2025/2574

23.12.2025 г.

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2025/2574 НА КОМИСИЯТА

от 19 декември 2025 година

за изменение на Решение за изпълнение (ЕС) 2021/1772 на Комисията съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство

(нотифицирано под номер C(2025) 8771)

(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) В Решение за изпълнение (ЕС) 2021/1772 на Комисията ([2]) се стига до заключението, че за целите на член 45 от Регламент (ЕС) 2016/679 Обединеното кралство осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз на Обединеното кралство в рамките на обхвата на посочения регламент ([3]).

(2) При приемането на Решение за изпълнение (ЕС) 2021/1772 Комисията взе предвид, че след края на преходния период, предвиден в Споразумението за оттеглянето на Обединеното кралство Великобритания и Северна Ирландия от Европейския съюз и Европейската общност за атомна енергия ([4]), и след като временната разпоредба по 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 ([5]) престане да се прилага, Обединеното кралство ще приеме и ще прилага нов режим за защита на данните, различен от режима, който е бил в сила, когато е било обвързано от правото на Съюза.

(3) Тъй като имаше вероятност този нов режим да съдържа изменения на уредбата за защита на данните, оценени в Решение за изпълнение (ЕС) 2021/1772, или други съответни промени, беше счетено за целесъобразно да се предвиди, че посоченото решение ще се прилага за срок от четири години, считано от влизането му в сила. Поради това срокът на действие на Решение за изпълнение (ЕС) 2021/1772 беше определен да изтече 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.

([1]) ОВ L 119, 4.5.2016 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

([2]) Решение за изпълнение (ЕС) 2021/1772 на Комисията от 28 юни 2021 г. съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство (ОВ L 360, 11.10.2021 г., стр. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

([3]) Вж. член 1, параграф 1 от Решение за изпълнение (ЕС) 2021/1772. Съгласно член 1, параграф 2 от посоченото решение решението не обхваща лични данни, които се предават за целите на имиграционния контрол на Обединеното кралство или които по друг начин попадат в обхвата на освобождаването от прилагането на определени права на субекта на данни за целите на поддържането на ефективен имиграционен контрол съгласно точка 4, подточка 1 от приложение 2 към Закона за защита на данните на Обединеното кралство от 2018 г.

([4]) ОВ C 384I, 12.11.2019 г., стр. 1.

([5]) ОВ L 149, 30.4.2021 г., стр. 10., ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) За да вземе решение относно евентуално удължаване на срока на действие на Решение за изпълнение (ЕС) 2021/1772, Комисията трябва да прецени дали заключението, че Обединеното кралство осигурява адекватно ниво на защита, продължава да бъде фактически и правно обосновано с оглед на промените, настъпили след приемането на Решение за изпълнение (ЕС) 2021/1772 по отношение на елементите, изброени в член 45, параграф 2 от Регламент (ЕС) 2016/679.

(5) По-специално на 23 октомври 2024 г. правителството на Обединеното кралство внесе в Парламента на Обединеното кралство Закона за данните (използване и достъп) ([6]), с който се предлагат изменения на Общия регламент относно защитата на данните на Обединеното кралство (ОРЗД на Обединеното кралство) и Закона за защита на данните от 2018 г. (ЗЗД от 2018 г.), които са оценени в Решение за изпълнение (ЕС) 2021/1772. На 24 юни 2025 г. Комисията прие Решение за изпълнение (ЕС) 2025/1226 ([7]), с което срокът на действие на Решение за изпълнение (ЕС) 2021/1772 беше удължен с шест месеца до 27 декември 2025 г. Това ограничено във времето техническо удължаване даде възможност на Комисията да завърши оценката си на адекватното ниво на защита на личните данни, осигурено от Обединеното кралство, въз основа на стабилна правна уредба, т.е. след приключване на съответния законодателен процес ([8]).

(6) След приемането на Решение за изпълнение (ЕС) 2021/1772 Комисията наблюдаваше постоянно съответните промени в Обединеното кралство ([9]). В съответствие със съображение 281 от Решение за изпълнение (ЕС) 2021/1772 беше обърнато 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 Решение за изпълнение (ЕС) 2021/1772, 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 Службата на комисаря по информацията и други независими органи бяха използвани за наблюдението от страна на Комисията.

(7) Въз основа на оценката на тези промени, включително измененията в ОРЗД на Обединеното кралство и ЗЗД от 2018 г., въведени със Закона за данните (използване и достъп), Комисията стига до заключението, че Обединеното кралство продължава да 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.

(8) Освен това Комисията заключава, че с оглед на измененията в съответните разпоредби на законодателството на Обединеното кралство ([10]) изключването от приложното поле на Решение за изпълнение (ЕС) 2021/1772 на личните данни, предавани за целите на имиграционния контрол на Обединеното кралство, или на данните, които по друг начин попадат в обхвата на освобождаването по отношение на определени права на субекта на данни за целите на поддържането на ефективен имиграционен контрол („освобождаването във връзка с имиграционния контрол“) съгласно точка 4, подточка 1 от приложение 2 към Закона за защита на данните на Обединеното кралство, вече не е оправдано, както е обяснено в съображение 37 от настоящото решение.

([6]) На разположение на следния адрес: https://bills.parliament.uk/bills/3825/news.

([7]) Решение за изпълнение (ЕС) 2025/1226 на Комисията от 24 юни 2025 г. за изменение на Решение за изпълнение (ЕС) 2021/1772 съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Обединеното кралство (ОВ L, 2025/1226, 26.6.2025 г., ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) Законът за данните (използване и достъп) получи кралско одобрение на 19 юни 2025 г.

([9]) Член 45, параграф 4 от Регламент (ЕС) 2016/679.

([10]) През май 2021 г. Апелативният съд на Англия и Уелс установи, че освобождаването във връзка с имиграционния контрол, формулирано към онзи момент в точка 4, подточка 1 от приложение 2 към Закона за защита на данните на Обединеното кралство, е несъвместимо със законодателството на Обединеното кралство, тъй като законодателната мярка не съдържа конкретни разпоредби за определяне на гаранциите, изброени в член 23, параграф 2 от ОРЗД на Обединеното кралство. За да се съобрази с решението, правителството на Обединеното кралство преразгледа освобождаването във връзка с имиграционния контрол, като прие Наредби от 2022 г. към Закона за защита на данните от 2018 г. (изменение на освобожданията по приложение 2). Преразгледаното освобождаване обаче отново беше оспорено на основание, че не отговаря на всички изисквания по член 23, параграф 2 от ОРЗД на Обединеното кралство. В решение от 11 декември 2023 г. Апелативният съд отново обяви преразгледаното освобождаване във връзка с имиграционния контрол за несъвместимо с член 23, параграф 2 от ОРЗД на Обединеното кралство. За да се съобрази с това решение, правителството на Обединеното кралство прие Наредби от 2024 г. към Закона за защита на данните от 2018 г. (изменение на освобожданията по приложение 2), които влязоха в сила на 8 март 2024 г.

2. СЪОТВЕТНИ ПРОМЕНИ ВЪВ ВРЪЗКА С ПРАВИЛАТА, ПРИЛОЖИМИ КЪМ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

2.1. Уредбата на Обединеното кралство за защита на данните

(9) Към момента на приемането на Решение за изпълнение (ЕС) 2021/1772 правната уредба за защита на личните данни в Обединеното кралство се състоеше от:

— ОРЗД на Обединеното кралство ([11]), включен в правото на Обединеното кралство съгласно Закона от 2018 г. за оттеглянето от Европейския съюз ([12]) и изменен с Наредбите от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Излизане от ЕС) ([13]),

— ЗЗД от 2018 г. ([14]), изменен с Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения.

(10) Въпреки че тези два законодателни акта, които отразяват в голяма степен съответните норми, приложими в рамките на Европейския съюз, продължават да стоят в основата на законодателството в областта на защитата на данните на Обединеното кралство, оттогава те са били обект на ограничени изменения, за да бъде отразен фактът, че Обединеното кралство вече не е обвързано с правото на Европейския съюз.

(11) Първо, със Закона за запазеното право на ЕС (отмяна и реформа) от 2023 г. ([15]) беше пояснено, че след края на 2023 г. общите принципи на правото на Съюза вече не са част от националното законодателство на Обединеното кралство ([16]). Освен това от съдилищата на Обединеното кралство вече не се изисква да тълкуват „асимилираното право“, което не е изменено, наричано по-рано „запазено право на ЕС“, в съответствие с общите принципи на правото на Съюза, като вместо това обаче това право трябва да се тълкува в съответствие с националното право на Обединеното кралство ([17]). Въпреки това „асимилираното право“, което не е изменено, все още трябва да се тълкува от съответните съдилища на Обединеното кралство съгласно съответната съдебна практика на Съда на Европейския съюз отпреди края на преходния период ([18]), както е посочено и в съображение 13 от Решение за изпълнение (ЕС) 2021/1772. ЗЗД от 2018 г. беше изменен със Закона за данните (използване и достъп), за да се изясни въздействието на Закона за запазеното право на ЕС (отмяна и реформа) върху законодателството на Обединеното кралство в областта на защитата на данните. В член 183а, параграф 1 от ЗЗД от 2018 г. например като общо правило се предвижда, че всяко ново законодателство (прието на 20 август 2025 г. или след тази дата), с което се въвеждат нови задължения или правомощия за обработване на лични данни, се счита за подчинено на законодателството на Обединеното кралство за защита на данните. Това означава, че уредбата на Обединеното кралство за защита на данните продължава да има предимство пред другите законодателни актове. Съгласно

([11]) Общият регламент относно защитата на данните, достъпен на следния адрес: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) Със Закона от 2018 г. за оттеглянето от Европейския съюз, достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2018/16/contents, в правото на Обединеното кралство беше включено законодателството на Съюза, пряко приложимо в Обединеното кралство в края на преходния период. Това така наречено „запазено право на ЕС“ включваше Регламент (ЕС) 2016/679 в неговата цялост, заедно със съображенията към него (вж. Обяснителни бележки към Закона от 2018 г. за оттеглянето от Европейския съюз, параграф 83, достъпни на следния адрес: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf). По силата на горепосочения закон запазеното право на ЕС, което не е изменено, трябваше 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“).

([13]) Наредбите от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Излизане от 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, достъпни на следния адрес: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. С Наредбите за защита на данните, неприкосновеността на личния живот и електронните съобщения се изменя Регламент (ЕС) 2016/679, както 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.

([14]) Закон за защита на данните от 2018 г., достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2018/12/contents. Преди оттеглянето на Обединеното кралство от Европейския съюз и по време на преходния период със ЗЗД от 2018 г. бяха установени национални правила в областите, в които това е допустимо съгласно Регламент (ЕС) 2016/679, беше уточнено и ограничено прилагането на правилата на Регламент (ЕС) 2016/679 и беше транспонирана 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, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) На разположение на следния адрес: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) Член 5 от Закона от 2018 г. за оттеглянето от Европейския съюз, изменен със Закона за запазеното право на ЕС (отмяна и реформа).

([17]) Член 5, параграф А2 от Закона от 2018 г. за оттеглянето от Европейския съюз, изменен със Закона за запазеното право на ЕС (отмяна и реформа).

([18]) Член 6, параграфи 3 и 7 от Закона от 2018 г. за оттеглянето от Европейския съюз, изменен със Закона за запазеното право на ЕС (отмяна и реформа).

член 183а, параграф 2, буква b) от ЗЗД от 2018 г. тази презумпция може да не се прилага, ако Парламентът на Обединеното кралство съзнателно реши да включи това изрично в законодателството, като запази парламентарния суверенитет. Освен това в член 186, параграф 2А от ЗЗД от 2018 г. се пояснява, че член 186, параграф 1 от ЗЗД от 2018 г., в който се предвижда, че актовете, с които се забранява или ограничава разкриването на информация, нямат предимство над определени права на защита на данните, не надделява над ограниченията на правата на субектите на данни, изброени в член 186, параграф 3 от ЗЗД от 2018 г. С това се гарантира например, че ограниченията на правата на субектите на данни, определени в ЗЗД от 2018 г., сами по себе си не попадат в обхвата на общото „предимство на защитата на данните“ съгласно член 186, параграф 1 от ЗЗД от 2018 г.

(12) Второ, след приемането на Решение за изпълнение (ЕС) 2021/1772 законодателството в областта на защитата на данните на Обединеното кралство беше изменено посредством Наредбите от 2023 г. за изменение на Закона за защита на данните (основни права и свободи) ([19]). С тези наредби позоваванията на основните права или основните свободи в ОРЗД на Обединеното кралство и ЗЗД от 2018 г. (които преди това бяха определени така, че да обхващат основните права и основните свободи на ЕС ([20]) се определят като позовавания на правата съгласно Европейската конвенция за правата на човека, въведени в националното законодателство на Обединеното кралство със Закона за правата на човека от 1998 г. ([21]). Със Закона за правата на човека от 1998 г. правата, съдържащи се в Европейската конвенция за правата на човека, 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 защитата на личните данни като част от това право) и правото на справедлив съдебен процес ([22]).

