби, като цели, които според тях представляват оперативни цели, за които прихванатото съдържание или вторичните данни, получени по силата на заповеди за масово прихващане, може да подлежат на подбор за целите на прегледа. Списъкът на оперативните цели трябва да бъде одобрен от министъра. Министърът може да даде такова одобрение само ако е убеден, че оперативната цел е посочена по-подробно, а не само с позоваване на общите основания за разрешаване на заповедта (национална сигурност или национална сигурност и икономическо благосъстояние, или предотвратяване на тежки престъпления) ([370]). В края на всяко тримесечие министърът трябва да предоставя копие от списъка на оперативните цели на Парламентарната комисия по разузнаване и сигурност. И накрая, министър-председателят трябва да преразглежда списъка с оперативни цели най-малко веднъж годишно ([371]). Както отбеляза Висшият съд, „тези гаранции не трябва да бъдат омаловажавани като незначителни, тъй като заедно изграждат сложен набор от режими на отчетност, в които участват Парламентът, както и членовете на правителството на най-високо равнище“ ([372]).

(222) С тези оперативни цели също така се ограничава обхватът на подбора на материалите от прихващането за етапа на преглед. Подборът на материалите, събрани съгласно заповед във връзка с масиви от данни, за целите на прегледа трябва да бъде оправдан с оглед на оперативната цел (оперативните цели). Както е обяснено от органите на Обединеното кралство, това означава, че практическите условия и ред за прегледа трябва да бъдат оценени от министъра още на етапа на издаване на заповедта, като се предоставят достатъчно подробности, за да бъдат изпълнени законоустановените задължения по член 152 и член 193 от ЗПР от 2016 г. ([373]). Подробностите, предоставени на министъра във връзка с тези условия и ред, трябва да включват например информация (ако е приложимо) за това как механизмите за филтриране може да се променят в периода на действие на заповедта ([374]). За повече подробности относно процеса и гаранциите, прилагани на етапите на филтриране и преглед, вж. съображение 229 по-долу.

([365]) Член 136, параграф 4 от ЗПР от 2016 г. Според обясненията, предоставени от правителството на Обединеното кралство, прихващане в голям обем може да се извършва например за установяване на неизвестни досега заплахи за националната сигурност на Обединеното кралство чрез филтриране и анализ на прихванатите материали с цел да се установят съобщения с разузнавателна стойност (Обяснителна рамка на Обединеното кралство — раздел H: Национална сигурност, стр. 27—28, вж. бележка под линия 29. Както е обяснено от органите на Обединеното кралство, такива инструменти могат да се използват за установяване на връзки между известни на органите субекти, представляващи интерес за разследването, както и за търсене на следи от дейност на лица, които все още не са известни, но се появяват в хода на разследването, и за установяване на модели на поведение, които може да представляват заплаха за Обединеното кралство.

([366]) В съответствие с член 13, параграф 1 от ЗПР от 2016 г., за да осъществи дадена разузнавателна служба намеса в оборудването, е необходимо разрешение, което се издава чрез заповед съгласно ЗПР от 2016 г., при условие че има „връзка с Британските острови“; вж. съображение 211.

([367]) Член 176 от ЗПР от 2016 г. Със заповед за масова намеса в оборудването не може да се разрешават действия, които биха представлявали (освен ако не са извършени въз основа на законни правомощия) незаконно прихващане (освен по отношение на съхранявана комуникация). Съгласно Обяснителната рамка получената информация може да е необходима за установяване на лица, представляващи интерес за разследването, и обикновено би била подходяща при мащабни операции (Обяснителна рамка, раздел H: Национална сигурност, стр. 28, вж. бележка под линия 29.

([368]) Член 138, параграф 1 и член 178, параграф 1 от ЗПР от 2016 г.

([369]) Член 138, параграф 2 и член 178, параграф 2 от ЗПР от 2016 г.

([370]) Според обясненията, предоставени от органите на Обединеното кралство, една оперативна цел например може да ограничава обхвата на мярката до наличието на заплаха в конкретен географски район.

([371]) Член 142, параграфи 4—10 от ЗПР от 2016 г.

([372]) High Court of Justice, Liberty, [2019] EWHC 2057 (Admin), т. 167.

([373]) В член 152 и член 193 от ЗПР от 2016 г. са предвидени следните изисквания: а) подборът за преглед да се извършва само за оперативните цели, посочени в заповедта, б) подборът за преглед да е необходим и пропорционален при всички обстоятелства, и в) подборът за преглед да не нарушава забраната за подбор на материали и да не включва комуникация изпратена от или предназначена за лица, за които се знае, че по това време са на Британските острови.

([374]) Вж. параграф 6.6 от Кодекса за поведение относно прихващането на комуникация, вж. бележка под линия 278.

(223) Упражняването на правомощие във връзка с масиви от данни може да бъде разрешено само ако е пропорционално на това, което се цели да бъде постигнато ([375]). Както е посочено в Кодекса за поведение относно прихващането [на комуникация], всяка оценка на пропорционалността предполага „да се намери баланс между сериозността на намесата в личния живот (и другите съображения, посочени в член 2, параграф 2) и необходимостта от дейността от гледна точка на разследването, оперативната дейност или способностите. Разрешеното действие следва да предлага реална възможност за постигане на очакваната полза и не следва да е непропорционално или произволно“ ([376]). Както вече беше споменато, това на практика означава, че проверката на пропорционалността се основава на преценка дали е намерен баланс между това, което се цели да бъде постигнато („оперативна цел/и“), и наличните технически възможности (напр. целево прихващане или масово прихващане, намеса в оборудването, събиране на комуникационни данни), като се дава предпочитание на средствата, които предполагат най-малка намеса (вж. съображения 181 и 182 по-горе). Когато за целта е подходяща повече от една мярка, трябва да се предпочитат средствата, които предполагат по-малка намеса.

(224) Допълнителна гаранция за оценка на пропорционалността на исканата мярка се осигурява от факта, че министърът трябва да получи съответната информация, необходима, за да извърши правилно оценката. По-конкретно съгласно Кодекса за поведение относно прихващането на комуникация и Кодекса за поведение относно намесата в оборудването подадената от съответния орган молба трябва да съдържа обща информация за молбата, описание на комуникацията, която ще бъде прихваната, и операторите на далекосъобщителни мрежи, които са длъжни да окажат съдействие, описание на действията, за които се иска разрешение, оперативните цели и обосновка на необходимостта и пропорционалността на действията ([377]).

(225) В заключение и най-важно, решението на министъра да издаде заповедта трябва да бъде одобрено от независим съдебен комисар, който проверява оценката на необходимостта и пропорционалността на предложената мярка, като използва същите принципи, които биха били използвани от съд при жалба по линия на съдебния контрол ([378]). Съдебният комисар прави преглед на заключенията на министъра по отношение на това дали заповедта е необходима и дали действията са пропорционални с оглед на принципите, определени в член 2, параграф 2 от ЗПР от 2016 г. (общи задължения във връзка с неприкосновеността на личния живот). Съдебният комисар също така прави преглед на заключенията на министъра по отношение на това дали всяка от оперативните цели, посочени в заповедта, е цел, за която е необходим или може да е необходим подбор. Ако съдебният комисар откаже да одобри решението за издаване на заповед, министърът може: i) да приеме решението на съдебния комисар и следователно да не издаде заповедта; или ii) да отнесе въпроса за решаване до комисаря по правомощията за разследване (освен когато комисарят по правомощията за разследване е взел първоначалното решение) ([379]).

ii) *Допълнителни гаранции*

(226) Със ЗПР от 2016 г. са въведени допълнителни ограничения по отношение на срока на валидност, подновяването и изменението на заповед във връзка с масиви от данни. Срокът на валидност на заповедта трябва да е максимум шест месеца и всяко решение за подновяване или изменение (с изключение на незначителни изменения) трябва да бъде одобрено от съдебен комисар ([380]). В Кодекса за поведение относно прихващането на комуникация и в Кодекса за поведение относно намесата в оборудването се посочва, че промяната в оперативните цели на заповедта се смята за сериозно изменение на заповедта ([381]).

([375]) Член 138, параграф 1, букви b) и c) и член 178, букви b) и c) от ЗПР от 2016 г.

([376]) Параграф 4.10 от Кодекса за поведение относно прихващането на комуникация, вж. бележка под линия 278.

([377]) Кодекс за поведение относно прихващането на комуникация, параграф 6.20, вж. бележка под линия 278, и Кодекс за поведение относно намесата в оборудването, параграф 6.13, вж. бележка под линия 348.

([378]) Член 138, параграф 1, буква g) и член 178, параграф 1, буква f) от ЗПР от 2016 г. Предварителното разрешение от независим орган беше определено по-специално от Европейския съд по правата на човека като важна предпазна мярка срещу злоупотреби в контекста на масовото прихващане. Европейски съд по правата на човека (голям състав), Big Brother Watch и други/Обединено кралство (вж. бележка под линия 269 по-горе), точки 351 и 352. Важно е да се има предвид, че това решение се отнася до предишната правна уредба (ЗУПР от 2000 г.), която не съдържа някои от гаранциите (включително предварително разрешение от независим съдебен комисар), въведени със ЗПР от 2016 г.

([379]) Член 159, параграфи 3 и 4 от ЗПР от 2016 г.

([380]) Членове 143—146 и членове 184—188 от ЗПР от 2016 г. В случай на неотложност министърът може да направи изменението без одобрение, но трябва да уведоми комисаря и комисарят трябва да реши дали да одобри или да откаже изменението (член 147 от ЗПР от 2016 г.). Заповедта трябва да бъде отменена, когато вече не е необходима или пропорционална, или когато прегледът на прихванатото съдържание, метаданни или други данни, получени по силата на заповедта, вече не е необходим за нито една от оперативните цели, посочени в заповедта (член 148 и член 189 от ЗПР от 2016 г.).