(13) Накрая, ОРЗД на Обединеното кралство и ЗЗД от 2018 г. бяха обект на целеви реформи, предвидени в части пета и шеста от Закона за данните (използване и достъп). Въпреки че обхватът на Закона за данните (използване и достъп) надхвърля защитата на личните данни, в него се предвиждат ограничени изменения по отношение на няколко аспекта на режима за защита на данните, например, наред с другото, правилата за обработване на данни за целите на научни изследвания, правните основания за обработване на данни, правилата, свързани с принципа на ограничаване в рамките на целта, и условията за автоматизирано вземане на решения. Освен това със Закона за данните (използване и достъп) се правят изменения в структурата на управление на Службата на комисаря по информацията. След като бъдат приложени, тези мерки ще заменят Службата на комисаря по информацията с нов субект — Комисията по информацията. Ролята и функциите на регулатора като независим надзорен орган по защита на данните в Обединеното кралство ще останат непроменени. Със закона се въвеждат и нови правомощия за правоприлагане за регулатора.

(14) С настоящото решение се оценяват законодателните, регулаторните и други промени, имащи отношение към заключението относно нивото на защита, гарантирано от Обединеното кралство, направено в Решение за изпълнение (ЕС) 2021/1772. Оценката, направена в Решение за изпълнение (ЕС) 2021/1772, продължава да бъде валидна по отношение на онези аспекти на уредбата за защита на данните на Обединеното кралство, които не са били изменени или засегнати от други промени след приемането на Решение за изпълнение (ЕС) 2021/1772.

(15) В следващите раздели подробно са анализирани законодателните, регулаторните и други съответни промени въз основа на стандарта за адекватно ниво на защита, съгласно който Комисията трябва да определи дали въпросната трета държава гарантира ниво на защита, „по същество равностойно“ на осигуреното в рамките на Европейския съюз ([23]). Както бе пояснено от Съда на Европейския съюз, това не изисква установяване на идентично ниво на защита ([24]). 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 ([25]). 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 личните данни и неговото ефективно прилагане, надзор и изпълнение чуждестранната правна система като цяло осигурява необходимото ниво на защита ([26]).

([19]) На разположение на следния адрес: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) Основните права и основните свободи на ЕС бяха запазени в законодателството на Обединеното кралство в член 4 от Закона от 2018 г. за оттеглянето от Европейския съюз, който беше отменен в края на 2023 г. посредством Закона за запазеното право на ЕС (отмяна и реформа).

([21]) Член 2, параграф 3 от Наредбите от 2023 г. за изменение на Закона за защита на данните (основни права и свободи).

([22]) Членове 6, 8, 10 и 13 от ЕКПЧ (вж. също приложение 1 към Закона за правата на човека от 1998 г.).

([23]) Съображение 104 от Регламент (ЕС) 2016/679.

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

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

([26]) 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.

2.1.1. *Определения*

(16) Основните понятия за защита на данните, отразяващи терминологията на Регламент (ЕС) 2016/679, продължават да се прилагат в режима за защита на данните на Обединеното кралство. Тези понятия са оценени в съображение 23 от Решение за изпълнение (ЕС) 2021/1772.

(17) Въпреки че в Закона за данните (използване и достъп) по-голямата част от определенията остават непроменени, с него се въвеждат специфични определения, свързани с обработването на лични данни за научни, исторически и статистически цели, в член 4, параграфи 2, 3, 4 и 5 от ОРЗД на Обединеното кралство. В параграф 2 понятието „обработване за научни цели“ се определя като обработване на лични данни, извършвано за целите на всяко изследване, което с основание може да бъде описано като научно. Изследването може да бъде финансирано с публични или частни средства и може да се провежда като търговска или нетърговска дейност. Отразявайки съдържанието на съображение 159 от Регламент (ЕС) 2016/679, в параграф 3 е предоставен неизчерпателен списък с примери за изследователски дейности, които се определят като преследващи научни цели, включително технологично развитие и демонстрационни дейности, фундаментални научни изследвания и приложни научни изследвания. В параграф 4 се пояснява, че понятието „историческо изследване“ включва генеалогичните изследвания, които също са признати като изследвания за исторически цели в съображение 160 от Регламент (ЕС) 2016/679. И накрая, в параграф 5 обработването за статистически цели се определя като обработване на данни за статистически изследвания или за изготвяне на статистически резултати, при което данните се агрегират до степен, в която вече не представляват лични данни. Освен това обработените данни или получената в резултат на това информация не трябва да се използват за вземане на решения или предприемане на действия, насочени към конкретно лице. Това определение е в съответствие с разбирането за статистически цели, посочено в съображение 162 от Регламент (ЕС) 2016/679.

(18) В заключение, макар че с измененията на член 4 от ОРЗД на Обединеното кралство се добавят специфични определения за обработването на данни за научни, исторически и статистически цели, тези определения са в съответствие с буквата и духа на Регламент (ЕС) 2016/679, както е посочено в гореспоменатите съображения 159, 160 и 162.

(19) Посредством добавянето на параграф 6 към член 4 от ОРЗД на Обединеното кралство със Закона за данните (използване и достъп) се установява и специфична рамка за получаване на съгласие от субекта на данните за обработването на неговите лични данни за научни цели. С много сходни формулировки на тези в съображение 33 от Регламент (ЕС) 2016/679, в което се признава, че в областта на научните изследвания невинаги може да се получи съгласие за обработване с конкретна цел, в новата разпоредба се допускат по-широки форми на съгласие, като се дава възможност на субектите на данни да дадат валидно съгласие дори когато точните цели на изследването не могат да бъдат напълно идентифицирани към момента на събиране на данните, при условие че искането на съгласие е в съответствие с общопризнатите етични стандарти, отнасящи се до конкретната област на изследване. Във всеки случай субектите на данни трябва да имат възможност да дадат съгласие за обработване на личните данни само за определени части от изследването, когато това е възможно.

(20) Накрая, в Закона за данните (използване и достъп) допълнително се уточняват гаранциите, установени преди това в член 89 от ОРЗД на Обединеното кралство и член 19 от ЗЗД от 2018 г., за обработването на данни с цел архивиране в обществен интерес, както и за целите на научни, исторически и статистически изследвания, в нова глава 8A от ОРЗД на Обединеното кралство ([27]). Тези гаранции са подобни на изискваните по член 89 от Регламент (ЕС) 2016/679 и включват изискването за предоставяне на технически и организационни мерки с оглед спазването на принципа на свеждане на данните до минимум.

2.2. **Гаранции, права и задължения**

2.2.1. *Законосъобразност и добросъвестност на обработването*

(21) Съгласно уредбата за защита на данните на Обединеното кралство продължава да се изисква данните да бъдат обработвани по законосъобразен, добросъвестен и легитимен начин, както е оценено в съображения 24—26 от Решение за изпълнение (ЕС) 2021/1772.

([27]) Членове 84A—84D от ОРЗД на Обединеното кралство, въведени с член 86 от Закона за данните (използване и достъп).

(22) Принципите на законосъобразност и добросъвестност и основанията за законосъобразно обработване на лични данни продължават да бъдат 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, както е оценено в Решение за изпълнение (ЕС) 2021/1772. Въпреки че тези разпоредби остават до голяма степен идентични ([28]) със съответните разпоредби в Регламент (ЕС) 2016/679, със Закона за данните (използване и достъп) първо се изменя член 6, параграф 1 от ОРЗД на Обединеното кралство, като се въвежда допълнително законово основание за обработването на лични данни съгласно член 6, параграф 1, буква еа) ([29]). Съгласно тази разпоредба обработването е законосъобразно, ако и доколкото е „необходимо за целите на признат легитимен интерес“. За разлика от правното основание за легитимен интерес съгласно член 6, параграф 1, буква f) от ОРЗД на Обединеното кралство, при нововъведеното правно основание за признат легитимен интерес не се изисква балансиране на легитимните интереси на администратора спрямо интересите или основните права и свободи на субекта на данните във всеки отделен случай, което има за цел да осигури по-голяма правна сигурност на администраторите, които не са публични органи. С нововъведения член 6, параграф 5 от ОРЗД на Обединеното кралство се уточнява, че обработването е необходимо за целите на признат легитимен интерес само ако отговаря на условие в Приложение 1 ([30]), където впоследствие се посочват случаите, в които обработването се счита за необходимо за целите на признат легитимен интерес, например когато то се извършва в отговор на искане, получено от публичен орган, който се нуждае от данните за целите на изпълнението на задача в обществен интерес, за която съществува правно основание, отговарящо на член 6, параграф 3 от ОРЗД на Обединеното кралство, когато обработването е необходимо с оглед защита на националната сигурност, защита на обществената сигурност или за целите на отбраната, за реагиране при извънредна ситуация, за разкриване, разследване или предотвратяване на престъпления или за защита на уязвими лица ([31]).

(23) Въпреки че със Закона за данните (използване и достъп) се разширява списъкът с правни основания за обработване на лични данни, които са на разположение на администратора, при нововъведеното правно основание за признат легитимен интерес съществуват няколко важни ограничения. Първо, признатите легитимни интереси са ограничени до особени случаи, които са изчерпателно изброени в закона. Второ, това правно основание не може да бъде използвано от публичните органи при изпълнението на техните задачи ([32]). Трето, то се отнася само за области, в които има ясен обществен интерес от дейността по обработване (съгласно условията, определени в приложение 1), т.е. когато обработването служи за цели, посочени в член 23 от ОРЗД на Обединеното кралство (съответстващ на член 23 от Регламент (ЕС) 2016/679), и следователно не може да се използва за търговски цели. Четвърто, макар че със Закона за данните (използване и достъп) на министъра (Secretary of State) се предоставя правото да изменя

([28]) За по-голяма яснота със Закона за данните (използване и достъп) в член 6 от ОРЗД на Обединеното кралство се въвежда и нов параграф, където се посочват примери за видове обработване, които могат да се считат за необходими за целите на легитимен интерес по смисъла на член 6, параграф 1, буква f) от ОРЗД на Обединеното кралство. Тези примери (директен маркетинг, вътрешногрупово предаване на данни за административни цели и мрежова и информационна сигурност) са посочени и в съображения 47 и 48 от Регламент (ЕС) 2016/679 като случаи, в които би се считало, че обработването е от законен интерес на администратора.

([29]) Член 70, параграф 2, буква b) от Закона за данните (използване и достъп). Съгласно член 70, параграф 5 от Закона за данните (използване и достъп) беше разширено правото на възражение по член 21 от ОРЗД на Обединеното кралство с разпоредбите на новия член 6, параграф 1, буква еа) от ОРЗД на Обединеното кралство.

([30]) Член 70, параграф 4 от Закона за данните (използване и достъп).

([31]) Вж. приложение 4 към Закона за данните (използване и достъп). Според органите на Обединеното кралство примерите за случаи, при които може да се наложи непублични органи да обработват лични данни с цел предотвратяване или разкриване на престъпления, включват случая на дружество, което узнава за опити за незаконно хакерство спрямо компютърните му системи, или на банка или финансова институция, която узнава за опити за измама с цел откриване на сметка. Обработването на лични данни от непубличен орган може например да бъде необходимо за защитата на националната сигурност или отбрана, когато търговска организация подозира, че онлайн дейността на даден клиент сочи за участие в терористична дейност. Комисарят по информацията работи по конкретни насоки по този въпрос, включително по определението за съответните понятия. Например в тях се посочва, че е вероятно „националната сигурност“ да обхваща сигурността и благосъстоянието на Обединеното кралство като цяло, неговото население, институции и система на управление. Вж. проекта на насоки на комисаря по информацията относно признатия легитимен интерес, публикуван за обществена консултация и достъпен на следния адрес: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Член 6, параграф 1, последна алинея, изменен с член 70, параграф 2, точка c) от Закона за данните (използване и достъп).

списъка в приложение 1 с наредба ([33]), министърът може да издава такава наредба само след като се е консултирал с комисаря по информацията ([34]), и да добавя признат легитимен интерес към този списък само когато обработването е необходимо отново за защитата на цел от обществен интерес, посочена в член 23, параграф 1, букви c)—j) от ОРЗД на Обединеното кралство ([35]). И накрая, както се потвърждава и от насоките на комисаря по информацията ([36]), администраторите, които се позовават на признат легитимен интерес като правно основание, са длъжни да спазват всички други изисквания съгласно ОРЗД на Обединеното кралство, включително да гарантират, че обработването е необходимо и пропорционално за постигане на легитимния интерес.

(24) Второ, със Закона за данните (използване и достъп) в член 6, параграф 3, член 9, параграф 2, буква g) и член 10, параграф 1 от ОРЗД на Обединеното кралство, отразяващи съответните разпоредби на Регламент (ЕС) 2016/679, се пояснява, че основанието за обработването на лични данни, специални категории лични данни и лични данни, свързани с присъди и нарушения, в съответствие със законово задължение или с оглед изпълнение на задача от обществен интерес може да се намира не само в националното право, но и в съответното международно право ([37]). В такива случаи съответното международно право е ограничено съгласно нововъведения член 9A от ОРЗД на Обединеното кралство във връзка с приложение A1 само до едно споразумение, а именно 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, подписано на 3 октомври 2019 г. („Споразумението между Обединеното кралство и САЩ“) ([38]). Предвидените в посоченото споразумение гаранции са оценени в съображения 153—155 от Решение за изпълнение (ЕС) 2021/1772, а тяхното прилагане е анализирано в съображения 87—93 от настоящото решение.

2.2.2. *Обработване на специални категории лични данни*

(25) В уредбата за защита на данните на Обединеното кралство продължават да се предоставят специфични гаранции, когато става въпрос за специални категории данни, както е оценено в съображения 27—42 от Решение за изпълнение (ЕС) 2021/1772.

(26) Както определението за специални категории лични данни, така и специфичните правила, приложими за обработването на тези категории данни съгласно ОРЗД на Обединеното кралство и ЗЗД от 2018 г., остават в сила. Същевременно със Закона за данните (използване и достъп) на министъра се предоставят нови правомощия за изготвяне на наредби с оглед добавяне на специални категории данни, адаптиране на условията, приложими за тяхното използване, и добавяне на нови определения, ако е необходимо ([39]). Важно е да се отбележи, че това не означава, че министърът има правомощия да премахва или изменя съществуващи специални категории данни, нито да променя условията за обработването на тези категории данни ([40]). Така съгласно нововъведеното правомощие за изготвяне на наредби правителството може единствено да добавя нови категории чувствителни данни и да определя условията за обработването на тези категории данни, като целта е да се даде възможност на правителството да реагира на технологичните и обществените промени в бъдеще, когато е необходимо.

(27) Следователно тези изменения не засягат нивото на защита за специалните категории лични данни, определено съгласно Решение за изпълнение (ЕС) 2021/1772 като по същество равностойно на защитата в рамките на ЕС.

([33]) Преди да изготви такава наредба, министърът трябва да вземе предвид последиците от промените за интересите и основните права и свободи на субектите на данни, както и факта, че на децата (където е приложимо) се полага специална защита по отношение на техните лични данни. Наредбите трябва да бъдат въведени чрез нормативен акт и подлежат на процедурата за потвърдителна резолюция, което означава, че трябва да бъдат изрично одобрени от Парламента на Обединеното кралство. Член 70, параграф 4, алинея 8 от Закона за данните (използване и достъп).

([34]) Член 182, параграф 2 от ЗЗД от 2018 г.

([35]) Член 70, параграф 4, алинея 9 от Закона за данните (използване и достъп).

([36]) Вж. Насоките на комисаря по информацията относно легитимните интереси, достъпни на следния адрес: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) Член 72 от Закона за данните (използване и достъп).

([38]) 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.

([39]) Член 74 от Закона за данните (използване и достъп). Тези наредби подлежат на процедурата за потвърдителна резолюция, което означава, че се изисква изрично одобрение от страна на Парламента на Обединеното кралство.

([40]) Вж. новия член 11a, параграф 1, буква b) и член 11a, параграф 2 от ОРЗД на Обединеното кралство, както и обяснителните бележки към Закона за данните (използване и достъп), параграф 571, достъпни на следния адрес: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Ограничение в рамките на целта*

(28) Съгласно режима на Обединеното кралство за защита на личните данни продължава да се изисква данните да се обработват с конкретна цел и впоследствие да се използват само дотолкова, доколкото употребата им не е несъвместима с първоначалната цел на обработването, както е оценено в съображения 43—48 от Решение за изпълнение (ЕС) 2021/1772.

(29) Първо, със Закона за данните (използване и достъп) са направени няколко целеви изменения на принципа за ограничение в рамките на целта, установен в член 5, параграф 1, буква b) от ОРЗД на Обединеното кралство. С тези изменения се разяснява прилагането на този принцип, без да се променя същността му. В член 71, параграфи 1, 2 и 3 от Закона за данните (използване и достъп) се уточнява, че принципът на ограничаване в рамките на целта се прилага, когато данните са събрани от субекта на данните или по друг начин, че той се прилага единствено когато по-нататъшното обработване на личните данни се извършва от същия администратор или от негово име (т.е. не се прилага, когато е налице смяна на администратора) и че обработването не се счита за законосъобразно само поради факта, че е съвместимо с целите, за които са събрани личните данни.

(30) Второ, със Закона за данните (използване и достъп) се пояснява правилата за по-нататъшното обработване на лични данни чрез прегрупирането им съгласно новодобавения член 8А от ОРЗД на Обединеното кралство, с който се определя пълният режим за по-нататъшното обработване на лични данни. В член 8А, параграф 2 от ОРЗД на Обединеното кралство се посочват елементите, които трябва да се вземат предвид, за да се определи дали дадена нова цел на обработването е съвместима с първоначалната цел. Преди това тези елементи бяха посочени в член 6, параграф 4 от ОРЗД на Обединеното кралство, който съответства на член 6, параграф 4 от Регламент (ЕС) 2016/679 ([41]). Съгласно член 8А, параграф 3 от ОРЗД на Обединеното кралство случаите, в които обработването на лични данни с нова цел се третира като съвместимо с първоначалната цел, са прегрупирани в една наредба. Това включва случаи, в които субектът на данните е съгласен личните му данни да бъдат обработвани с тази нова цел или когато обработването е необходимо за защитата на цел, посочена в член 23, параграф 1 ([42]), когато обработването се извършва за целите на научни или исторически изследвания, с цел архивиране в обществен интерес или за статистически цели ([43]). Накрая, в Закона за данните (използване и достъп) се пояснява, че всяко обработване на данни с цел да се гарантира, че обработването е в съответствие с принципите за защита на данните, посочени в член 5, параграф 1 от ОРЗД на Обединеното кралство, или да се докаже, че това е така, се счита за съвместимо с първоначалната цел. Гореспоменатите случаи продължават да съответстват на случаите, при които се счита, че е налице съвместимо по-нататъшно обработване и съгласно Регламент (ЕС) 2016/679.

(31) Трето, със Закона за данните (използване и достъп) в член 8А, параграф 3, буква d) от ОРЗД на Обединеното кралство се въвеждат и допълнителни нови случаи, в които по-нататъшното обработване на лични данни с нова цел се счита за съвместимо с първоначалната цел. Тези случаи са посочени в приложение 2 към ОРЗД на Обединеното кралство ([44]) и включват например случаите, в които обработването се извършва в отговор на искане, получено от публичен орган, който се нуждае от данните за целите на изпълнението на задача в обществен интерес, за която съществува правно основание, отговарящо на член 6, параграф 3 от ОРЗД на Обединеното кралство, когато обработването е необходимо с оглед защита на обществената сигурност, за реагиране при извънредна ситуация, за разкриване, разследване или предотвратяване на престъпления, за защита на жизненоважните интереси на субекта на данните и други лица, за защита на уязвими лица, за данъчни цели или ако е необходимо с оглед спазване на правно задължение ([45]).

(32) Въпреки че със Закона за данните (използване и достъп) се разширява списъкът със ситуации, при които по-нататъшното обработване с различна цел се счита за съвместимо с първоначалната цел на обработването, при това разширение съществуват някои важни ограничения. Първо, то е ограничено до особени случаи, които са изчерпателно изброени в закона. Второ, то се отнася само за области, в които има ясен обществен интерес от дейността по обработване, т.е. когато по-нататъшното обработване служи за цели, посочени в член 23 от ОРЗД на

([41]) Както в Регламент (ЕС) 2016/679, тези елементи включват всяка връзка между първоначалната и новата цел, контекста, в който са били събрани личните данни, включително връзката между субекта на данните и администратора, естеството на обработването и дали то включва специални категории данни, възможните последици от планираното обработване за субекта на данните и наличието на подходящи гаранции.

([42]) Вж. също член 6, параграф 4 от Регламент (ЕС) 2016/679.

([43]) Съображение 50 от Регламент (ЕС) 2016/679.

([44]) Приложение 2 е въведено в ОРЗД на Обединеното кралство посредством приложение 5 към Закона за данните (използване и достъп), вж. член 71, параграф 6 от този закон.

([45]) Вж. приложение 5 към Закона за данните (използване и достъп).

Обединеното кралство (съответстващ на член 23 от Регламент (ЕС) 2016/679). Следователно то не може да се използва за търговски цели. Трето, макар че със Закона за данните (използване и достъп) на министъра (Secretary of State) се предоставя правото да изменя списъка в приложение 2 с наредба ([46]), министърът може да добавя видове обработване към този списък само когато обработването е необходимо отново за защитата на цел от обществен интерес, посочена в член 23, параграф 1, букви c)—j) от ОРЗД на Обединеното кралство ([47]). Четвърто, когато събирането на лични данни от администратора се основава на съгласието на субекта на данните, обработването с нова цел в случаите, посочени в приложение 2, се счита за съвместимо с първоначалната цел само ако не може с основание да се очаква администраторът да получи ново съгласие от субекта на данните ([48]).

2.2.4. *Индивидуални права*

(33) Съгласно уредбата на Обединеното кралство за защита на личните данни субектите на данни продължават да се ползват от същите индивидуални права, както съгласно Регламент (ЕС) 2016/679, без никакви съществени изменения ([49]), които могат да бъдат упражнявани спрямо обработващия лични данни или администратора, по-специално правото на достъп до данните, правото на възражение срещу тяхното обработване, правото на коригиране или изтриване на данните, както е оценено в съображения 51—54 от Решение за изпълнение (ЕС) 2021/1772.

(34) Първо, със Закона за данните (използване и достъп) се пояснява някои условия, при които тези права могат да бъдат упражнявани. От една страна, чрез изменение на член 12 и въвеждането на нов член 12A в ОРЗД на Обединеното кралство ([50]) се уточняват сроковете, в които администраторите трябва да отговорят на исканията на субекта на данни. По-конкретно член 12 от ОРЗД на Обединеното кралство е изменен по такъв начин, че администраторът вече не е длъжен да предоставя информация за предприетите действия (или за причините за непредприемането на действия) в отговор на искане от страна на субект на данни в съответствие с членове 15—22 от ОРЗД на Обединеното кралство „в срок от един месец от получаване на искането“, а „преди края на приложимия срок“. Приложимият срок е допълнително определен в нововъведения член 12A от ОРЗД на Обединеното кралство като срок от един месец, считано от съответния момент, като това може да бъде моментът, в който администраторът получава искането или получава каквато и да е информация, поискана във връзка с искане по член 12, параграф 6 от ОРЗД на Обединеното кралство, или в който е платена такса, начислена във връзка с искането по член 12, параграф 5 от ОРЗД на Обединеното кралство, като се избира по-късната дата ([51]). Освен това с член 12A, параграф 3 на администратора се дава възможност да удължи приложимия срок с още два месеца, когато това е необходимо поради сложността на исканията, отправени от субекта на данните, или поради броя на тези искания. От друга страна, единствено по отношение на правото на достъп до информация и лични данни, със Закона за данните (използване и достъп) се изменя член 15 от ОРЗД на Обединеното кралство, за да се включи поясненията, разработено съгласно съществуващата национална съдебна практика — въз основа на принципа на пропорционалност съгласно правото на ЕС — че администраторите трябва да извършват само разумни и пропорционални търсения за поисканата информация и лични данни ([52]). Очаква се новата разпоредба да се тълкува в съответствие със съществуващата съдебна практика, в която се предвижда, че „[…] *това, което се преценява при проверката на пропорционалността, е крайната цел на търсенето, а именно потенциалната полза, която предоставянето на информацията може да донесе на субекта на данните, съпоставена спрямо средствата, чрез които се получава тази информация. Във всеки конкретен случай ще се преценява дали за намиране и предоставяне на информацията ще бъдат необходими усилия, които са непропорционални спрямо ползите, които тя може да донесе на субекта на данните*“ ([53]).

([46]) Член 8A, параграф 5 от ОРЗД на Обединеното кралство, въведен с член 71, параграф 1 от Закона за данните (използване и достъп).

([47]) Член 8A, параграф 6 от ОРЗД на Обединеното кралство, въведен с член 71, параграф 1 от Закона за данните (използване и достъп).

([48]) Член 8A, параграф 4, буква b) от ОРЗД на Обединеното кралство, въведен с член 71, параграф 1 от Закона за данните (използване и достъп).

([49]) С член 31 от Закона за жертвите и затворниците от 2024 г. при правото на изтриване, предвидено в член 17 от ОРЗД на Обединеното кралство, се въвежда допълнително основание, като на субектите на данни се предоставя правото да поискат от администраторите да изтрият личните им данни, когато те са били обработени в резултат на неоснователно твърдение по отношение на субекта на данните, отправено от злонамерено лице. Дадено лице се счита за „злонамерено“, ако е осъдено за нарушение, посочено в член 31, параграф 3 от Закона за жертвите и затворниците (например за тормоз), или ако срещу него има издадена заповед за защита. Законът за жертвите и затворниците е достъпен на следния адрес: https://www.legislation.gov.uk/ukpga/2024/21/contents. Освен това с член 77 от Закона за данните (използване и достъп) се изменя правото на информация, както е предвидено в член 13 от ОРЗД на Обединеното кралство, по такъв начин, че администраторът вече не е длъжен да информира субекта на данните за по-нататъшното обработване на неговите лични данни с нова цел, ако то е за целите на научни или исторически изследвания, с цел архивиране в обществен интерес или за статистически цели, ако обработването се извършва в съответствие със специфичните гаранции, посочени в новия член 84B от ОРЗД на Обединеното кралство, и ако предоставянето на информацията би било невъзможно или непропорционално.