([381]) Кодекс за поведение относно прихващането на комуникация, параграфи 6.44—6.47, вж. бележка под линия 278, и Кодекс за поведение относно намесата в оборудването, параграф 6.48, вж. бележка под линия 348.

(227) Подобно на предвиденото по отношение на целевото прихващане, в част 6 от ЗПР от 2016 г. се предвижда, че министърът трябва да се увери, че са налице договорености, които осигуряват гаранции за съхраняването и разкриването на материалите, получени по силата на заповедта ([382]), както и за разкриването в чужбина ([383]). По-специално съгласно член 150, параграф 5 и член 191, параграф 5 от ЗПР от 2016 г. всяко направено копие на който и да е от материалите, събрани по силата на заповедта, трябва да се съхранява по сигурен начин и да бъде унищожено веднага след отпадането на съответните основания за съхраняването му, а съгласно член 150, параграф 2 и член 191, параграф 2 от ЗПР от 2016 г. броят на лицата, на които се разкрива материалът, и степента на разкриването, предоставянето или копирането на материала трябва да бъдат ограничени до необходимия минимум за постигането на законоустановените цели ([384]).

(228) И накрая, когато материалът, който е прихванат въз основа на заповед за масово прихващане или на заповед за масова намеса в оборудването, трябва да бъде предаден на трета държава („разкриване в чужбина“), в ЗПР от 2016 г. се предвижда, че министърът трябва да се увери, че са налице подходящи договорености, които да гарантират, че в тази трета държава съществуват подобни гаранции за сигурност, съхраняване и разкриване ([385]). Освен това в член 109 от ЗЗД от 2018 г. са определени конкретни изисквания за международното предаване на лични данни от разузнавателни служби към трети държави или международни организации и не се разрешава предаване на лични данни на държава или територия извън Обединеното кралство, или на международна организация, освен ако предаването е необходимо и пропорционално за целите на законоустановените функции на администратора или за други цели, предвидени в член 2, параграф 2, буква а) от Закона за службите за сигурност от 1989 г. или в член 2, параграф 2, буква а) и член 4, параграф 2, буква а) от Закона за разузнавателните служби от 1994 г. ([386]) Важно е да се отбележи, че тези изисквания се прилагат и в случаите, когато се прави позоваване на изключението във връзка с националната сигурност съгласно член 110 от ЗЗД от 2018 г., тъй като в него не е посочен член 109 от ЗЗД от 2018 г. като една от разпоредбите, която може да не се прилага, ако се изисква освобождаване от определени разпоредби с цел опазване на националната сигурност.

(229) След като заповедта бъде одобрена и се събере масивът от данни, данните се подлагат на подбор, преди да бъдат проверени. На етапите на подбор и преглед анализаторът извършва допълнителна проверка на пропорционалността, като определя критериите за подбор въз основа на оперативните цели, включени в заповедта (и на потенциално съществуващите механизми за филтриране). Както е предвидено в член 152 и член 193 от ЗПР, когато издава заповед, министърът трябва да се увери, че са въведени мерки, с които се гарантира, че подборът на материала се извършва само за определените оперативни цели и че е необходим и пропорционален при всякакви обстоятелства. В това отношение органите на Обединеното кралство поясниха, че подборът на материалите, прихващани в масиви, се извършва преди всичко чрез автоматизирано филтриране с цел отхвърляне на данните, които е малко вероятно да представляват интерес за националната сигурност. Филтрите се променят от време на време (когато се променят моделите, видовете и протоколите на интернет трафика) и зависят от технологията и оперативния контекст. След този етап данните могат да бъдат подбирани за преглед само ако са от значение за оперативните цели, посочени в заповедта ([387]). Гаранциите, предвидени в ЗПР от 2016 г. за проверка на събраните материали, се прилагат за всякакъв вид данни (както прихванато съдържание, така и вторични данни) ([388]). В член 152 и член 193 от ЗПР от 2016 г. е предвидена и обща забрана за подбор с цел преглед на материали, отнасящи се до разговори, изпратени от или предназначени за лица, които се намират на Британските острови. Ако органите желаят да проверят такива материали, те следва да подадат искане за заповед за целеви преглед по част 2 и част 4 от ЗПР от 2016 г., която се издава от министъра и се одобрява от съдебен комисар ([389]). Ако дадено лице умишлено подбере за преглед прихванато съдържание в нарушение на изискванията, заложени в законодателството ([390]), то извършва престъпление ([391]).

([382]) Член 156 от ЗПР от 2016 г.

([383]) Член 150 и член 191 от ЗПР от 2016 г.

([384]) Големият състав на Европейския съд по правата на човека по дело Big Brother Watch и др./Обединено кралство (вж. бележка под линия 268 по-горе) потвърди системата от допълнителни гаранции за съхраняването, достъпа и оповестяването, предвидена в ЗУПР от 2000 г., вж. точки 392—394 и 402—405. Същата система от гаранции е предвидена в ЗПР от 2016 г.

([385]) Член 151 и член 192 от ЗПР от 2016 г.

([386]) За повече информация относно тези цели, вж. бележка под линия 312.

([387]) В това отношение в Кодекса относно прихващането на съобщения се посочва следното: „С тези системи за обработване се обработват данни от комуникационните връзки или сигнали, които прихващащият орган е избрал да прихване. След това към трафика по тези връзки и сигнали се прилага филтриране, чиято цел е да се изберат видовете комуникация с потенциална разузнавателна стойност, като същевременно се отхвърли комуникацията, която е най-малко вероятно да има разузнавателна стойност. В резултат на това филтриране, което е различно в различните системи за обработване, значителна част от комуникацията по тези връзки и сигнали ще бъде автоматично отхвърлена. След това може да се извършват допълнителни сложни търсения, за да се извлече допълнителна комуникация, за която е най-вероятно да има най-голяма разузнавателна стойност и която е свързана със законовите функции на агенцията. След това тези комуникации могат да бъдат подбрани за преглед за една или повече от оперативните цели, посочени в заповедта, когато са изпълнени условията за необходимост и пропорционалност. Упълномощените лица могат потенциално да подбират за преглед единствено информация, която не е била изключена при филтрирането“ (Кодекс за поведение относно прихващането на комуникации, параграф 6.6, вж. бележка под линия 278).

([388]) Вж. член 152, параграф 1, букви а) и b) от ЗПР от 2016 г., съгласно който прегледът на двата вида данни (прихванато съдържание и вторични данни) трябва да се извършва само за конкретната цел и да бъде необходим и пропорционален във всички случаи.

([389]) Този вид заповед не се изисква, когато данните, свързани с лица, които се намират на Британските острови, са „вторични данни“ (вж. член 152, параграф 1, буква с) от ЗПР от 2016 г.).

([390]) Членове 152 и 193 от ЗПР от 2016 г.

([391]) Членове 155 и 196 от ЗПР от 2016 г.

(230) Оценката, извършена от анализатора по отношение на подбора на материала, подлежи на последващ контрол от страна на IPC, който оценява спазването на специфичните гаранции, предвидени в ЗПР от 2016 г. за етапа на преглед ([392]) (вж. също съображение 229). IPC трябва да контролира (включително чрез одити, проверки и разследвания) упражняването от публичните органи на правомощията за разследване, посочени в ЗПР от 2016 г. ([393]) В това отношение в Кодекса за поведение относно прихващането [на комуникация] и в Кодекса за поведение относно намесата в оборудването се пояснява, че агенцията трябва да води документация за целите на последващи проверки и одити и в тази документация трябва да се посочва защо е необходим и пропорционален достъпът до материала от упълномощени лица и приложимите оперативни цели ([394]). Например в своя Годишен доклад за 2018 г. Службата на комисаря по правомощията за разследване (IPCO) ([395]) заключава, че документираните от анализаторите обосновки за прегледа на определени материали, събрани масово, отговарят на изискванията стандарт за пропорционалност, тъй като в тях се предоставят достатъчно подробности за причините за „запитванията“ им във връзка с целта, която трябва да бъде постигната ([396]). В своя доклад за 2019 г. IPCO заяви ясно намерението си във връзка правомощията, свързани с масиви от данни, да продължи проверките на масови прихващания, включително подробното разглеждане на превключвателите и критериите за търсене ([397]). IPCO ще продължи също така да следи внимателно и за всеки отделен случай избора на мерки за наблюдение (целеви срещу масови), както при разглеждането на молбите за издаване на заповед по процедурата с „двойна защита“, така и при инспекциите ([398]). Това по-нататъшно наблюдение ще бъде взето предвид в контекста на мониторинга на Комисията на настоящото решение, упоменат в съображения 281—284.

3.3.1.1.4.2. Масово събиране на комуникационни данни

(231) В част 6, глава 2 от ЗПР от 2016 г. са уредени заповедите за масово събиране на данни, с които на адресата се разрешава да изиска от оператор на далекосъобщителна мрежа да разкрие или да получи всякакви комуникационни данни, които операторът притежава. С тези заповеди на органа, подал молбата, се разрешава също да извърши подбор на данните за следващия етап на преглед. Както и при целевото съхраняване и събиране на комуникационни данни (вж. съображение 199), масовото събиране на комуникационни данни също обикновено не касае лични данни на субекти на данни от ЕС, предадени на Обединеното кралство съгласно настоящото решение. Задължението за разкриване на комуникационни данни съгласно част 6, глава 2 от ЗПР от 2016 г. обхваща данни, които се събират от оператори на далекосъобщителни мрежи в Обединеното кралство директно от потребителите на далекосъобщителна услуга ([399]). Този тип „насочено към потребителя“ обработване обикновено не включва предаване въз основа на настоящото решение, т.е. предаване от администратор/обработващ в ЕС към администратор/обработващ в Обединеното кралство.