([50]) Член 76 от Закона за данните (използване и достъп).

([51]) Член 12A, параграфи 1 и 2 от ОРЗД на Обединеното кралство, въведен с член 76 от Закона за данните (използване и достъп).

([52]) Член 15, параграф 1A от ОРЗД на Обединеното кралство, въведен с член 78 от Закона за данните (използване и достъп).

([53]) *Dawson-Damer/Taylor Wessing LLP* [2017] EWCA Civ 74.

(35) Следователно, макар че сроковете за отговор на искания от страна на субектите на данни и специфичните задължения на администраторите на данни по отношение на правото на достъп подлежат на по-подробни правила, системата на Обединеното кралство продължава да гарантира, че исканията на субектите на данни трябва да се обработват в разумни срокове, определени въз основа на обективни фактори. Освен това материалните задължения на администратора при отговарянето на искания за достъп са формулирани въз основа на установени правни стандарти, при които се отчитат и интересите на субекта на данните. И накрая, в актуалните насоки на комисаря по информацията вече е посочено, че от администратора не се изисква да извършва търсения, които биха били неразумни или непропорционални спрямо значението на предоставянето на достъп до информацията ([54]).

(36) Ограниченията на тези индивидуални права, посочени в ЗЗД от 2018 г., които се вписват в разпоредбите на член 23 от ОРЗД на Обединеното кралство, както и ограниченията и гаранциите, с които се очертава прилагането на тези ограничения, продължават да са в сила в уредбата на Обединеното кралство ([55]), както е описано подробно в съображения 55—67 от Решение за изпълнение (ЕС) 2021/1772.

(37) Що се отнася по-специално до ограничението във връзка с личните данни, обработвани с цел поддържане на ефективен имиграционен контрол или разследване или разкриване на дейности, които биха попречили да се поддържа ефективен имиграционен контрол, доколкото прилагането на тези разпоредби би могло да засегне някои от тези въпроси (освобождаването във връзка с имиграционния контрол) ([56]), правителството на Обединеното кралство измени точка 4 от приложение 2 към ЗЗД от 2018 г. посредством Наредбите от 2022 г. към Закона за защита на данните от 2018 г. (Изменение на освобожданията по приложение 2) ([57]) и Наредбите от 2024 г. към Закона за защита на данните от 2018 г. (Изменение на освобожданията по приложение 2) ([58]), с които се допълват Наредбите от 2022 г. ([59]). С тези изменения в точки 4А и 4В от приложение 2 към ЗЗД от 2018 г. се интегрират гаранциите за прилагане на освобождаването във връзка с имиграционния контрол, изисквани съгласно член 23, параграф 2 от ОРЗД на Обединеното кралство. По-специално в тях се изисква i) освобождаването във връзка с имиграционния контрол да се прилага само за всеки отделен случай, отделно по отношение на всяка от съответните разпоредби на ОРЗД на Обединеното кралство, и отново във всички случаи, когато министърът обмисля възможността да не приложи или да ограничи прилагането на някоя от съответните разпоредби на ОРЗД на Обединеното кралство ([60]), ii) правата и свободите на субекта на данни и неговите потенциални уязвимости да бъдат взети предвид при прилагането на освобождаването във връзка с имиграционния контрол ([61]), iii) министърът да води отчет за прилагането на освобождаването във връзка с имиграционния контрол и да информира субекта на данни за това (освен при специфични обстоятелства, когато предоставянето на тази информация би навредило на целта, за която се прилага освобождаването) ([62]) и iv) да се поясни, че прилагането на освобождаването във връзка с имиграционния контрол е ограничено до обработването на лични данни от страна на министъра ([63]), което на практика е Министерството на вътрешните работи за функциите му съгласно точка 4, подточка 1 от приложение 2 към ЗЗД от 2018 г. Освен това в тях се обяснява и балансирането, което трябва да се предприеме при определяне на това дали има вероятност упражняването на правата на субекта на данни да навреди на ефективния имиграционен контрол и дали поради тази причина е необходимо и пропорционално да бъдат ограничени тези права.

([54]) На разположение на следния адрес: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) С член 88, параграф 2 от Закона за данните (използване и достъп) е въведена малка промяна в член 26, параграф 2, буква f) от ЗЗД от 2018 г. (освобождаването, свързано с националната сигурност и отбрана), с която се пояснява, че правото на подаване на жалба до комисаря съгласно член 77 от ОРЗД на Обединеното кралство не е част от разпоредбите, чието прилагане може да бъде ограничено за целите на националната сигурност или отбрана.

([56]) Към момента на приемането на Решение за изпълнение (ЕС) 2021/1772 валидността и тълкуването на освобождаването във връзка с имиграционния контрол съгласно правото на Обединеното кралство не бяха уредени вследствие на решение на Апелативния съд на Англия и Уелс от 26 май 2021 г., който установи, че освобождаването във връзка с имиграционния контрол във вида, в който е било предвидено в ЗЗД от 2018 г. към онзи момент, е несъвместимо с правото на Обединеното кралство, тъй като в него липсват конкретни разпоредби за определяне на гаранциите, изброени в член 23, параграф 2 от ОРЗД на Обединеното кралство, който отразява член 23, параграф 2 от Регламент (ЕС) 2016/679. Поради тази причина личните данни, предавани за целите на имиграционния контрол на Обединеното кралство или които по друг начин попадат в обхвата на освобождаването във връзка с имиграционния контрол, бяха изключени от обхвата на Решение за изпълнение (ЕС) 2021/1772.

([57]) Наредбите влязоха в сила на 31 януари 2022 г. и са достъпни на следния адрес: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Наредбите влязоха в сила на 8 март 2024 г. и са достъпни на следния адрес: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) Освобождаването във връзка с имиграционния контрол, преработено с Наредбите от 2022 г., беше оспорено отново чрез съдебен контрол на основание, че все още не отговаря на всички изисквания съгласно член 23, параграф 2 от ОРЗД на Обединеното кралство. През декември 2023 г. Апелативният съд го обяви за несъвместимо с изискванията съгласно член 23, параграф 2 от ОРЗД на Обединеното кралство. В резултат на това решение Наредбите от 2022 г. бяха допълнени с Наредбите от 2024 г., с които бяха направени допълнителни изменения на освобождаването във връзка с имиграционния контрол.

([60]) Точка 4А, подточка 2 от приложение 2 към ЗЗД от 2018 г.

([61]) Точка 4АВ, подточки 3 и 4 от приложение 2 към ЗЗД от 2018 г. Във връзка с проекта на Наредбите от 2024 г. беше проведена консултация със Службата на комисаря по информацията, която изрази публично своето съгласие с наредбата. Писмото, публикувано в отговор на консултацията, в което се потвърждава становището на службата, е достъпно на следния адрес: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) Точка 4В, подточки 1 и 2 от приложение 2 към ЗЗД от 2018 г.

([63]) Точка 4, подточка 1 от приложение 2 към ЗЗД от 2018 г.

(38) Освен това комисарят по информацията на Обединеното кралство е издал подробни насоки за прилагането на това конкретно ограничение ([64]). В насоките се посочва по-специално следното: „Освобождаването във връзка с имиграционния контрол следва да не се прилага на общо основание с цел ограничаване на […] права за всички данни, които съхранявате. Обхватът на освобождаването е ограничен до онези права, които, ако бъдат упражнени по отношение на съхраняваните данни, биха навредили на установените имиграционни цели. […]. Следователно позицията по подразбиране на администратора следва да бъде да спазва изискванията съгласно Регламент (ЕС) 2016/679 и ЗЗД, доколкото е възможно. […] Прагът при оценката на вероятността е висок и освобождаването не следва да се прилага на общо основание. […] Трябва да прецените дали прилагането на освобождаването представлява пропорционален отговор на искането на лицето за защита на данните. Възможно е да смятате, че има належаща социална необходимост да бъде приложено освобождаването във връзка с имиграционния контрол, но трябва също така да вземете предвид дали тази необходимост има превес над задължението ви към лицата съгласно Регламент (ЕС) 2016/679. Те имат права по отношение на личните си данни, които трябва да вземете предвид при всички обстоятелства, по-специално правото на достъп. Ето защо е важно във всеки отделен случай да прецените дали правата на лицето по отношение на защитата на неговите данни имат превес над установения риск от вреда. Освобождаването трябва да бъде прилагано пропорционално на обстоятелствата и всеки случай трябва да бъде внимателно преценяван и документиран.“

(39) Като цяло изключението във връзка с имиграционния контрол, предвидено в точка 4 от приложение 2 към ЗЗД от 2018 г., преработено от правителството на Обединеното кралство през 2022 г. и 2024 г., както е тълкувано от съдебната практика ([65]) и насоките на комисаря по информацията, подлежи на редица строги условия, които оформят неговото прилагане и са много подобни на условията, определени в правото на Съюза, по-специално член 23 от Регламент (ЕС) 2016/679, за ограничаване на правата и задълженията в областта на защитата на данните за важни цели от обществен интерес, например имиграционния контрол.

2.2.5. *Ограничения на последващото предаване на данни*

(40) Нивото на защита, което се осигурява за личните данни, предавани от Европейския съюз към администратори или обработващи лични данни в Обединеното кралство, продължава да не е подкопавано от по-нататъшното предаване на такива данни към получатели в трета държава. Режимът относно международното предаване на лични данни от Обединеното кралство остава много близък до правилата, определени в глава V от Регламент (ЕС) 2016/679, както е оценено в съображения 74—82 от Решение за изпълнение (ЕС) 2021/1772.

(41) Въпреки че със Закона за данните (използване и достъп) беше изменена глава 5 от ОРЗД на Обединеното кралство относно предаването на лични данни към трети държави или международни организации, се запазва основното изискване, че личните данни могат да бъдат предавани на трета държава или международна организация само когато предаването се осъществява въз основа на i) наредби за одобряване на предаването на данни (това е нов термин за предишното понятие „наредби относно адекватното ниво на защита“), ii) подходящи гаранции, или iii) дерогация в особени случаи. Тези общи принципи за предаването на данни са отразени в новия член 44A, с който се заменя член 44 от ОРЗД на Обединеното кралство ([66]), в който също се уточнява, че предаването на лични данни към трета държава или международна организация е разрешено само ако се извършва в съответствие с другите разпоредби на ОРЗД на Обединеното кралство.

(42) Що се отнася по-специално до наредбите за одобряване на предаването на данни, в член 45a, параграф 2 от ОРЗД на Обединеното кралство се посочва, че министърът може да приема такива наредби само ако счита, че са изпълнени условията на оценката на защитата на данните. Това означава, че въведената с член 45a, параграф 3 от ОРЗД на Обединеното кралство възможност министърът да взема предвид желателността на улесняването на потоците от данни, когато приема такива наредби, винаги е обвързана с изискването да бъдат изпълнени условията на оценката на защитата на данните. Правният стандарт за изпълнението на условията на оценката на защитата на данните е определен в новия член 45B, параграф 1 от ОРЗД на Обединеното кралство, съгласно който се изисква стандартът на защита на субектите на данни в държавите получателки или в международните организации да не е съществено по-нисък от стандарта, предвиден за субектите на данни съгласно съответното законодателство за защита на данните на Обединеното кралство. В член 45B, параграф 2 от ОРЗД на Обединеното кралство е предоставен неизчерпателен списък на елементи, които трябва да се вземат предвид, за да се прецени дали условията на тази оценка са изпълнени, например зачитането на върховенството на закона и правата на човека, съществуването на орган за защита на данните и неговите правомощия, условията за съдебна или извънсъдебна защита, правилата относно

([64]) На разположение на следния адрес: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) *Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), точки 40 и 41.

([66]) Член 85 и приложение 7 към Закона за данните (използване и достъп).

предаването на лични данни от държавата или от организацията към други държави или международни организации, съответните международни задължения на държавата или организацията и конституцията, традициите и културата на държавата или организацията. Въпреки че с новия член 45B, параграф 2 се преформулира списъкът със съответните елементи, предвиден в предишния член 45 от ОРЗД на Обединеното кралство, основните елементи от този списък се запазват и следователно той остава близък до предвиденото в глава V от Регламент (ЕС) 2016/679. Освен това органите на Обединеното кралство потвърдиха, че министърът ще взема предвид елементи, които не са изброени в член 45B, параграф 2, като например законите и практиките в дадена трета държава, свързани с начина, по който публичните органи осъществяват достъп до лични данни за цели като националната сигурност или правоприлагането, доколкото те засягат общия стандарт за защита. Освен това органите на Обединеното кралство считат, че съответната съдебна практика в третата държава ще бъде съществен елемент при разглеждането на въпросите, изброени неизчерпателно в член 45B, параграф 2 от ОРЗД на Обединеното кралство.