(232) За целите на изчерпателността обаче условията и гаранциите, уреждащи масовото събиране на комуникационни данни, са описани по-долу.

([392]) Членове 152 и 193 от ЗПР от 2016 г.

([393]) Член 229 от ЗПР от 2016 г.

([394]) Кодекс за поведение относно прихващането на комуникация, параграф 6.74, вж. бележка под линия 278, и Кодекс за поведение относно намесата в оборудването, параграф 6.78, вж. бележка под линия 348.

([395]) IPCO е създадена съгласно член 238 от ЗПР от 2016 г., за да се осигурят на комисаря по правомощията за разследване необходимият персонал, помещения, оборудване и други съоръжения и услуги, необходими за изпълнението на неговите функции (вж. съображение 251).

([396]) В годишния доклад на IPCO за 2018 г. се посочва, че обосновките, документирани от анализаторите от Правителствената централа за комуникации, „отговарят на изисквания стандарт и анализаторите отразяват достатъчно подробно пропорционалността на своите запитванията във връзка с масиви от данни“. Годишен доклад на комисаря по правомощията за разследване за 2018 г., параграф 6.22, вж. бележка под линия 464.

([397]) Годишен доклад на комисаря по правомощията за разследване за 2019 г., параграф 7.6, вж. бележка под линия 463.

([398]) Годишен доклад на комисаря по правомощията за разследване за 2019 г., параграф 10.22, вж. бележка под линия 463.

([399]) Това следва от определението за комуникационни данни в член 261, параграф 5 от ЗПР от 2016 г., съгласно което комуникационните данни се съхраняват или получават от оператор на далекосъобщителна мрежа и или се отнасят до потребителя на телекомуникационна услуга и са свързани с предоставянето на тази услуга, или се съдържат в дадена комуникация, представляват част от нея, добавени са към нея или са свързани логически с нея (вж. също Кодекса за поведение относно масовото събиране на комуникационни данни, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf paragraphs 2.15 to 2.22). Освен това съгласно определението за „оператор на далекосъобщителна мрежа“ в член 261, параграф 10 от ЗПР от 2016 г. операторът на далекосъобщителната мрежа трябва да е лице, което предлага или предоставя далекосъобщителна услуга на лица в Обединеното кралство, или лице, което контролира или предоставя далекосъобщителна система, която (изцяло или частично) се намира в Обединеното кралство или се контролира от Обединеното кралство. От тези определения става ясно, че не могат да бъдат налагани задължения съгласно ЗПР от 2016 г. на оператори на далекосъобщителни мрежи, чието оборудване не се намира в Обединеното кралство или не се контролира от него и които не предлагат или не предоставят услуги на лица в Обединеното кралство (вж. също Кодекса за поведение относно масовото събиране на комуникационни данни, параграф 2.2). Ако абонати от ЕС (независимо дали се намират в ЕС или в Обединеното кралство) използват услуги в Обединеното кралство, всички комуникации във връзка с предоставянето на тези услуги ще се събират директно от доставчика на услуги в Обединеното кралство, а няма да подлежат на предаване от ЕС.

(233) ЗПР от 2016 г. заменя законодателството относно масовото събиране на комуникационни данни, което беше предмет на решението на Съда на Европейския съюз по дело Privacy International. Законодателството, разгледано в производството по това дело, беше отменено и в новия режим се предвиждат специфични условия и гаранции, при които може да бъде разрешена такава мярка.

(234) По-специално, за разлика от предишния режим, при който министърът имаше пълна свобода да разреши мярката ([400]), в ЗПР от 2016 г. е поставено изискването министърът да издава заповед само ако мярката е необходима и пропорционална. Това на практика означава, че следва да има връзка между достъпа до данните и преследваната цел ([401]). По-конкретно министърът трябва да оцени наличието на връзка между исканата мярка и една или повече „оперативни цели“, посочени в заповедта (вж. съображение 219). По отношение на оценката на пропорционалността в съответния кодекс за поведение се посочва, че „министърът трябва да вземе предвид дали това, което се цели да бъде постигнато със заповедта, е практически възможно да бъде постигнато с други средства, които предполагат по-малка намеса (член 2, параграф 2, буква а) от закона). Например осигуряване на необходимата информация чрез упражняването на правомощие, което предполага по-малка намеса, като целево събиране на комуникационни данни“ ([402]).

(235) За да извърши такава оценка, министърът ще разчита на информация, която ръководителите на разузнавателните служби ([403]) са длъжни да предоставят в молбите си, като например причините, поради които мярката се счита за необходима за едно от законоустановените основания, и причините, поради които това, което се цели да бъде постигнато, практически не може да бъде постигнато с други средства, които предполагат по-малка намеса ([404]). Освен това оперативните цели ограничават обхвата, за който получените по силата на заповедта данни може да бъдат подбрани за преглед ([405]). Както е посочено в съответния кодекс за поведение, в оперативните цели трябва да бъде формулирано ясно изискване и да се съдържат достатъчно подробности, за да се убеди министърът, че получените данни могат да бъдат подбрани за преглед единствено поради конкретни причини ([406]). В действителност, преди да одобри заповедта, министърът ще трябва да се увери, че са въведени конкретни мерки, с които се гарантира, че за преглед ще бъдат подбрани единствено тези материали, чийто преглед се счита за необходим за оперативна цел и за законоустановена цел, и че тези материали са необходими и пропорционални при всякакви обстоятелства. Това конкретно изискване за предварителна оценка на необходимостта и пропорционалността на критериите, използвани за целите на подбора, отразено в член 158 и в член 172 ([407]) от ЗПР от 2016 г., представлява друга важна новост на режима, въведен със ЗПР от 2016 г., в сравнение със съществувалия преди това режим.

(236) Със ЗПР от 2016 г. също така се въвежда задължението, преди издаването на заповедта за масово събиране на комуникационни данни, министърът да гарантира, че са налице специфични ограничения за сигурността, съхраняването и разкриването на събраните лични данни ([408]). В случай на разкриване в чужбина в този контекст се прилагат и гаранциите, описани в съображение 227, за масово прихващане и масова намеса в оборудването ([409]). В законодателството са определени допълнителни ограничения относно срока на действие ([410]), подновяването ([411]) и изменението на заповедите във връзка с масиви от данни ([412]).

(237) Важен елемент е, че що се отнася до останалите правомощия във връзка с масиви от данни, преди издаването на заповедта министърът трябва да получи одобрението на съдебен комисар ([413]). Това е ключова особеност на режима, въведен със ЗПР от 2016 г.

([400]) В член 94, параграф 1 от Закона за далекосъобщенията (Telecommunication Act) от 1984 г. е предвидено, че министърът може да издава „указания от общ характер, които според него са необходими или целесъобразни в интерес на националната сигурност (...)“ (вж. бележка под линия 451).

([401]) Вж. решението по дело Privacy International, т. 78.

([402]) Вж. параграф 4.11 от Кодекса за поведение относно масовото събиране на комуникационни данни (вж. бележки под линия 399 и 414).

([403]) Заповед за масово събиране на данни може да се иска само от ръководителите на разузнавателните служби, които са: i) генералният директор на Службата за сигурност; ii) началникът на Службата за тайно разузнаване; или iii) директорът на Правителствената централа за комуникации (вж. член 158 и член 263 от ЗПР от 2016 г.).

([404]) Параграф 4.5 от Кодекса за поведение относно масовото събиране на комуникационни данни (вж. бележка под линия 399).

([405]) Съгласно член 161 от ЗПР от 2016 г. оперативните цели, посочени в заповедта, трябва да бъдат упоменати в списък, поддържан от ръководителите на разузнавателните служби („списъкът с оперативни цели“), като цели, които според тях представляват оперативни цели, за които комуникационните данни, получени по силата на заповеди за масово събиране на данни, може да подлежат на подбор за целите на прегледа.

([406]) Параграф 6.6 от Кодекса за поведение относно масовото събиране на комуникационни данни (вж. бележка под линия 399).

([407]) Съгласно член 172 от ЗПР от 2016 г. трябва да бъдат въведени специфични гаранции за етапа на филтриране и подбор на масивите от данни за целите на прегледа. Освен това преднамереният преглед в нарушение на тези гаранции представлява престъпление (вж. член 173 от ЗПР от 2016 г.).

([408]) Член 171 от ЗПР от 2016 г.

([409]) Член 171, параграф 9 от ЗПР от 2016 г.

([410]) Член 162 от ЗПР от 2016 г.

([411]) Член 163 от ЗПР от 2016 г.

([412]) Членове 164—166 от ЗПР от 2016 г.

([413]) Член 159 от ЗПР от 2016 г.

(238) Комисарят по правомощията за разследване осъществява последващ контрол върху процедурата за преглед на масово събраните материали (комуникационните данни) (вж. съображение 254 по-долу). В това отношение със ЗПР от 2016 г. е въведено изискването, преди да подбере данните за преглед, анализаторът от разузнаването, който извършва прегледа, да запише причината, поради която предложеният преглед е необходим и пропорционален за определена оперативна цел ([414]). По отношение на практиката на Правителствената централа за комуникации и MI5 в годишния доклад на IPCO за 2019 г. се отбелязва, че „решаващата роля на масовото събиране на комуникационни данни за спектъра от дейности, провеждани в Правителствената централа за комуникации, е добре отразена в документацията по случаите, която проверихме. Разгледахме естеството на исканите данни и заявените потребности за целите на разузнаването и се уверихме, че документацията показва, че подходът е необходим и пропорционален ([415]). Обосновките, документирани от MI5, бяха с добро качество и отговаряха на принципите на необходимост и пропорционалност“ ([416]).

3.3.1.1.4.3. Съхраняване и преглед на масиви от лични данни

(239) Със заповедите за масиви от лични данни ([417]) разузнавателните служби се оправомощават да съхраняват и преглеждат набори от данни, които съдържат лични данни, свързани с редица лица. Според обясненията, предоставени от органите на Обединеното кралство, анализът на такива набори от данни може да бъде „единственият начин UKIC да продължи разследването и да идентифицира терористи въз основа на много ограничени разузнавателни данни или когато комуникацията между тях е умишлено скрита“ ([418]). Съществуват два вида заповеди: „групови заповеди за масиви от лични данни“ ([419]), които се отнасят за определена категория набори от данни, т.е. набори от данни, които са сходни по своето съдържание и по предложения начин на използването им и пораждат сходни съображения по отношение например на степента на намеса и чувствителността и пропорционалността на тяхното използване, поради което министърът може да разгледа необходимостта и пропорционалността на получаването на всички данни от съответната група наведнъж. Например груповата заповед за масиви от лични данни може да обхваща набори от данни за пътуване, които са свързани с подобни маршрути ([420]). „Заповедите за конкретни масиви от лични данни“ ([421]) се отнасят за един конкретен набор от данни, като например набор от данни, съдържащ нов или необичаен тип информация, който не попада в обхвата на съществуваща групова заповед за масиви от лични данни, или набор от данни, който се отнася до конкретни видове лични данни ([422]) и поради това са необходими допълнителни гаранции ([423]). Разпоредбите на ЗПР от 2016 г., свързани с масивите от лични данни, дават възможност такива набори от данни да бъдат преглеждани и съхранявани само когато това е необходимо и пропорционално ([424]) и в съответствие с общите задължения, свързани с неприкосновеността на личния живот ([425]).

(240) По отношение на правомощието за издаване на заповед за масиви от лични данни се прилага процедурата с „двойна защита“: оценката на необходимостта и пропорционалността на мярката се извършва първо от министъра, а след това от съдебния комисар ([426]). Министърът е длъжен да вземе предвид естеството и обхвата на искания тип заповед, категорията на съответните данни и броя на отделните масиви от лични данни, които може да попаднат в обхвата на конкретния тип заповед ([427]). Също така, както е посочено в Кодекса за поведение относно съхраняването и използването на масиви от лични данни от разузнавателните служби, трябва да се води подробна документация и тя подлежи на одит от страна на IPC ([428]). Съхраняването и прегледът на масиви от лични данни извън ограниченията, предвидени в ЗПР от 2016 г., е престъпление ([429]).

([414]) Годишен доклад на IPCO за 2019 г., параграф 8.6, вж. бележка под линия 463.
([415]) Годишен доклад на IPCO за 2019 г., параграф 10.4, вж. бележка под линия 463.
([416]) Годишен доклад на IPCO за 2019 г., параграф 8.37, вж. бележка под линия 463.
([417]) Член 200 от ЗПР от 2016 г.
([418]) Вж. Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална сигурност, стр. 34, вж. бележка под линия 29.
([419]) Член 204 от ЗПР от 2016 г.
([420]) Параграф 4.7 от Кодекса за поведение относно съхраняването и използването на масиви от лични данни от разузнавателните служби, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf
([421]) Член 205 от ЗПР от 2016 г.
([422]) Като например чувствителни лични данни, вж. член 202 от ЗПР от 2016 г. и Кодекса за поведение относно съхраняването и използването на масиви от лични данни от разузнавателните служби, параграфи 4.21 и 4.12, вж. бележка под линия 469.
([423]) Молбата за заповед за конкретни масиви от лични данни трябва да бъде разгледана от министъра индивидуално, т.е. по отношение на един конкретен набор от данни. Съгласно член 205 от ЗПР разузнавателната служба трябва да включи в молбата си за заповед за конкретен масив от лични данни подробно обяснение на естеството и обхвата на въпросния материал и списък на „оперативните цели“, за които съответната разузнавателна служба желае да прегледа масива от лични данни (когато разузнавателната служба иска заповед за съхраняване и преглед, а не само за съхраняване). Когато издава групови заповеди за масиви от лични данни, министърът разглежда цялата категория набори от данни наведнъж.
([424]) Членове 204 и 205 от ЗПР от 2016 г.
([425]) Член 2 от ЗПР от 2016 г.
([426]) Член 204 и член 205 от ЗПР от 2016 г.
([427]) Кодекс за поведение относно съхраняването и използването на масиви от лични данни от разузнавателните служби, параграф 5.2, вж. бележка под линия 420.
([428]) Кодекс за поведение относно съхраняването и използването на масиви от лични данни от разузнавателните служби, параграфи 8.1—8.15, вж. бележка под линия 420.
([429]) Вж. Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална сигурност, стр. 34, вж. бележка под линия 29.

3.3.2. *По-нататъшно използване на събраната информация*

(241) Личните данни, обработвани в съответствие с част 4 от ЗЗД от 2018 г., не трябва да се обработват по начин, който е несъвместим с целта, за която са събрани ([430]). В ЗЗД от 2018 г. е предвидено, че администраторът може да обработва данните за друга цел, различна от тази, за която са били събрани, когато тази цел е съвместима с първоначалната цел и при условие че администраторът е оправомощен по закон да обработва данните и обработването е необходимо и пропорционално ([431]). Освен това в Закона за службите за сигурност от 1989 г. и в Закона за разузнавателните служби от 1994 г. се уточнява, че ръководителите на разузнавателните служби са длъжни да гарантират, че не се получава или разкрива информация, освен доколкото е необходимо за правилното изпълнение на функциите на службата или за други ограничени и конкретни цели, изброени в съответните разпоредби ([432]).

(242) Освен това в член 109 от ЗЗД от 2018 г. са определени конкретни изисквания за международното предаване на лични данни от разузнавателни служби към трети държави или международни организации. Съгласно тази разпоредба не се разрешава предаване на лични данни на държава или територия извън Обединеното кралство, или на международна организация, освен ако предаването е необходимо и пропорционално за целите на законоустановените функции на администратора или за други цели, предвидени в член 2, параграф 2, буква а) от Закона за службите за сигурност от 1989 г. или в член 2, параграф 2, буква а) и член 4, параграф 2, буква а) от Закона за разузнавателните служби от 1994 г. ([433]). Важно е да се отбележи, че тези изисквания се прилагат и в случаите, когато се прави позоваване на изключението във връзка с националната сигурност съгласно член 110 от ЗЗД от 2018 г., тъй като в него не е посочен член 109 от ЗЗД от 2018 г. като една от разпоредбите, която може да не се прилага, ако се изисква освобождаване от определени разпоредби с цел опазване на националната сигурност.

(243) Освен това, както беше подчертано от ICO в нейните насоки относно обработването на лични данни от разузнавателните служби, в допълнение към гаранциите, предвидени в част 4 от ЗЗД от 2018 г., разузнавателната служба, когато обменя данни с разузнавателен орган на трета държава, също е обект на гаранции, предвидени в други приложими към тях законодателни мерки, за да се гарантира, че личните данни се получават, споделят и обработват законосъобразно и отговорно ([434]). И накрая, в ЗПР от 2016 г. са предвидени допълнителни гаранции във връзка с предаването на трета държава на материали, събрани чрез целево прихващане ([435]), целева намеса в оборудването ([436]), масово прихващане ([437]), масово събиране на комуникационни данни ([438]) и масова намеса в оборудването ([439]) (така нареченото „разкриване в чужбина“). По-специално органът, който издава заповедта, трябва да се увери, че са налице договорености, които гарантират, че третата държава, която получава данните, ограничава броя на лицата, които виждат материалите, степента на разкриване и броя на копията, които се правят от който и да е материал, до необходимия минимум за разрешените цели, определени в ЗПР от 2016 г. ([440]).

3.3.3. *Надзор*

(244) Надзор върху достъпа на правителството за цели, свързани с националната сигурност, се упражнява от редица различни органи. Комисарят по информацията контролира обработването на лични данни с оглед на ЗЗД от 2018 г. (за повече информация относно независимостта, ролята по отношение на назначаването и правомощията на комисаря вж. съображения 85—98), а независим и съдебен надзор върху упражняването на правомощията за разследване по

([430]) Член 87, параграф 1 от ЗЗД от 2018 г.

([431]) Член 87, параграф 3 от ЗЗД от 2018 г. Въпреки че администраторите могат да бъдат освободени от този принцип в съответствие с член 110 от ЗЗД от 2018 г., доколкото такова изключение е необходимо за защита на националната сигурност, то трябва да се оценява за всеки отделен случай и може да се използва единствено доколкото прилагането на конкретна разпоредба би имало отрицателни последици за националната сигурност (вж. съображение (132)). Удостоверенията за национална сигурност за разузнавателните служби на Обединеното кралство (достъпни на следния адрес: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) do not cover Section 87(3) of the DPA 2018. Освен това, тъй като всяко обработване за различна цел трябва да бъде разрешено от закона, разузнавателните служби трябва да имат ясно правно основание за по-нататъшното обработване.

([432]) За повече информация относно тези цели, вж. бележка под линия 312.

([433]) Вж. бележка под линия 312.

([434]) Насоки на ICO относно обработването на лични данни от разузнавателните служби (вж. бележка под линия 161).

([435]) Член 54 от ЗПР от 2016 г.

([436]) Член 130 от ЗПР от 2016 г.