(43) Наредбите за одобряване на предаването на данни продължават да са подчинени на „общите“ процесуални изисквания, предвидени в член 182 от ЗЗД от 2018 г., както е посочено в съображение 77 от Решение за изпълнение (ЕС) 2021/1772. В рамките на тази процедура, когато предлага да се приемат наредби на Обединеното кралство относно адекватното ниво на защита, министърът трябва да се консултира с комисаря по информацията ([67]). 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 ([68]).

(44) Що се отнася до подходящите гаранции, с новия член 46, параграф 1A от ОРЗД на Обединеното кралство се определя, че такова предаване може да се извършва само ако са предвидени съответни гаранции в инструментите, налични съгласно член 46, параграфи 2 и 3 ([69]) от ОРЗД на Обединеното кралство, и ако администраторът, обработващият лични данни или съответните публични органи, действайки разумно и пропорционално, считат, че са изпълнени условията на оценката на защитата на данните. С нововъведените параграфи 6 и 7 се пояснява, че условията на оценката на защитата на данните са изпълнени, ако благодарение на необходимите гаранции след предаването на данните стандартът на защита, предоставен на субектите на данни, не е съществено по-нисък от стандарта съгласно съответното законодателство за защита на данните на Обединеното кралство, т.е. както при Регламент (ЕС) 2016/679 едни и същи правни стандарти се прилагат за наредбите за одобряване на предаването на данни и за подходящите гаранции. Съгласно същия параграф дали дадено действие е разумно и пропорционално, трябва да се определя въз основа на всички обстоятелства или вероятни обстоятелства при предаването на данните или вида на предаването, включително естеството и обема на предаваните лични данни.

(45) Що се отнася до дерогациите в особени случаи, с член 49 от ОРЗД на Обединеното кралство относно условията, при които могат да се прилагат дерогации в особени случаи, се въвеждат редица технически изменения, с които разпоредбата се привежда в съответствие с промените в други разпоредби, без да се засяга нивото на защита на личните данни в Обединеното кралство. Освен това се добавя нов параграф 4A, за да се възпроизведе действието на член 18, параграф 1 от ЗЗД от 2018 г., с който на министъра се предоставя правомощието да определя посредством наредби обстоятелствата, при които предаването на данни се счита за необходимо по съображения от обществен интерес. Накрая, с нов член 49A се възпроизвежда действието на член 18, параграф 2 от ЗЗД от 2018 г., с който на министъра се дава възможност, посредством наредби, да налага ограничения върху предаването на данни, когато то не е одобрено съгласно член 45A (предаване, одобрено с наредба) и когато това се счита за необходимо поради съображения от важен обществен интерес.

(46) По отношение на прилагането на правилата на Обединеното кралство за международно предаване на данни, след приемането на Решение за изпълнение (ЕС) 2021/1772 са настъпили няколко промени.

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

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

([69]) Инструментите за предаване, налични съгласно член 46, параграфи 2 и 3 от ОРЗД на Обединеното кралство, представляват инструменти със задължителен характер и с изпълнителна сила между публичните органи или структури, задължителни фирмени правила в съответствие с член 47 от ОРЗД на Обединеното кралство, стандартни клаузи за защита на данните, заложени в издадени от министъра наредби или в издаден от Комисията по информацията документ, одобрен кодекс за поведение и одобрен механизъм за сертифициране.

(47) Що се отнася до наредбите за одобряване на предаването на данни, досега са приети две нови наредби, отразяващи решенията относно адекватното ниво на защита, които са в сила и в рамките на Съюза, т.е. за предаване на данни към Република Корея и за предаване на данни към търговски субекти, които са се присъединили към разширяването на Рамката за защита на личните данни в отношенията между ЕС и САЩ с оглед включване на Обединеното кралство. Наредбите относно адекватното ниво на защита за Република Корея ([70]) влязоха в сила на 19 декември 2022 г. и с тях се дава възможност за предаването на лични данни от Обединеното кралство към Република Корея. Съответните наредби за разширяването на Рамката за защита на личните данни в отношенията между ЕС и САЩ с оглед включване на Обединеното кралство ([71]) влязоха в сила на 12 октомври 2023 г. и с тях се дава възможност за свободното движение на лични данни към сертифицирани организации в САЩ.

(48) Що се отнася до подходящите гаранции, Обединеното кралство публикува собствени стандартни договорни клаузи за защита на данните, Споразумението за международно предаване на данни ([72]) и допълнение към стандартните договорни клаузи на ЕС, като и двете влязоха в сила през март 2022 г. Посредством Споразумението за международно предаване на данни се предоставя специфичен за Обединеното кралство механизъм за осигуряване на подходящи гаранции при предаването на лични данни, като са налице редица прилики със стандартните договорни клаузи на ЕС. С допълнението, издадено от комисаря по информацията, на администраторите и обработващите лични данни в Обединеното кралство се дава възможност да използват стандартните договорни клаузи на ЕС съгласно ОРЗД на Обединеното кралство за международно предаване на данни. Комисарят по информацията предостави и инструмент за оценка на риска при предаването на данни с цел да подпомогне организациите в Обединеното кралство при оценката на рисковете, свързани с международното предаване на данни.

(49) Освен това Обединеното кралство рационализира процеса на одобряване на задължителните фирмени правила (ЗФП) чрез нови насоки и нови възможности за одобряване на ЗФП. През юли 2022 г. комисарят по информацията публикува насоки и справочни таблици, за да се разясни подходът на Обединеното кралство към ЗФП след Брексит, а през декември 2023 г. беше публикувано допълнение към ЗФП на ЕС, за да се гарантира, че одобрените съгласно рамката на Съюза ЗФП са изпълняеми в Обединеното кралство ([73]).

(50) Накрая, през юли 2023 г. Обединеното кралство стана асоцииран член на Глобалния форум за трансграничните правила за защита на неприкосновеността на личния живот (ТПЗНЛЖ) ([74]). Важно е да се отбележи, че това членство не води до улесняване на предаването на данни от Обединеното кралство към други членове на форума за ТПЗНЛЖ. Обединеното кралство поясни, че всяко предаване на лични данни от Обединеното кралство към трети държави или международни организации трябва да отговаря на условията, определени в законодателството на Обединеното кралство, както е описано по-горе, по-специално оценката на защитата на данните, при която се изисква предоставяните стандарти за защита да не са „съществено по-ниски“ от тези съгласно ОРЗД на Обединеното кралство.

(51) Както Комисията вече обясни, с ТПЗНЛЖ не се гарантира достатъчно ниво на защита на личните данни с произход от ЕС. По-специално при тях не се предвиждат изпълняеми индивидуални права ([75]). Следователно е особено важно да се отбележи, че макар и Обединеното кралство да е асоцииран член на Глобалния форум за ТПЗНЛЖ, ТПЗНЛЖ не могат да представляват валиден механизъм за предаване на данни съгласно законодателството на Обединеното кралство за защита на данните. Ако в това отношение настъпи промяна, това би подкопало нивото на защита, което понастоящем е гарантирано за личните данни, предавани от ЕС към Обединеното кралство. Следователно Комисията ще продължи да следи отблизо по-нататъшните развития в това отношение.

([70]) На разположение на следния адрес: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) На разположение на следния адрес: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) На разположение на следния адрес: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/.

([73]) След Брексит комисарят по информацията получи значителен брой заявления за ЗФП в Обединеното кралство. Много одобрени ЗФП вече не можеше да бъдат използвани, тъй като след Брексит можеше да продължат да се използват само ЗФП, при които комисарят по информацията е участвал в процеса на одобряване, а притежателите на такива ЗФП бяха длъжни да представят на комисаря по информацията актуализирана документация за ЗФП в съответствие с ОРЗД на Обединеното кралство.

([74]) Членове на форума за ТПЗНЛЖ са Съединените американски щати, Канада, Япония, Република Корея, Филипините, Сингапур, Тайван и Австралия, а Мавриций, Международният финансов център на Дубай и Бермудските острови са асоциирани членове като Обединеното кралство.

([75]) Вж. например сравнителния анализ, извършен от органите за защита на данните на Г-7 относно основните елементи на схемата за сертифициране по ОРЗД и системата за ТПЗНЛЖ, в който се посочват „значителни различия“ между системите, включително по отношение на изпълнителната сила и правната защита, правилата относно независимия надзор и държавния достъп). На разположение на следния адрес: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165
Вж. съображение 79 от Решение за изпълнение (ЕС) 2019/419 на Комисията от 23 януари 2019 г. съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Япония по Закона за защита на личната информация (ОВ L 76, 19.3.2019 г., стр. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Вж. също Работна група по член 29, Становище 02/2014 относно референтен документ за изискванията към задължителните фирмени правила, представени на националните органи по защита на данните в ЕС, и към трансграничните правила за защита на неприкосновеността на личния живот, представени на отговорниците по отчетността на АТИС в сферата на ТПЗНЛЖ, 6 март 2014 г.

2.2.6. *Автоматизирано вземане на решения*

(52) Въпреки че в Закона за данните (използване и достъп) са запазени няколко елемента от правилата за автоматизираното вземане на решения, оценени в съображение 54 от Решение за изпълнение (ЕС) 2021/1772, с него са изменени някои аспекти на тези правила.

(53) На първо място, с нововъведения член 22B от ОРЗД на Обединеното кралство се установява обща забрана за обработването на специални категории лични данни (определени в член 9, параграф 1 от ОРЗД на Обединеното кралство) за решения, основаващи се единствено на автоматизирано обработване, които имат правни или също толкова значителни последици за субекта на данни. В него обаче се очертават три изключения от тази забрана: субектът на данните е дал изрично съгласие за такова обработване; или решението е необходимо за сключването или изпълнението на договор между администратора и субекта на данните; или обработването се изисква или разрешава от закона. При последните две изключения автоматизираното обработване трябва да е необходимо по съображения от важен обществен интерес ([76]). Общата забрана не се прилага за важните решения, основаващи се на автоматизирано обработване на неспециални категории данни.

(54) Освен това с новия член 22A от ОРЗД на Обединеното кралство се пояснява определението за решение, „основаващо се единствено на автоматизирано обработване“, като в него се предвижда, че това е решение, при което няма съществено човешко участие в процеса на вземане на решения. Важно е да се отбележи, че администраторите са длъжни да оценят степента, до която профилирането допринася за решението, за да може да се определи дали човешкото участие е съществено. Освен това в член 22A от ОРЗД на Обединеното кралство се пояснява, че „важно решение“ е такова решение, което поражда правни последици за субекта на данни или го засяга също толкова значително ([77]).

(55) Второ, с нововъведения член 22C от ОРЗД на Обединеното кралство от администраторите се изисква да въведат мерки за осигуряване на съответни гаранции за всяко важно решение, основаващо се изцяло или частично на лични данни и единствено на автоматизирано обработване (включване на неспециални категории лични данни). Тези гаранции трябва да включват предоставяне на информация на субекта на данните относно процеса на вземане на решения, даване на възможност на субекта на данните да оспори решението и да представи становище, и предоставяне на гаранции, че субектът на данните може да получи човешка намеса в процеса на вземане на решения ([78]).

(56) И накрая, с нововъведения член 22D от ОРЗД на Обединеното кралство на министъра се предоставя правомощието да приема вторично законодателство, за да се опише какво представлява (и какво не представлява) съществено човешко участие, както и какво решение трябва (и какво решение не трябва) да се счита за имащо също толкова значителни последици за субекта на данни. С посочените разпоредби също така се дава възможност на министъра да приема вторично законодателство, с което: i) се добавят нови гаранции; ii) се налагат изисквания, допълващи съществуващите гаранции; и iii) се определят мерките, които не отговарят на гаранциите ([79]). Важно е да се отбележи, че преди да приеме наредби в съответствие с член 22D от ОРЗД на Обединеното кралство, министърът трябва да се консултира с комисаря по информацията ([80]), с наредбите не може да се изменя член 22C от ОРЗД на Обединеното кралство ([81]), както и че те подлежат на процедурата за потвърдителна резолюция ([82]), което означава, че наредбите трябва да бъдат одобрени и от двете камари на Парламента на Обединеното кралство, преди да могат да бъдат приети.

(57) Въпреки че по този начин със Закона за данните (използване и достъп) са въведени промени в рамката за автоматизираното вземане на решения, важно е да се отбележи, че съгласно правната уредба на Обединеното кралство автоматизираното вземане на решения продължава да бъде предмет на основните гаранции, с които се гарантира правото на човешка намеса във всички случаи на важни решения, основаващи се единствено на автоматизирано обработване, т.е. независимо дали те се основават на обработването на чувствителни или

([76]) Член 22B от ОРЗД на Обединеното кралство, въведен с член 80, параграф 1 от Закона за данните (използване и достъп).
([77]) Член 22a от ОРЗД на Обединеното кралство, въведен с член 80, параграф 1 от Закона за данните (използване и достъп).
([78]) Член 22C от ОРЗД на Обединеното кралство, въведен с член 80, параграф 1 от Закона за данните (използване и достъп).
([79]) Член 22D от ОРЗД на Обединеното кралство, въведен с член 80, параграф 1 от Закона за данните (използване и достъп). Всички наредби, приети съгласно тези правомощия, подлежат на процедурата за потвърдителна резолюция, чрез която се осъществява парламентарен надзор. С наредбите не могат да се изменят изискванията, предвидени в член 22C.
([80]) Член 182, параграф 2 от ЗЗД от 2018 г.
([81]) Член 22D, параграф 4 от ОРЗД на Обединеното кралство.
([82]) Член 22D, параграф 5 от ОРЗД на Обединеното кралство.