([437]) Член 151 от ЗПР от 2016 г.

([438]) Член 171, параграф 9 от ЗПР от 2016 г.

([439]) Член 192 от ЗПР от 2016 г.

([440]) Договореностите трябва да включват мерки, с които се осигурява, че всяко копие, направено от който и да е от тези материали, се съхранява по сигурен начин за срока на неговото съхраняване. Материалите, получени по силата на заповед, и всяко копие, направено от който и да е от тези материали, трябва да бъдат унищожени, когато съответните основания за съхраняването им отпаднат (вж. член 150, параграф 2, член 150, параграф 5 и член 151, параграф 2 от ЗПР от 2016 г.). Следва да се отбележи, че подобни гаранции, предвидени в предходната правна уредба (ЗУПР от 2000 г.), са били установени в съответствие с изискванията на Европейския съд по правата на човека за споделяне на материали, получени чрез масово прихващане, с чужди държави или международни организации (Европейски съд по правата на човека (голям състав), Big Brother Watch и др./Обединено кралство (вж. бележка под линия 279 по-горе), точки 362 и 399).

ЗПР от 2016 г. се осигурява от IPC. IPC контролира упражняването на правомощията за разследване по ЗПР от 2016 г. както от правоприлагащите органи, така и от органите за национална сигурност. Политическият надзор се осигурява от Парламентарната комисия за разузнавателните служби.

3.3.3.1. Контрол съгласно част 4 от ЗЗД

(245) Обработването на лични данни, извършвано от разузнавателните служби съгласно част 4 от ЗЗД от 2018 г., се надзирава от комисаря по информацията ([441]).

(246) 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, провеждане на разследвания и др.

(247) Що се отнася до част 3 от ЗЗД от 2018 г., комисарят има правомощията 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 ([442]). 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 ([443]).

(248) 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, правомощията за влизане и проверка, както и правилата относно нарушенията ([444]). Както е обяснено в съображение 126, тези изключения се прилагат само ако е необходимо и пропорционално и въз основа на анализа на всеки отделен случай.

(249) ICO и разузнавателните служби на Обединеното кралство подписаха меморандум за разбирателство ([445]), 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 прилагането на освобождаване, свързано с националната сигурност, е направено законосъобразно. Отговорите на запитвания, отправени от ICO в контекста на разглеждането на индивидуални жалби, трябва да бъдат дадени в срок от 20 работни дни от съответната разузнавателна агенция, 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 ([446]).

([441]) Член 116 от ЗЗД от 2018 г.

([442]) Съгласно точка 2 от приложение 13 към 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 допълнителни подробности относно изпълнителните и наказателните постановления вж. съображение 92).

([443]) Съгласно член 147, параграф 6 от ЗЗД от 2018 г. комисарят по информацията не може да изпраща ревизионно постановление до орган, посочен в член 23, параграф 3 от Закона за свободата на информацията от 2000 г. Това включва Службата за сигурност (MI5), Службата за тайно разузнаване (MI6) и Правителствената централа за комуникации.

([444]) 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).

([445]) Меморандум за разбирателство между Службата на комисаря по информацията и разузнавателната общност на Обединеното кралство, вж. бележка под линия 165.

([446]) 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).

3.3.3.2. Надзор на упражняването на правомощията за разследване съгласно ЗПР от 2016 г.

(250) Съгласно част 8 от ЗПР от 2016 г. надзорът над упражняването на правомощията за разследване се осъществява от комисаря по правомощията за разследване (IPC). IPC се подпомага от други съдебни комисари, които заедно се наричат съдебни комисари ([447]). В ЗПР от 2016 г. се определят гаранциите, които защитават независимостта на съдебните комисари. От съдебните комисари се изисква да заемат или да са заемали висша съдебна длъжност (т.е. трябва да са или да са били членове на най-висшите съдилища) ([448]) и, като всеки член на съдебната власт, те са независими от правителството ([449]). Съгласно член 227 от ЗПР от 2016 г. министър-председателят назначава IPC и толкова съдебни комисари, колкото счита за необходимо. Всички комисари, независимо дали са настоящи или бивши членове на съдебната власт, могат да бъдат назначавани само въз основа на съвместна препоръка от трите главни съдии за Англия и Уелс, Шотландия и Северна Ирландия и лорд-канцлера ([450]). Министърът трябва да осигури на IPC персонал, помещения, оборудване и други съоръжения и услуги ([451]). Мандатът на комисарите е три години и те могат да бъдат преназначавани ([452]). Съдебните комисари могат да бъдат отстранявани от длъжност единствено при строги условия, налагащи висок праг: или от министър-председателя при специфичните обстоятелства, изброени изчерпателно в член 228, параграф 5 от ЗПР от 2016 г. (напр. несъстоятелност или лишаване от свобода), или ако всяка от камарите на Парламента приеме решение за одобряване на отстраняването ([453]).

(251) IPC и съдебните комисари се подпомагат в изпълнението на задълженията си от Службата на комисаря по правомощията за разследване (IPCO). Персоналът на IPCO включва екип от инспектори, вътрешни служители с правен и технически опит и Технически консултативен комитет, който предоставя експертни съвети. Както за отделните съдебни комисари, независимостта на IPCO е защитена. IPCO е „несвързан орган“ на Министерството на вътрешните работи, т.е. получава финансиране от Министерството на вътрешните работи, но изпълнява функциите си независимо ([454]).

(252) Основните функции на съдебните комисари са посочени в член 229 от ЗПР от 2016 г. ([455]). По-специално съдебните комисари имат широко правомощие за предварително одобрение, което е част от гаранциите, въведени в правната уредба на Обединеното кралство със ЗПР от 2016 г. Заповедите във връзка с целево прихващане, намеса в оборудването, масиви от лични данни, масово събиране на комуникационни данни, както и постановленията за съхраняване на данни за комуникацията трябва да бъдат одобрени от съдебни комисари ([456]). IPC също така трябва винаги да разрешава предварително събирането на комуникационни данни за целите на правоприлагането ([457]). Ако комисар откаже да одобри заповед, министърът може да обжалва отказа пред комисаря по правомощията за разследване, чието решение е окончателно.

([447]) В съответствие с член 227, параграфи 7 и 8 от ЗПР от 2016 г. комисарят по правомощията за разследване е съдебен комисар, а комисарят по правомощията за разследване и другите съдебни комисари се наричат заедно съдебни комисари. Понастоящем има 15 съдебни комисари.

([448]) Съгласно член 60, параграф 2 от част 3 от Закона за конституционната реформа от 2005 г. „висша съдебна длъжност“ означава длъжност като съдия в някое от следните съдилища: i) Върховния съд; ii) Апелативния съд в Англия и Уелс; iii) Висшия съд в Англия и Уелс; iv) Върховния съд по граждански дела (Court of Session); v) Апелативния съд в Северна Ирландия; vi) Висшия съд в Северна Ирландия; или като апелативен съдия в обикновен съд.

([449]) Независимостта на съдебната власт се основава на установена практика и е широко призната от Закона за наследяване на престола (Act of Settlement) от 1701 г.

([450]) Член 227, параграф 3 от ЗПР от 2016 г. Съдебните комисари трябва да бъдат препоръчани и от комисаря по правомощията за разследване, член 227, параграф 4, буква е) от ЗПР от 2016 г.

([451]) Член 238 от ЗПР от 2016 г.

([452]) Член 227, параграф 2 от ЗПР от 2016 г.

([453]) Процедурата за отстраняване е идентична с процедурата за отстраняване на други съдии в Обединеното кралство (вж. например член 11, параграф 3 от Закона за висшите съдилища (Senior Courts Act) от 1981 г. и член 33 от Закона за конституционната реформа от 2005 г., съгласно които също се изисква решение, прието и от двете камари на Парламента). Към днешна дата нито един съдебен комисар не е бил отстранен от длъжност.

([454]) Независим орган е организация или агенция, която получава финансиране от правителството, но може да действа независимо (за определение и повече информация за несвързаните органи вж. Наръчника на кабинета на министър-председателя за класификация на публичните органи, достъпен на следния адрес: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf, както и първия доклад от сесията 2014—2015 г. на Специалната комисия за публичната администрация на Камарата на общините, достъпен на следния адрес: https://publications.parliament.uk/pa/cm201415/cmselect/cmpubadm/110/110.pdf)

([455]) Съгласно член 229 от ЗПР от 2016 г. съдебният комисар има широки надзорни правомощия, които обхващат и надзора върху съхранението и разкриването на данните, събирани от разузнавателните служби.

([456]) Решенията дали да бъде одобрено решение на министъра за издаване на заповед се вземат от самите съдебни комисари. Ако комисар откаже да одобри заповед, министърът може да обжалва отказа пред комисаря по правомощията за разследване, чието решение е окончателно.

([457]) Когато комуникационните данни се събират за целите на правоприлагането, винаги се изисква разрешението на IPC (член 60A от ЗПР от 2016 г.). Когато комуникационните данни се получават за целите на националната сигурност, разрешението може да бъде дадено от IPC или, като алтернатива, от специално определен висш служител на съответния публичен орган (вж. член 61 и член 61A от ЗПР от 2016 г. и съображение 203).

(253) Специалният докладчик на ООН за правото на неприкосновеност на личния живот силно приветства създаването на длъжността „съдебен комисар“ със ЗПР от 2016 г., тъй като „всички по-чувствителни или свързани с намеса искания за провеждане на наблюдение трябва да бъдат разрешавани както от министър, така и от Службата на комисаря по правомощията за разследване“. По-специално той подчертава, че „този елемент на съдебен контрол [чрез функциите на IPC], подпомаган от по-добре осигурен с ресурси екип от опитни инспектори и експерти в областта на технологиите, е една от най-важните нови гаранции, въведени със ЗПР“, която заменя съществувалата по-рано фрагментирана система от надзорни органи и допълва ролята на парламентарната Комисия по разузнаване и сигурност и на Трибунала за правомощията за разследване“ ([458]).