нечувствителни лични данни ([83]). Освен това, както е отбелязано от Комисията в предишни решения относно адекватното ниво на защита ([84]), малко вероятно е специфичните правила за автоматизираното вземане на решения в ОРЗД на Обединеното кралство да повлияят на нивото на защита на личните данни, предавани от Съюза към Обединеното кралство. Що се отнася до събраните в Съюза лични данни, всички решения, основаващи се на автоматизирано обработване, обикновено се вземат от администратора в Съюза (който има пряка връзка със съответния субект на данни) и следователно се подчиняват на правилата на Регламент (ЕС) 2016/679.

2.3. **Надзор и привеждане в изпълнение**

2.3.1. *Независим надзор*

(58) В Обединеното кралство надзорът и привеждането в изпълнение на уредбата за защита на данните продължават да се осъществяват от независим надзорен орган по защита на данните, както е анализирано в съображения 85—91 от Решение за изпълнение (ЕС) 2021/1772. Със Закона за данните (използване и достъп) се реформира структурата на управление на този орган, като се създава юридическо лице — Комисията по информацията, която ще замести комисаря по информацията, който беше орган с еднолична корпоративна структура.

(59) По-конкретно, след като бъдат приложени, с мерките за управление, определени в Закона за данните (използване и достъп), ще се премахне длъжността на комисаря по информацията и неговите функции, персонал и имущество ще се прехвърлят към новия орган — Комисията по информацията. Комисията по информацията се състои от членове с изпълнителни функции и членове без изпълнителни функции ([85]). В посочения закон се предвижда също така, че комисарят по информацията ще поеме длъжността председател на Комисията по информацията, който е един от членовете без изпълнителни функции ([86]). Освен това в Закона за данните (използване и достъп) се предвижда, че доколкото е уместно вследствие на прехвърлянето на тези функции, позоваванията на комисаря по информацията във всички нормативни актове или други документи (независимо от това кога са били приети или изготвени) се третират като позовавания на Комисията по информацията. За да изпълнява функциите си, Комисията по информацията може да създава комитети и да делегира функции на даден член, служител или комитет на комисията ([87]), като може и да предприема мерки за уреждане на своите процедури и процедурите на комитетите, включително по отношение на кворума и вземането на решения с мнозинство. Тези процедури трябва да бъдат оповестени публично ([88]).

(60) Важно е да се отбележи, че независимостта на Комисията по информацията подлежи на същите гаранции като оценените в съображения 87—90 от Решение за изпълнение (ЕС) 2021/1772 ([89]), включително по отношение на правилата за назначаване и освобождаване от длъжност на председателя. Подобна защита се прилага и по отношение на другите членове без изпълнителни функции на Комисията по информацията. По-специално председателят на Комисията по информацията се назначава от Негово Величество по препоръка на министъра. Той се избира по заслуги и въз основа на безпристрастен конкурс на общо основание ([90]). Останалите членове без изпълнителни функции се назначават от министъра след консултации с председателя. Кандидатите могат да бъдат препоръчани за назначаване или да бъдат назначени само ако са избрани по заслуги и въз основа на безпристрастен конкурс на общо основание и ако министърът е убеден, че те не са в конфликт на интереси ([91]). Членовете с изпълнителни функции са служители на Комисията по информацията, наети по реда и условията, определени от членовете без изпълнителни функции ([92]). Изпълнителният директор се назначава от председателя и другите членове без изпълнителни функции след консултации с министъра. Назначенията на членовете с изпълнителни функции също подлежат на подбор по заслуги въз основа на безпристрастен конкурс на общо основание ([93]).

(61) Председателят може да бъде отстранен от длъжност само от Негово Величество след обръщение от страна на двете камари на Парламента и само ако министърът е представил доклад на камарата, в който посочва, че е убеден, че председателят е извършил тежко нарушение, има конфликт на интереси, не е спазил специфични изисквания за

([83]) Член 22C, параграф 2 от ОРЗД на Обединеното кралство, въведен с член 80, параграф 1 от Закона за данните (използване и достъп).
([84]) Вж. например съображение 94 от Решение за изпълнение (ЕС) 2019/419 и съображение 81 от Решение за изпълнение (ЕС) 2022/254 на Комисията от 17 декември 2021 г. съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Република Корея по Закона за защита на личните данни (ОВ L 44, 24.2.2022 г., стр. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).
([85]) Точка 3, подточка 1 от приложение 12A към ЗЗД от 2018 г.
([86]) Членове 117, 118, 119 и 120, наред с приложение 14 към Закона за данните (използване и достъп).
([87]) Точки 13 и 14 от приложение 12A към ЗЗД от 2018 г.
([88]) Точка 16 от приложение 12A към ЗЗД от 2018 г.
([89]) Член 52 от ОРЗД на Обединеното кралство, както и приложение 12A към ЗЗД от 2018 г., въведени с член 114A от Закона за данните (използване и достъп).
([90]) Точка 5, подточка 1 и точка 3, подточка 2 от приложение 12A към ЗЗД от 2018 г.
([91]) Точка 3, подточка 2 и точки 5 и 6 от приложение 12A към ЗЗД от 2018 г.
([92]) Точка 11 от приложение 12A към ЗЗД от 2018 г.
([93]) Точка 5, подточка 2 от приложение 12A към ЗЗД от 2018 г.

предоставяне на информация по отношение на потенциални конфликти на интереси или е неспособен, негоден или не желае да изпълнява функциите на председател ([94]). Членовете без изпълнителни функции могат да бъдат отстранени от длъжност от министъра само ако той е убеден, че са изпълнени специалните условия, определени в законодателството. Те включват конфликт на интереси, тежко нарушение или неспособност, негодност или нежелание за изпълнение на функциите. Що се отнася до допълнителните гаранции, министърът е длъжен да оповести публично решението за това и да предостави на члена изложение на причините за отстраняването ([95]).

(62) Основната роля на Комисията по информацията ще продължи да бъде наблюдението и прилагането на уредбата за защита на данните в Обединеното кралство, „за да се защитят основните права и свободи“ на физическите лица ([96]). Що се отнася до функцията на Комисията по информацията да осигурява подходящо ниво на защита на личните данни, в Закона за данните (използване и достъп) от Комисията по информацията изрично се изисква да взема предвид интересите на субектите на данни, администраторите и други лица, както и въпроси от обществен интерес, и да насърчава общественото доверие в обработването на лични данни ([97]). Тези цели са посочени и в съображение 7 от Регламент (ЕС) 2016/679.

(63) Освен това в Закона за данните (използване и достъп) се уточнява, че когато изпълнява функциите си съгласно законодателството за защита на данните, Комисията по информацията взема предвид насърчаването на иновациите и конкуренцията, значението на предотвратяването, разследването, разкриването и наказателното преследване на престъпления, необходимостта да се гарантират обществената сигурност и националната сигурност, както и специфичните нужди, свързани със закрилата на детето ([98]). В законодателството на ЕС за защита на данните също така се признава необходимостта от балансиране на защитата на личните данни спрямо някои други основни права и цели, като например постигането на икономически и социален напредък, сигурността и правосъдието, както и свободата на стопанската инициатива ([99]).

2.3.2. *Привеждане в изпълнение, включително санкции*

(64) Правомощията и задачите на Комисията по информацията продължават да съответстват на тези на надзорните органи по защита на данните на държавите членки съгласно съответните членове на Регламент (ЕС) 2016/679 ([100]), както е оценено в съображения 91—95 от Решение за изпълнение (ЕС) 2021/1772.

(65) Със Закона за данните (използване и достъп) са въведени определени пояснения относно упражняването на някои от тези правомощия.

(66) От една страна, със Закона за данните (използване и достъп) се пояснява, че Комисията може да изисква специфични „документи“ и „информация“, когато използва правомощието за издаване на информационно постановление ([101]). От друга страна, със Закона за данните (използване и достъп) се въвеждат две нови правомощия за разследване за Комисията по информацията: ново правомощие за изискване на доклад ([102]) и ново правомощие за издаване на „постановления за изслушване“ на администратори в случай на предполагаемо нарушение на ОРЗД на Обединеното кралство или на ЗЗД от 2018 г. ([103]).

([94]) Точка 7, подточки 6 и 7 от приложение 12А към ЗЗД от 2018 г.

([95]) Точка 9, подточки 6, 7, 8 и 9 от приложение 12А към ЗЗД от 2018 г.

([96]) Член 51 от ОРЗД на Обединеното кралство.

([97]) Член 91 от Закона за данните (използване и достъп), с който се въвежда член 120А от ЗЗД от 2018 г.

([98]) Член 91 от Закона за данните (използване и достъп), с който се въвежда член 120В от ЗЗД от 2018 г. Със Закона за данните (използване и достъп) в ЗЗД от 2018 г. също така се въвежда нов член 120С, съгласно който от Комисията по информацията се изисква да изготви и публикува стратегия, отразяваща, наред с другото, начина, по който комисията ще разгледа гореспоменатите въпроси и насърчаването на икономическия растеж при упражняването на своите регулаторни функции.

([99]) Вж. по-специално съображения 2 и 4, както и член 23 от Регламент (ЕС) 2016/679.

([100]) Членове 57 и 58 от ОРЗД на Обединеното кралство.

([101]) Член 97 от Закона за данните (използване и достъп), с който се изменя член 142 от ЗЗД от 2018 г. Съображенията относно въздействието на технологиите и ролята на защитата на данните за изграждането на доверие в цифровата икономика са част от дейностите на регулаторните органи за защита на данните както в Обединеното кралство, така и в ЕС. Вж. например годишния доклад на Европейския комитет по защита на данните за 2024 г., страница 12: „ЕКЗД е динамичен и сътрудничещ орган, който играе основна роля, за да се гарантира последователното прилагане на законите за защита на данните в цяла Европа. От моята гледна точка като заместник-председател аз го възприемам като пазител на правото на неприкосновеност на личния живот на физическите лица, който умело балансира нуждите от иновации и икономически растеж.“

([102]) Член 98 от Закона за данните (използване и достъп), с който се изменя член 146 от ЗЗД от 2018 г.

([103]) Член 100 от Закона за данните (използване и достъп), с който се въвежда член 148А от ЗЗД от 2018 г.

(67) Що се отнася до упражняването на тези правомощия от страна на Комисията по информацията, от влизането в сила на Решение за изпълнение (ЕС) 2021/1772 комисарят по информацията е обработвал около 40 000 жалби от субекти на данни годишно, което е подобно на броя на обработваните жалби, когато Обединеното кралство все още беше част от Съюза и прилагаше Регламент (ЕС) 2016/679 ([104]). Комисарят по информацията също провеждаше служебни разследвания, обхващащи широк спектър от въпроси, свързани със сектора и със съответствието, включително правата на субектите на данни ([105]).

(68) Що се отнася до мерките за изпълнение, от влизането в сила на Решение за изпълнение (ЕС) 2021/1772 комисарят е издал 120 официални предупреждения, 32 информационни постановления, 3 ревизионни постановления, 12 изпълнителни постановления и 2 предупреждения и е наложил 12 глоби ([106]). Това включва няколко значителни парични санкции, наложени съгласно ОРЗД на Обединеното кралство и ЗЗД от 2018 г. Например през април 2023 г. комисарят по информацията наложи глоба от 12,7 милиона британски лири на платформа на социални медии за злоупотреба с данни на деца ([107]). През март 2025 г. софтуерна компания беше глобена с 3,07 милиона британски лири за пропуски по отношение на сигурността, в резултат на които личната информация на повече от 70 000 души беше изложена на риск ([108]). Съвсем наскоро, през юни 2025 г., комисарят по информацията глоби компания за генетични изследвания с 2,31 милиона британски лири, тъй като не е въвела подходящи мерки за сигурност, за да защити личната информация на потребителите в Обединеното кралство след мащабна кибератака през 2023 г. ([109]).

(69) След приемането на Решение за изпълнение (ЕС) 2021/1772 Службата на комисаря по информацията разработи и публикува значителен брой насоки, становища и други документи с указания, в които се пояснява прилагането на правилата за защита на данните във важни области, като например разпознаване на лица, справедливост в областта на изкуствения интелект, данни на деца, директен маркетинг, видеонаблюдение, право на достъп, прозрачност в областта на здравеопазването и социалните грижи и др., и които са насочени към различни аудитории, включително малки и средни предприятия, специфични субекти като училища, детски градини или малки публични органи, както и към бизнеса като цяло, широката общественост или субектите на данни ([110]).

3. СЪОТВЕТНИ ПРОМЕНИ ВЪВ ВРЪЗКА С ДОСТЪПА И ИЗПОЛЗВАНЕТО ОТ ПУБЛИЧНИ ОРГАНИ В ОБЕДИНЕНОТО КРАЛСТВО НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ

3.1. Обща правна уредба

(70) Обединеното кралство продължава да бъде член на Съвета на Европа, да се придържа към Европейската конвенция за правата на човека и да бъде подчинено на юрисдикцията на Европейския съд по правата на човека. Следователно то продължава да бъде обвързано от задълженията, залегнали в международното право, както е описано в съображения 116—119 от Решение за изпълнение (ЕС) 2021/1772, които оформят системата му за държавен достъп до лични данни въз основа на принципи, гаранции и индивидуални права, идентични с тези, които се прилагат за 27-те държави членки като страни по ЕКПЧ и които до голяма степен са отразени в съответната съдебна практика на Съда на Европейския съюз.

(71) Специфичните гаранции и права за защита на личните данни продължават да бъдат гарантирани от ЗЗД от 2018 г., когато данните се обработват от публични органи на Обединеното кралство, включително от правоприлагащи органи и органи за национална сигурност, както е анализирано в съображения 121—132 от Решение за изпълнение (ЕС) 2021/1772. Със Закона за данните (използване и достъп) са направени само ограничени и целеви изменения в онези части от ЗЗД от 2018 г., в които се предвиждат правилата за обработването на лични данни в контекста на наказателното правоприлагане (част 3 от ЗЗД от 2018 г.) и националната сигурност (част 4 от ЗЗД от 2018 г.).

([104]) Годишни доклади на комисаря по информацията от 2021—2022 г., 2022—2023 г. и 2023—2024 г. Вж. също Решение за изпълнение (ЕС) 2021/1772, съображение 96.

([105]) Годишен доклад на комисаря по информацията от 2023—2024 г., страница 41.

([106]) Годишни доклади на комисаря по информацията от 2021—2022 г., 2022—2023 г. и 2023—2024 г.

([107]) За повече информация относно тези и други изпълнителни действия вж. уебсайта на комисаря по информацията, достъпен на следния адрес: https://ico.org.uk/action-weve-taken/enforcement/

([108]) Повече информация можете да намерите на следния адрес: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

([109]) Повече информация можете да намерите на следния адрес: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

([110]) На разположение на следния адрес: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/.

(72) Що се отнася до 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, в част 3 от ЗЗД от 2018 г. продължават да се предвиждат принципи, права и задължения, подобни на тези, определени в Директива (ЕС) 2016/680 ([111]).

(73) По-специално на датата на настоящото решение Комисията прие решение 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 за целите на наказателното правоприлагане, продължава да осигурява ниво на защита, което по същество е равностойно на гарантираното съгласно Директива (ЕС) 2016/680.

(74) Със Закона за данните (използване и достъп) бяха изменени и консолидирани съществуващите освобождавания в част 3 от ЗЗД от 2018 г., с които разполагат компетентните органи за целите на националната сигурност. Освобождаването, свързано с националната сигурност, позволява на компетентните органи да не прилагат определени разпоредби на част 3 от ЗЗД от 2018 г., ако освобождаването по отношение на тази разпоредба е необходимо за целите на защитата на националната сигурност ([112]). Това отразява свързаните с националната сигурност освобождавания, които са предвидени за обработването на лични данни съгласно ОРЗД на Обединеното кралство (предвидени в член 26 от ЗЗД от 2018 г.) и съгласно част 4 от ЗЗД от 2018 г. (предвидени в член 110 от ЗЗД от 2018 г.).

(75) Освобождаването, свързано с националната сигурност, подлежи на същите ограничения и гаранции като освобожданията съгласно ОРЗД на Обединеното кралство и част 4 от ЗЗД от 2018 г., както е анализирано в съображения 64—67 и съображение 126 от Решение за изпълнение (ЕС) 2021/1772. По-специално, освобождаването може да се прилага само ако и дотолкова, доколкото е необходимо с оглед защитата на националната сигурност. Това не е общо освобождаване и то трябва да се преценява и прилага от администратора за всеки отделен случай ([113]). Освен това всяко негово прилагане трябва да бъде в съответствие със стандартите за правата на човека (залегнали в Закона за правата на човека от 1998 г. и в Европейската конвенция за правата на човека), съгласно които в едно демократично общество всяка намеса в правата на неприкосновеност на личния живот следва да бъде необходима и пропорционална ([114]). Това се потвърждава и в насоките на комисаря по информацията относно прилагането на освобожданията, свързани с националната сигурност ([115]).

(76) Освен това, въз основа на измененията, въведени със Закона за данните (използване и достъп) ([116]), с разпоредбите на част 4 от ЗЗД от 2018 г., която обикновено се прилага само за обработването на данни от органите за национална сигурност, може да се регулира и специфична дейност по обработване на данни от органи, компетентни в областта на наказателното правоприлагане.

([111]) С член 69 от Закона за данните (използване и достъп) се въвеждат определението за „съгласие“ и условията за използването на съгласие, както е предвидено в член 4, параграф 11 и член 7 от ОРЗД на Обединеното кралство (които отразяват съответните разпоредби в Регламент (ЕС) 2016/679), под формата на нов член 33, параграф 1А и член 40а в ЗЗД от 2018 г., като по този начин се пояснява понятието за съгласие и условията за използването на съгласие, когато то служи за правно основание за обработването на лични данни от компетентните органи за целите на наказателното правоприлагане. Освен това с член 71, параграфи 7 и 8 от Закона за данните (използване и достъп) леко се пояснява формулировката на член 36, параграф 1 от ЗЗД от 2018 г. Накрая, където е уместно, измененията на ОРЗД на Обединеното кралство, въведени със Закона за данните (използване и достъп), както е описано в член 2, са отразени и в част 3 от ЗЗД от 2018 г., вж. например член 74, параграфи 2—5 относно обработването на чувствителни данни, член 76, параграфи 4—6 относно сроковете за отговор на исканията на субекта на данни, член 78, параграфи 2 и 3 относно търсенията в отговор на исканията на субектите на данни и член 80, параграфи 3—5 относно автоматизираното вземане на решения.

([112]) Член 78А, параграф 1 от ЗЗД от 2018 г., въведен с член 88 от Закона за данните (използване и достъп). Съгласно член 78а, параграфи 2—4 от ЗЗД от 2018 г. с освобождаването се позволява да не се прилагат принципите за защита на данните (с изключение на принципа на законосъобразност и условията и гаранциите за обработването на чувствителни данни), индивидуалните права, задълженията на администраторите и обработващите лични данни по отношение на нарушенията на сигурността на данните, определени части от правилата относно международното предаване на данни и някои от правомощията на комисаря по информацията за влизане с цел извършване на проверки и предприемане на изпълнителни действия.

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

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

([115]) 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/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) Членове 89 и 90 от Закона за данните (използване и достъп).

(77) Въпреки че по този начин режимът за защита на данните при обработването им в контекста на националната сигурност в определени ситуации обхваща и обработването на данни от органи за наказателно правоприлагане, това важи само при специфични обстоятелства и при спазване на строги условия и гаранции, т.е. ако i) компетентен орган е посочен като „квалифициран компетентен орган“ в издадени от министъра наредби, за които се изисква парламентарно одобрение ([117]), и ii) министърът определи чрез постановление конкретна дейност по обработване на данни, извършвана от квалифицирания компетентен орган. Важно е да се отбележи, че определянето на дейността по обработване на данни може да се осъществи само ако министърът счете, че това е необходимо за целите на защитата на националната сигурност, т.е. когато орган за наказателно правоприлагане действа за целите на националната сигурност и дейността по обработване на данни се извършва от квалифицирания компетентен орган като съвместен администратор с поне една разузнавателна служба ([118]). Като допълнителни гаранции министърът трябва да се консултира с комисаря, преди да издаде постановление за определяне ([119]), текстът на постановлението по принцип трябва да бъде публикуван ([120]), а лицата, пряко засегнати от дадено постановление за определяне, могат да поискат съдебен контрол ([121]). Следователно основната цел на това изменение е да се поясни, че когато органите на Обединеното кралство имат правомощия както в областта на правоприлагането, така и в областта на националната сигурност, и обработват данни в контекста на правомощията си в областта на националната сигурност, може да се приложи режимът за защита на данните за службите за национална сигурност.

(78) С част 4 от ЗЗД от 2018 г. се урежда обработването на данни от разузнавателните служби на Обединеното кралство. В нея продължават да се определят основните принципи за защита на данните, да се поставят условия за обработването на специални категории данни, да се предоставят права на субектите на данни, да се изисква защита на данните на етапа на проектирането и да се урежда предаването на лични данни, както е описано в съображения 125—132 от Решение за изпълнение (ЕС) 2021/1772.

(79) Измененията в този режим, въведени със Закона за данните (използване и достъп), са ограничени. Що се отнася до правото на достъп на субектите на данни, предвидено в член 94 от ЗЗД от 2018 г., със Закона за данните (използване и достъп) се въвежда нов параграф 2A, в който се пояснява, че субектът на данни има право на съответната информация само доколкото администраторът може да я предостави въз основа на разумно и пропорционално търсене ([122]). Както е обяснено в съображение 35, с това изменение се определя правото на достъп въз основа на установени правни стандарти, при които се отчитат и интересите на субекта на данните. Докато в областта на автоматизираното вземане на решения на администраторите продължава да бъде забранено да вземат решение, засягащо значително субект на данни, изцяло въз основа на автоматизирано обработване на лични данни, свързани със субекта на данните, освен ако това решение не се изисква или не е разрешено от закона, субектът на данните е дал съгласие за вземането на решението по този начин или решението е взето в контекста на договор ([123]); със Закона за данните (използване и достъп) в част 4 от ЗЗД от 2018 г. ([124]) се въвежда същото определение на понятието „решения, основаващи се изцяло на автоматизирано обработване“ като това, което е включено в член 22A от ОРЗД на Обединеното кралство и анализирано в съображение 53 от настоящото решение.

3.2. **Съответни промени във връзка с достъпа и използването от публични органи на Обединеното кралство за целите на наказателното правоприлагане**

(80) Законодателството на Обединеното кралство продължава да налага важни ограничения на достъпа и използването на лични данни за целите на наказателното правоприлагане и да осигурява механизми за надзор и правна защита в тази област, както е анализирано в съображения 134—174 от Решение за изпълнение (ЕС) 2021/1772.

([117]) Член 82, параграфи A1, 2A и 4 от ЗЗД от 2018 г., въведени с член 89, параграф 2 от Закона за данните (използване и достъп).

([118]) Член 82A, параграфи 1 и 2, въведени с член 89, параграф 3 от Закона за данните (използване и достъп). Като допълнителни гаранции министърът трябва да се консултира с комисаря, преди да издаде постановление за определяне (вж. новия член 82A, параграф 8 от ЗЗД от 2018 г.), текстът на постановлението по принцип трябва да бъде публикуван (вж. новия член 82D, параграф 1), при спазване на освобождаванията, посочени в новия член 82D, параграф 3 от ЗЗД от 2018 г., и лице, пряко засегнато от постановление за определяне, може да поиска съдебен контрол (вж. новия член 82E от ЗЗД от 2018 г.).

([119]) Член 82a, параграф 8 от ЗЗД от 2018 г.

([120]) Член 82D, параграф 1, при спазване на освобождаванията, предвидени в новия член 82D, параграф 3 от ЗЗД от 2018 г.

([121]) Член 82E от ЗЗД от 2018 г.

([122]) Член 78, параграф 4 от Закона за данните (използване и достъп).

([123]) Член 96 от ЗЗД от 2018 г.

([124]) Съгласно новия член 96, параграф 4 от ЗЗД от 2018 г. едно решение се основава изцяло на автоматизирано обработване, ако процесът на вземане на решение не включва възможност човешко същество да приеме, отхвърли или повлияе на решението. Вж. член 80, параграф 4, буква c) от Закона за данните (използване и достъп).

3.2.1. *Правни основания и приложими ограничения/гаранции*

(81) Събирането на лични данни от стопански оператори в Обединеното кралство за целите на наказателното правоприлагане продължава да бъде допустимо в правния ред на Обединеното кралство въз основа на заповеди за претърсване и заповеди за предоставяне при спазване на условията и гаранциите, описани в съображения 135—138 от Решение за изпълнение (ЕС) 2021/1772.

(82) Освен това със Закона за националната сигурност от 2023 г. ([125]), чиято цел е да се справи със заплахите за националната сигурност от шпионаж, саботаж и агенти на чужди сили, за полицията на Обединеното кралство бяха въведени нови правомощия за влизане, претърсване и изземване, включително възможността за получаване на лични данни, когато има основателни причини да се подозира, че ще бъдат получени материали, които вероятно представляват доказателство, че е извършено или предстои да бъде извършено някое от по-тежките престъпления или заплаха от чужда сила съгласно Закона за националната сигурност от 2023 г. ([126]). За тези правомощия се прилагат условия и гаранции, подобни на тези, които са анализирани в Решение за изпълнение (ЕС) 2021/1772 за съществуващите към онзи момент правомощия. По-специално за използването им е необходимо разрешение чрез заповед, заповед за предоставяне или заповед за предоставяне на обяснение, издадена от независим съдебен орган, по искане на полицая/разследващия служител ([127]). Съществуват специфични защити за поверителни материали, като например журналистически материали и елементи, които са обект на адвокатска тайна ([128]). По подобен начин издаването на заповеди за разкриване на информация ([129]), заповеди за предоставяне на информация за клиенти ([130]) и заповеди за наблюдение на сметки ([131]), също установени със Закона за националната сигурност от 2023 г., трябва да бъде разрешено от съдия по искане на съответно длъжностно лице и подлежи на специални условия и гаранции, включително следните: заповедта се иска по отношение на конкретно лице за целите на разследване на дейност, представляваща заплаха от чужда сила, заповедта ще послужи да се подобри ефективността на разследването и заповедта не се използва за получаване на информация, която е обект на адвокатска тайна или подлежи на изключение по друга причина, например журналистически материали и определени медицински досиета ([132]).