(254) Освен това IPC има правомощията да осъществява последващ контрол на упражняването на правомощията за разследване съгласно ЗПР от 2016 г. ([459]), както и някои други правомощия и функции, предвидени в съответното законодателство ([460]). Резултатите от такъв последващ контрол се включват в доклада, който IPC трябва да изготвя ежегодно и да представя на министър-председателя ([461]) и който трябва да бъде публикуван и внесен в Парламента ([462]). Докладът съдържа подходящи статистически данни и информация за упражняването на правомощията за разследване от разузнавателните служби и от правоприлагащите органи, както и за прилагането на гаранциите по отношение на съобщения, които са обект на адвокатска тайна, поверителни журналистически материали и източници на журналистическа информация, и информация за предприетите мерки и оперативните цели, използвани в контекста на заповеди във връзка с масиви от данни. И накрая, в годишния доклад на IPCO се посочва в коя област са дадени препоръки на публичните органи и как тези препоръки са били отразени ([463]).

(255) Съгласно член 231 от ЗПР от 2016 г., ако узнае за грешка от значение, допусната от публични органи при упражняването на техните правомощия за разследване, IPC трябва да уведоми заинтересованото лице, когато смята, че грешката е сериозна и че е в обществен интерес лицето да бъде информирано ([464]). По-специално в член 231 от ЗПР от 2016 г. е посочено, че когато уведомява лице за грешка, IPC трябва да предостави информация за всяко право на това лице да внесе иск пред Трибунала за правомощията за разследване, както и да предостави такива подробности, каквито комисарят сметне за необходими за упражняването на тези права и по отношение на които смята, че е в обществен интерес те да бъдат разкрити ([465]).

([458]) Заключително изявление на специалния докладчик за правото на неприкосновеност на личния живот в края на неговата мисия в Обединеното кралство Великобритания и Северна Ирландия (вж. бележка под линия 281).

([459]) Член 229 от ЗПР от 2016 г. Правомощията на съдебния комисар, свързани с разследването и информация, са посочени в член 235 от ЗПР от 2016 г.

([460]) Тези правомощия включват мерки за наблюдение по ЗУПР от 2000 г., упражняване на функции по част 3 от Закона за полицията от 1997 г. (разрешаване на действия по отношение на имущество) и упражняване от министъра на функции съгласно членове 5—7 от Закона за разузнавателните служби от 1994 г. (заповеди за намеса в безжична телеграфия, за влизане и за намеса в имущество (член 229 от ЗПР от 2016 г.).

([461]) Член 230 от ЗПР от 2016 г. IPC може също да изготвя доклади до министър-председателя по своя инициатива по всеки въпрос, свързан с неговите функции. IPC също така трябва да докладва на министър-председателя по негово искане, а министър-председателят може да нареди на IPC да извърши проверка на всяка от функциите на разузнавателните служби.

([462]) Някои части може да бъдат изключени, ако публикуването им би противоречало на националната сигурност.

([463]) Например в годишния доклад на IPCO за 2019 г. (параграф 6.38) се споменава, че на MI5 е било препоръчано да промени политиката си на съхраняване на масиви от лични данни, тъй като следва да възприеме подход, при който се взема предвид пропорционалността на съхраняването за всички полета в съхраняваните масиви от лични данни и за всеки съхраняван масив от лични данни. В края на 2018 г. IPCO не е удовлетворена от изпълнението на тази препоръка и в доклада за 2019 г. е обяснено, че MI5 понастоящем въвежда нова процедура, за да изпълни това изискване. В годишния доклад за 2019 г. (параграф 8.22) се споменава също така, че на Правителствената централа за комуникации са дадени редица препоръки относно документирането на пропорционалността на нейните запитвания във връзка с масиви от данни. В доклада се потвърждава, че към края на 2018 г. са направени подобрения в тази област. Годишен доклад на Службата на комисаря по правомощията за разследване за 2019 г., достъпен на следния адрес: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Освен това всяка инспекция на IPCO на публичен орган завършва с доклад, който се предоставя на органа и включва всички препоръки, произтичащи от тази инспекция. След това IPCO започва всяка последваща инспекция с преглед на всички предишни препоръки от последната инспекция и в новия доклад от инспекцията е отразено дали предишните препоръки са били изпълнени или са били пренесени.

([464]) Дадена грешка се смята за „сериозна“, когато комисарят прецени, че е ощетила в значителна степен засегнатото лице или му е нанесла значителни вреди (член 231, параграф 2 от ЗПР от 2016 г.). През 2018 г. са били докладвани 22 грешки, от които осем са сметнати за сериозни и са довели до уведомяване на заинтересованото лице. Вж. Годишен доклад на Службата на комисаря по правомощията за разследване за 2018 г., приложение C (вж. https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). През 2019 г. за сериозни са били сметнати 14 грешки. Вж. Годишен доклад на комисаря по правомощията за разследване за 2019 г., приложение B, вж. бележка под линия 463.

([465]) В член 231 от ЗПР от 2016 г. се уточнява, че когато уведомява лице за грешка, IPC трябва да предостави такива подробности, каквито сметне за необходими за упражняването на тези права, като взема предвид по-специално степента, до която разкриването на подробностите би противоречало на обществения интерес или би навредило на предотвратяването или разкриването на тежки престъпления, на икономическото благосъстояние на Обединеното кралство или на по-нататъшното изпълнение на функциите на някоя от разузнавателните служби.

3.3.3.3. Парламентарен надзор на разузнавателните служби

(256) Правното основание за парламентарния надзор, упражняван от Комисията по разузнаване и сигурност (ISC), е в Закона за правосъдието и сигурността (Justice and Security Act) от 2013 г. (ЗПС от 2013 г.) ([466]). Със Закона ISC се създава като комисия на Парламента на Обединеното кралство. 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, че ISC има право да провежда разследвания по оперативни въпроси, когато те не са свързани с текущи операции ([467]). Меморандумът за разбирателство, договорен между министър-председателя и ISC ([468]), уточнява подробно елементите, които трябва да се вземат предвид, когато се преценява дали дадена дейност не е част от текуща операция ([469]). Министър-председателят може да поиска от ISC да разследва текущи операции и ISC може да прави преглед на информацията, предоставена доброволно от агенциите.

(257) 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 ([470]). Според обясненията, предоставени от органите на Обединеното кралство, на практика много малко информация не се предоставя на ISC ([471]).

(258) ISC се състои от членове, принадлежащи към двете камари на Парламента и назначени от министър-председателя след консултация с лидера на опозицията ([472]). От ISC се изисква да представя на Парламента годишен доклад относно изпълнението на своите функции и други доклади, които счита за подходящи ([473]). Освен това ISC има право да получава на всеки три месеца списъка с оперативни цели, които се използват за проверка на масиви от получени материали ([474]). Министър-председателят изпраща на ISC копия от извършените от комисаря по правомощията за разследване разследвания, проверки или одити, когато разгледаният в докладите въпрос е от значение за законоустановените правомощия на комисията ([475]). И накрая, комисията може да поиска от IPC да извърши разследване и комисарят трябва да уведоми ISC за решението дали да се извърши такова разследване ([476]).

(259) ISC също така даде своя принос към проекта на ЗПР от 2016 г. и това доведе до редица изменения, които сега са отразени в ЗПР от 2016 г. ([477]). По-специално ISC препоръча да се засили защитата на неприкосновеността на личния живот чрез въвеждане на набор от мерки за защита на неприкосновеността на личния живот, които се прилагат в

([466]) 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.

([467]) Член 2 от ЗПС от 2013 г.

([468]) Меморандум за разбирателство между министър-председателя и ISC, достъпен на следния адрес: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([469]) Меморандум за разбирателство между министър-председателя и ISC, параграф 14, вж. бележка под линия 468.

([470]) Министърът може да наложи вето върху разкриването на информация само на две основания: 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.).

([471]) Вж. Обяснителна рамка на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел H: Национална сигурност, стр. 43, вж. бележка под линия 31.

([472]) 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.

([473]) Докладите и изявленията на Комисията са достъпни онлайн на следния адрес: https://isc.independent.gov.uk/publications/. През 2015 г. ISC публикува доклад относно „Неприкосновеност на личния живот и сигурността: модерна и прозрачна правна уредба“ (вж.: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), в който се разглежда правната уредба на техниките за наблюдение, използвани от разузнавателните служби, и са отправени редица препоръки, впоследствие разгледани и включени в законопроекта за правомощията за разследване, който бе приет — 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

([474]) Членове 142, 161 и 183 от ЗПР от 2016 г.

([475]) Член 234 от ЗПР от 2016 г.

([476]) Член 236 от ЗПР от 2016 г.

([477]) Парламентарна Комисия по разузнаване и сигурност, Доклад относно Законопроекта за правомощията за разследване, достъпен на следния адрес: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

целия спектър от правомощия за разследване ([478]). Комисията също така предложи промени в предвижданите възможности по отношение на намесата в оборудването, големите масиви от лични данни и комуникационните данни и поиска други конкретни изменения, за да се засилят ограниченията и гаранциите при упражняването на правомощия за разследване ([479]).

3.3.4. *Средства за правна защита*

(260) В областта на държавния достъп за цели, свързани с националната сигурност, субектите на данни трябва да имат възможност да заведат иск пред независим и безпристрастен съд, за да получат достъп до своите лични данни или за да бъдат техните лични данни коригирани или изтрити ([480]). Такъв съдебен орган трябва по-специално да има правомощието да приема решения, които са задължителни за разузнавателната служба ([481]). В Обединеното кралство, както е обяснено в съображения 261—271, с редица възможни средства за правна защита на субектите на данни се предоставя възможност да търсят и получават такава правна защита.

3.3.4.1. Механизми за правна защита, предвидени в част 4 от ЗЗД

(261) Съгласно член 165 от ЗЗД от 2018 г. 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 4 от ЗЗД от 2018 г. Комисарят по информацията има правомощието да оценява дали администраторът и обработващият данни спазват ЗЗД от 2018 г., както и да изисква от тях да предприемат необходимите действия. 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 ([482]), да възразят срещу обработването ([483]) и на коригиране или изтриване ([484]).

(262) 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. ([485]). Вредите включват както финансови загуби, така и вреди, които не са свързани с финансови загуби, като например емоционално страдание ([486]).

3.3.4.2. Механизми за правна защита, предвидени в ЗПР от 2016 г.

(263) Физическите лица могат да получат правна защита във връзка с нарушения на ЗПР от 2016 г. от Трибунала за правомощията за разследване.

(264) Трибуналът за правомощията за разследване е създаден със ЗУПР от 2000 г. и е независим от изпълнителната власт ([487]). В съответствие с член 65 от ЗУПР от 2000 г. членовете на този трибунал се назначават от Нейно Величество за срок от пет години. Член на този трибунал може да бъде отстранен от длъжност от Нейно величество след обръщение ([488]) от страна на двете камари на Парламента ([489]).

([478]) Тези общи задължения във връзка с неприкосновеността на личния живот са определени в член 2, параграф 2 от ЗПР от 2016 г., в който се предвижда, че публичният орган, който действа съгласно ЗПР от 2016 г., трябва да вземе предвид дали това, което се цели да бъде постигнато със заповедта, разрешението или постановлението, е практически възможно да бъде постигнато с други средства, които предполагат по-малка намеса, дали нивото на защита, което трябва да се прилага във връзка с всяко получаване на информация по силата на заповедта, разрешението или постановлението, е по-високо поради особената чувствителност на тази информация, обществения интерес от целостта и сигурността на далекосъобщителните системи и пощенските услуги, и всички други аспекти на обществения интерес от защитата на правото на неприкосновеност на личния живот.

([479]) Например по искане на ISC дните, в които заповед „по неотложни причини“ може да бъде в сила, преди съдебният комисар да я одобри, са намалени от пет на три работни дни и на ISC е предоставено правомощието да отнася въпроси за разследване до комисаря по правомощията за разследване.

([480]) Решение по дело Schrems II, т. 194.

([481]) Решение по дело Schrems II, т. 197.

([482]) Член 94, параграф 11 от ЗЗД от 2018 г.

([483]) Член 99, параграф 4 от ЗЗД от 2018 г.

([484]) Член 100, параграф 1 от ЗЗД от 2018 г.

([485]) Съгласно член 169 от Закона за защита на данните от 2018 г. се допускат искове от „лице, което претърпява вреди поради нарушение на изискване на законодателството за защита на данните“. Според информацията, предоставена от органите на Обединеното кралство, на практика е вероятно иск или жалба срещу разузнавателните служби да бъдат подадени до Трибунала за правомощията за разследване, който има широка компетентност и е в състояние да присъди обезщетение за вреди, като предявяването на иск пред него не е свързано с никакви разходи.

([486]) Член 169, параграф 5 от ЗЗД от 2018 г.

([487]) Съгласно приложение 3 към ЗУПР от 2000 г. членовете трябва да имат определен съдебен опит и имат право на преназначаване.

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

([489]) Точка 1, подточка 5 от приложение 3 към ЗУПР от 2000 г.

(265) Съгласно член 65 от ЗУПР от 2000 г. Съдът е подходящият съдебен орган за всяка жалба от лице, пострадало в резултат на действия по ЗПР от 2016 г., по ЗУПР от 2000 г. или в резултат на каквото и да е действие на разузнавателните служби ([490]).

(266) За да предяви иск пред Трибунала за правомощията за разследване („изискване за процесуална легитимация“), съгласно член 65 от ЗУПР от 2000 г. дадено лице трябва да е убедено ([491]), че 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 е било извършено действие от разузнавателна служба“ ([492]). Освен това жалбоподателят трябва да е убеден, че действието е извършено при „подлежащи на обжалване обстоятелства“ ([493]) или „е извършено от или от името на разузнавателни служби“ ([494]). Тъй като по-специално понятието „убедено“ се тълкува доста широко ([495]), завеждането на дело пред този трибунал подлежи на ниски изисквания за процесуална легитимация.

(267) Когато Трибуналът за правомощията за разследване разглежда жалба, подадена до него, той е длъжен да разследва дали лицата, срещу които е отправено обвинение в жалбата, са имали контакт с жалбоподателя, както и да разследва органа, за който се твърди, че е участвал в нарушенията, и дали предполагаемото действие е било извършено ([496]). Когато води дадено производство, за да се произнесе в това производство, Трибуналът трябва да приложи същите принципи, които биха били приложени от съд във връзка с жалба по линия на за съдебния контрол ([497]). Освен това адресатите на заповедите или постановленията по ЗПР от 2016 г. и всяко друго лице, заемащо държавна длъжност, нает от полицията или от комисаря за разследване и проверка на полицията, са длъжни да разкрият пред този трибунал или да му предоставят всички документи и информация, които Трибуналът може да изиска, за да може да упражни своите правомощия ([498]).

(268) Трибуналът за правомощията за разследване трябва да уведоми жалбоподателя дали жалбата е решена в негова полза или не ([499]). 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. Това може да включва заповед за отмяна на заповед или разрешение, както и заповед, с която се изисква унищожаването на всички

([490]) Член 65, параграф 5 от ЗУПР от 2000 г.

([491]) Относно критериите за проверка на това „убеждение“ вж. дело Human Rights Watch/Secretary of State [2016] UKIPTrib15_165-CH, т. 41. По това дело Трибуналът за правомощията за разследване, позовавайки се на съдебната практика на Европейския съд по правата на човека, приема, че подходящият критерий за проверка на заявеното убеждение, че което и да е действие, попадащо в обхвата на член 68, параграф 5 от ЗУПР от 2000 г., е извършено от която и да е разузнавателна служба или от нейно име, е дали има основание за такова убеждение, така че дадено лице да 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 е в състояние да докаже, че поради личното си положение е изложено на риск от такива мерки.

([492]) Член 65, параграф 4, буква а) от ЗУПР от 2000 г.

([493]) Такива обстоятелства се отнасят до действия на публичните органи при упражняване на публична власт (напр. заповед, разрешение/постановление за получаване на комуникация 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 7ЩА 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.).

([494]) 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 Трибунала за правомощията за разследване 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

([495]) Вж. дело *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH. По това дело Трибуналът за правомощията за разследване, позовавайки се на съдебната практика на Европейския съд по правата на човека, 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).

([496]) Член 67, параграф 3 от ЗУПР от 2000 г.

([497]) Член 67, параграф 2 от ЗУПР от 2000 г.

([498]) Член 68, параграфи 6—7 от ЗУПР от 2000 г.

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

записи с информация, получена при упражняване на правомощия, предоставени със заповед, разрешение или постановление, или държана по друг начин от който и да е публичен орган във връзка с което и да е физическо лице ([500]). Съгласно член 67A от ЗУПР от 2000 г. решението на Трибунала може да бъде обжалвано, при условие че бъде допуснато от Трибунала или от съответния въззивен съд.

(269) И накрая, заслужава да се отбележи, че ролята на Съда за разследващите правомощия е разглеждана няколко пъти в контекста на производства пред Европейския съд по правата на човека, особено по делото Kennedy/Обединено кралство ([501]) и по-наскоро по делото Big Brother Watch и др./Обединено кралство ([502]) , по което Съдът заявява, че „по правило Съдът за разследващите правомощия се е доказал като средство за защита, достъпно на теория и на практика, което е в състояние да предложи правна защита на жалбоподателите, които подават жалби както във връзка с конкретни случаи на наблюдение, така и във връзка с общото спазване на конвенцията в режимите за наблюдение“ ([503]).

3.3.4.3. Други налични механизми за правна защита

(270) Както е обяснено в съображения 109—111, средствата за правна защита съгласно Закона за правата на човека от 1998 г. и Европейският съд по правата на човека ([504]) са на разположение и в областта на националната сигурност. С член 65, параграф 2 от ЗУПР от 2000 г. на Трибунала за правомощията за разследване е предоставена изключителна компетентност по отношение на всички искове по Закона за правата на човека във връзка с разузнавателните служби ([505]). 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 Съда вече са предмет на възможността за обжалване пред подходящ висшестоящ съд (в Англия и Уелс, това би бил Апелативният съд); и че Върховният съд наскоро реши, че Съдът по принцип подлежи на съдебен контрол: вж. R (Privacy International)/ Investigatory Powers Tribunal [2019] UKSC 22; [2019] 2 WLR 1219” ([506]).

(271) От гореизложеното следва, че когато правоприлагащите органи или органите за национална сигурност на Обединеното кралство имат достъп до лични данни, попадащи в обхвата на настоящото решение, този достъп се урежда от закони, в които са определени условията, при които може да се осъществи достъпът, и се гарантира, че достъпът до данните и по-нататъшното им използване са ограничени до това, което е необходимо и пропорционално за преследваната цел, свързана с правоприлагането или националната сигурност. Освен това в повечето случаи условие за такъв достъп е предварителното разрешение от съдебен орган, чрез одобряване на заповед или на заповед за представяне, и във всеки случай подлежи на независим надзор. След като публичните органи са осъществили достъп до данните, обработването на данните, включително по-нататъшното им споделяне и по-нататъшното им предаване, е обект на специални гаранции за защита на данните съгласно част 3 от ЗЗД от 2018 г., в която са отразени предоставените от Директива (ЕС) 2016/680 гаранции — по отношение на обработването от правоприлагащите органи, и съгласно част 4 от ЗЗД от 2018 г. — по отношение на обработването от разузнавателни служби. И накрая, субектите на данни се ползват в тази област с ефективни права на административна и правна защита, включително правото да получат достъп до своите данни или правото на коригиране или изтриване на такива данни.

(272) Като се има предвид значението на тези условия, ограничения и гаранции за целите на настоящото решение, Комисията ще следи отблизо прилагането и тълкуването на правилата на Обединеното кралство, уреждащи достъпа на правителството до лични данни. Това ще включва съответните законодателни и регулаторни промени, развитието на съдебната практика, както и дейностите на ICO и други надзорни органи в тази област. Ще бъде обърнато

([500]) Пример за прилагането на тези правомощия е дело Liberty & Others/the Security Service, SIS, GCHQ, [2015] UKIP Trib 13_77-H_2. Трибуналът отсъжда в полза на двама жалбоподатели, тъй като в единия случай комуникацията им е била запазена извън установените срокове, а в другия процедурата по разглеждане не е била спазена, както е предвидено във вътрешните правила на Правителствената централа за комуникации. По първото дело Съдът разпорежда на разузнавателните служби да унищожат комуникацията, която е била съхранена по-дълго от съответния срок. Във втория случай не е издадено разпореждане за унищожаване, тъй като комуникацията не е съхранена.

([501]) Дело Kennedy, вж. бележка под линия 129.

([502]) Европейски съд по правата на човека (голям състав), Big Brother Watch и др./Обединено кралство (вж. бележка под линия 268по-горе), точки 413 - 415.

([503]) Европейски съд по правата на човека, Big Brother Watch, т. 425.

([504]) Както се вижда например от неотдавнашното решение на големия състав на Европейския съд по правата на човека по дело Big Brother Watch и др./Обединено кралство (вж. бележка под линия 279 по-горе), това позволява ефективен съдебен контрол – подобен на този, на който подлежат държавите – членки на ЕС – от страна на международен съд върху спазването на основните права от страна на публичните органи при достъпа до лични данни. Освен това изпълнението на решенията на Европейския съд по правата на човека подлежи на специален надзор от страна на Съвета на Европа.

([505]) В Belhaj и други [2017] UKSC 3 определението за незаконосъобразността на прихващането на материали, които са обект на адвокатска тайна, се основава пряко на член 8 от ЕКПЧ (вж. определение 11).

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

специално внимание и на изпълнението от страна на Обединеното кралство на съответните решения на Европейския съд по правата на човека, включително мерките, посочени в „плановете за действие“ и „докладите за действие“, представени на Комитета на министрите в контекста на надзора за спазване на решенията на Съда.

4. **ЗАКЛЮЧЕНИЕ**

(273) Комисията счита, че ОРЗД на Обединеното кралство и ЗЗД от 2018 г. гарантират ниво на защита на личните данни, предавани от Европейския съюз, което по същество е равностойно на гарантираното от Регламент (ЕС) 2016/679.

(274) 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.

(275) 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, по-специално за целите на правоприлагането и националната сигурност, ще бъде ограничена до строго необходимото за постигане на въпросната законна цел, и че съществува ефективна правна защита срещу подобна намеса.

(276) Поради това, предвид изложените в настоящото решение констатации следва да се вземе решение, че Обединеното кралство осигурява адекватно ниво на защита по смисъла на член 45 от Регламент (ЕС) 2016/679, тълкуван в светлината на Хартата на основните права на Европейския съюз.

(277) 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.

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

(278) 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.

(279) Следователно решение на Комисията относно адекватното ниво на защита, прието съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679, 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 Европейския съюз на администратори или обработващи лични данни в Обединеното кралство може да се извършва, без да е необходимо допълнително разрешение.

(280) Следва да се припомни, че съгласно член 58, параграф 5 от Регламент (ЕС) 2016/679 и както е обяснено от Съда в решението по дело Schrems ([507]), 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 ([508]).

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

([508]) Решение по дело Schrems, т. 65. „В това отношение националният законодател трябва да предвиди правни способи, позволяващи на съответния национален надзорен орган да изложи твърденията за нарушения, които смята за основателни, пред националните юрисдикции, така че ако последните споделят съмненията на органа относно валидността на решението на Комисията, да отправят преюдициално запитване с цел проверка на валидността на решението.“.

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

(281) Съгласно член 45, параграф 4 от Регламент (ЕС) 2016/679 Комисията трябва да осъществява постоянно наблюдение на съответното развитие в Обединеното кралство след приемането на настоящото решение, за да прецени дали то все още осигурява по същество равностойно 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 Европейския съюз и който може да претърпи промени. Във връзка с това ще се обърне специално внимание на практическото прилагане на правилата на Обединеното кралство относно предаването на лични данни на трети държави и на въздействието, което това може да окаже върху нивото на защита на данните, предавани съгласно настоящото решение; ефективността на упражняването на индивидуалните права, включително всяко съответно развитие на законодателството и практиката относно изключенията или ограниченията на тези права (по-специално това, свързано с поддържането на ефективен имиграционен контрол); както и спазването на ограниченията и гаранциите по отношение на правителствения достъп. 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.

(282) За да се улесни този мониторинг, органите на Обединеното кралство следва своевременно да информират Комисията за всяка материалноправна промяна в правния ред на Обединеното кралство, която оказва въздействие върху правната уредба, която е предмет на настоящото решение, както и за всяко развитие на практиките, свързани с обработването на личните данни, оценени в настоящото решение, както по отношение на обработването на лични данни от администраторите и обработващите лични данни съгласно ОРЗД на Обединеното кралство, така и по отношение на ограниченията и гаранциите, приложими относно достъпа на публичните органи до лични данни. Това следва да включва промените по отношение на елементите, посочени в съображение 281.

(283) 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 администратори или обработващи лични данни в 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, или за националната сигурност, включително тези на надзорните органи, не гарантират изискваното ниво на защита.

(284) 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 да информира компетентните органи на Обединеното кралство за това и да поиска предприемането на подходящи мерки в определен разумен срок. 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. Например такава процедура ще бъде задействана в случаите, когато по-нататъшно предаване, включително въз основа на нови наредби относно адекватното ниво на защита, приети от министъра, или международни споразумения, сключени от Обединеното кралство, вече няма да се извършва при гаранциите, осигуряващи непрекъснатост на защитата по смисъла на член 44 от Регламент (ЕС) 2016/679.

(285) 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 93, параграф 2 от Регламент (ЕС) 2016/679, с оглед частично или пълно спиране на действието или отмяна на настоящото решение.

(286) 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.

(287) При надлежно обосновани наложителни причини за спешност Комисията ще използва възможността да приеме, в съответствие с процедурата, посочена в член 93, параграф 3 от Регламент (ЕС) 2016/679, актове за изпълнение с незабавно приложение за спиране на действието, отмяна или изменение на решението.

7. СРОК НА ДЕЙСТВИЕ И ПОДНОВЯВАНЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(288) Комисията трябва да 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 ЕС. Това може по-специално да включва изменения или промени в уредбата за защита на данните, оценена в настоящото решение, както и други релевантни развития.

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

(290) 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 93, параграф 2 от Регламент (ЕС) 2016/679.

8. **ЗАКЛЮЧИТЕЛНИ СЪОБРАЖЕНИЯ**

(291) Европейският комитет по защита на данните публикува становището си ([509]), като то бе взето предвид при изготвянето на настоящото решение.

(292) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден по силата на член 93 от Регламент (ЕС) 2016/679,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

1. За целите на член 45 от Регламент (ЕС) 2016/679 Обединеното кралство осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз към Обединеното кралство в рамките на приложното поле на Регламент (ЕС) 2016/679.

2. Настоящото решение не обхваща лични данни, които се предават за целите на имиграционния контрол в Обединеното кралство или които по друг начин попадат в обхвата на изключението от прилагането на определени права на субекта на данни за целите на поддържането на ефективен имиграционен контрол съгласно параграф 4, точка 1 от приложение 2 към ЗЗД от 2018 г.

Член 2

Когато с цел защита на физическите лица във връзка с обработване на техни лични данни компетентните органи в държавите членки упражняват правомощията си по член 58 от Регламент (ЕС) 2016/679 по отношение на предаването на данни, попадащи в приложното поле, посочено в член 1, съответната държава членка незабавно уведомява Комисията.

Член 3

1. Комисията наблюдава непрекъснато прилагането на правната рамка, на която се основава настоящото решение, включително условията, при които се извършват последващите предавания, условията, при които се упражняват индивидуалните права и при които публичните органи на Обединеното кралство имат достъп до данните, предадени въз основа на настоящото решение, 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.

([509]) Становище 14/2021 относно проекта на решение за изпълнение на Европейската комисия съгласно Регламент (ЕС) 2016/679 относно адекватната защита на личните данни в Обединеното кралство, достъпно на следния адрес: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en.

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, параграф 1.

Член 4

Срокът на действие на настоящото решение изтича на 27 юни 2025 г., освен ако не бъде удължен в съответствие с процедурата, посочена в член 93, параграф 2 от Регламент (ЕС) 2016/679.

Член 5

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 28 юни 2021 година.

За Комисията
Didier REYNDERS
Член на Комисията