(83) Както е описано в съображения 139—141 от Решение за изпълнение (ЕС) 2021/1772, в правната уредба на Обединеното кралство конкретни правоприлагащи органи, например Националната агенция по престъпността или Столичната полицейска служба, могат също да се ползват с целеви правомощия за разследване съгласно Закона за правомощията за разследване от 2016 г. (ЗПР от 2016 г.) ([133]) с цел предотвратяване или разкриване на тежки престъпления. 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.) и целева намеса в оборудването (част 5 от ЗПР от 2016 г.). Когато министърът издава постановления за съхраняване съгласно част 4 от ЗПР от 2016 г., правоприлагащите органи могат да се ползват и от достъп до съхранените комуникационни данни чрез правомощията за събиране на комуникационни данни съгласно част 3 от ЗПР от 2016 г.

([125]) На разположение на следния адрес: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) Приложение 2 към Закона за националната сигурност от 2023 г. Съответните престъпления съгласно Закона за националната сигурност от 2023 г. са например получаване или разкриване на защитена информация (член 1), получаване или разкриване на търговски тайни (член 3), подпомагане на чужда разузнавателна служба (член 4), извършване на саботаж (член 12) или извършване на конкретна забранена дейност за чужда сила с цел намеса (член 13).

([127]) Вж. точка 2, подточка 1, точка 3, подточка 1, точка 4, подточка 1 и точка 10, подточка 1 от приложение 2 към Закона за националната сигурност от 2023 г.

([128]) Вж. точка 2, подточка 4, буква b), точка 3, подточка 4, букви b) и c), точка 4, подточка 4, букви b) и c) и точка 10, подточка 1 от приложение 2 към Закона за националната сигурност от 2023 г.

([129]) Чрез заповедите за разкриване на информация съгласно приложение 3 към Закона за националната сигурност от 2023 г. служител може да уведоми лице, с което го задължава да предостави информация, да представи документи и/или да отговори на въпроси, свързани с разследване за идентифициране на имущество, свързано с дейност, представляваща заплаха от чужда сила, включително движението или използването на имуществото.

([130]) Чрез заповедите за предоставяне на информация за клиенти съгласно приложение 4 към Закона за националната сигурност от 2023 г. служител може да уведоми финансова институция, с което да изиска от нея да предостави всякаква информация за клиента във връзка с определено лице.

([131]) Чрез заповедите за наблюдение на сметки съгласно приложение 5 финансова институция може да бъде задължена да предостави на служител посочената в заповедта информация за периода и по начина, посочени в заповедта, като този период не може да надвишава 90 дни.

([132]) Точка 2, подточка 1 от приложение 3, точка 1 от приложение 4 и точка 1 от приложение 5 към Закона за националната сигурност от 2023 г.

([133]) 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 правоприлагащите органи и органите за национална сигурност.

(84) След приемането на Решение за изпълнение (ЕС) 2021/1772 Законът за правомощията за разследване от 2016 г., 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, продължи да осигурява правното основание и да определя ограниченията и гаранциите за упражняването на тези правомощия, както е описано в Решение за изпълнение (ЕС) 2021/1772. Важно е да се отбележи, че за да упражнят тези правомощия, съгласно правната рамка от органите продължава да се изисква да получат заповед ([134]), издадена от компетентен орган ([135]) и одобрена от независим съдебен комисар ([136]) (по така наречената „процедура с двойна защита“). Получаването на такава заповед продължава да подлежи на проверка на необходимостта и пропорционалността ([137]).

(85) Същевременно след приемането на Решение за изпълнение (ЕС) 2021/1772 със Закона за правомощията за разследване (изменение) от 2024 г., който получи кралско одобрение през април 2024 г., бяха изменени някои специфични елементи от ЗПР от 2016 г. ([138]) Тези изменения и други съответни промени са анализирани в следващите параграфи, доколкото те се отнасят до условията, ограниченията и гаранциите относно използването на гореспоменатите специфични правомощия за разследване от публичните органи в Обединеното кралство за целите на наказателното правоприлагане, както е оценено в съображения 177—215 от Решение за изпълнение (ЕС) 2021/1772. По отношение на елементите от правната уредба на Обединеното кралство, които не са били изменени с гореспоменатия закон или не са били засегнати от други съответни промени, анализът, извършен в Решение за изпълнение (ЕС) 2021/1772, продължава да бъде валиден.

(86) Що се отнася до целевото събиране и съхраняване на комуникационни данни ([139]), остават в сила условията и гаранциите, уреждащи тези правомощия, както са оценени в Решение за изпълнение (ЕС) 2021/1772. Със Закона за правомощията за разследване (изменение) от 2024 г. бяха пояснени съществуващите гаранции, като в член 11 от ЗПР от 2016 г. (съгласно който незаконното събиране на комуникационни данни от оператор на далекосъобщителна мрежа се определя като престъпление) беше въведен списък с примери на случаи, попадащи в обхвата на „законните правомощия“ по силата на тази разпоредба ([140]). Освен това със Закона за правомощията за разследване (изменение) от 2024 г. допълнително беше пояснено определението за комуникационни данни в член 261 от ЗПР от 2016 г., като изрично беше посочено, че данните за абонати се определят като комуникационни данни ([141]).

([134]) 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.

([135]) В повечето случаи органът, който издава заповедите съгласно ЗПР от 2016 г., е министърът (Secretary of State), 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 ще 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.

([136]) Съдебните комисари подпомагат комисаря по правомощията за разследване — независим орган, който упражнява надзорни функции над упражняването на правомощия за разследване от разузнавателните служби.

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

([138]) На разположение на следния адрес: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) Терминът „комуникационни данни“ обхваща кой, кога, къде и как е осъществил комуникацията, но не и нейното съдържание, т.е. какво е казано или написано. Комуникационните данни могат да включват 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 (вж. член 261, параграф 5 от ЗПР от 2016 г.). Със ЗПР от 2016 г. се 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.

([140]) Например, когато съответното лице получава комуникационните данни при упражняване на законово правомощие на съответния публичен орган или когато комуникационните данни са получени в съответствие със съдебно разпореждане или друго съдебно разрешение. Член 11, параграф 3A от ЗПР от 2016 г., въведен с член 12, параграф 3 от Закона за правомощията за разследване (изменение) от 2024 г.

([141]) Член 261, параграфи 5A и 5B, въведени с член 13, параграф 3 от Закона за правомощията за разследване (изменение) от 2024 г.

(87) Издаването на постановления, с които се изисква съхраняването на комуникационни данни ([142]), продължава да подлежи на ограничения и гаранции, както е описано в съображения 208—209 от Решение за изпълнение (ЕС) 2021/1772, по-специално изисквания за необходимост и пропорционалност и одобрение от независим съдебен комисар. Въпреки че със Закона за правомощията за разследване (изменение) от 2024 г. беше въведена възможността за подновяване на такива постановления, всяко подновяване подлежи на същите условия по отношение на необходимостта и пропорционалността и одобрението от съдебния комисар ([143]).

(88) По отношение на комуникационните данни със Закона за правомощията за разследване (изменение) от 2024 г. беше изменено и определението за оператор на далекосъобщителна мрежа, т.е. възможните адресати на постановленията за съхраняване. Посоченото определение понастоящем включва всяко лице, което „контролира или предоставя далекосъобщителна система, която i) не се намира (изцяло или частично) в Обединеното кралство или не е контролирана от него, и ii) се използва от друго лице за предлагане или предоставяне на далекосъобщителна услуга на лица в Обединеното кралство“ ([144]). Важно е да се отбележи, че съгласно измененото определение продължава винаги да се изисква тясна връзка с пазара на Обединеното кралство. По този начин с изменението се пояснява, че големите дружества със сложна корпоративна структура са обхванати от ЗПР от 2016 г. в своята цялост, без да се разширява обхватът на определението, така че да включва доставчиците на далекосъобщителни услуги, които не са насочени към лица в Обединеното кралство. Това се потвърждава и от Обяснителните бележки към Закона за правомощията за разследване (изменение) от 2024 г., в които се посочва, че целта на това изменение не е да бъдат включени допълнителни дружества в обхвата на съответните правомощия съгласно ЗПР от 2016 г. ([145]), а неговата функция е по същество пояснителна.

(89) Накрая, със Закона за правомощията за разследване (изменение) от 2024 г. бяха въведени някои целеви промени в процедурата за издаване на заповеди, включително по отношение на целево прихващане и целева намеса в оборудването, т.е. правомощия, които могат да бъдат използвани и от специфични правоприлагащи органи в Обединеното кралство с цел предотвратяване или разкриване на тежки престъпления. Промените се отнасят само до конкретния случай, в който тези правомощия се използват за получаване на съобщения на лице, което е член на съответен законодателен орган, или на лична информация за такова лице ([146]). Въпреки че заповедите за целево прихващане и целева намеса в оборудването обикновено може да бъдат издавани от министъра и одобрявани от съдебен комисар (вж. съображения 186—196 и 210—215 от Решение за изпълнение (ЕС) 2021/1772), когато заповедта се отнася до член на Парламента или друг съответен законодателен орган, съгласно членове 26 и 111 от ЗПР се изисква допълнително одобрение от министър-председателя (по така наречената „процедура с тройна защита“). Съгласно Закона за правомощията за разследване (изменение) от 2024 г. министър-председателят вече може да номинира петима министри, които ще бъдат оправомощени да упражняват правомощието на министър-председателя да издава разрешения за такива заповеди, при условие че разрешението е необходимо спешно, а министър-председателят не е в състояние да го издаде поради нетрудоспособност по медицински причини или липса на достъп до сигурни комуникации. Важно е да се отбележи, че ограниченията и гаранциите по отношение на издаването на тези заповеди, както е описано в гореспоменатите съображения на Решение за изпълнение (ЕС) 2021/1772, остават в сила.

3.2.2. *По-нататъшно използване на събраната информация*

(90) 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“), продължава да се извършва при условията, анализирани в съображения 142—156 от Решение за изпълнение (ЕС) 2021/1772.

([142]) Издаването на такива постановления за съхраняване съгласно членове 87—89 от ЗПР от 2016 г. има за цел да се гарантира, че операторите на далекосъобщителни мрежи съхраняват за срок от най-много 12 месеца подходящи комуникационни данни, които иначе биха били заличени, след като вече не са необходими за стопански цели. 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.

([143]) Член 94A от ЗПР от 2016 г., въведен с член 20, параграф 4 от Закона за правомощията за разследване (изменение) от 2024 г.

([144]) Член 261, параграф 10, буква c) от ЗПР от 2016 г., изменен с член 19 от Закона за правомощията за разследване (изменение) от 2024 г.

([145]) Обяснителни бележки към Закона за правомощията за разследване (изменение) от 2024 г., точка 359, достъпни на следния адрес: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Вж. член 26 и член 111 от ЗПР от 2016 г.

(91) Що се отнася до специфичния случай на последващо предаване на данни от Обединеното кралство към Съединените щати, от октомври 2022 г. влезе в сила и се прилага 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“) ([147]), което беше сключено през октомври 2019 г. По силата на Споразумението между Обединеното кралство и САЩ данните, предадени от ЕС на доставчици на услуги в Обединеното кралство, могат да бъдат обект на заповеди за предоставяне на доказателства, издадени от компетентните правоприлагащи органи на САЩ и приложими в Обединеното кралство.

(92) Важно е да се отбележи, че условията и гаранциите, при които може да се издават и изпълняват такива заповеди, както е оценено в съображение 154 от Решение за изпълнение (ЕС) 2021/1772, продължават да се прилагат. По-специално данните, получени по силата на споразумението, се ползват от защита, равностойна на специфичните гаранции, предоставени съгласно така наречения „Рамково споразумение между ЕС и САЩ“ ([148]), които са включени *mutatis mutandis* в Споразумението между Обединеното кралство и САЩ ([149]).

(93) След приемането на Решение за изпълнение (ЕС) 2021/1772 Обединеното кралство обясни, че е пояснило, включително чрез взаимодействие със съответните страни в контекста на прилагането на Споразумението между Обединеното кралство и САЩ, как специфичните гаранции по силата на Рамковото споразумение, предназначени за контекста на сътрудничество между правоприлагащи органи, се адаптират и прилагат към специфичните видове предаване на данни, обхванати от Споразумението между Обединеното кралство и САЩ. По-специално Обединеното кралство обясни, че разпоредбите на Рамковото споразумение, съгласно които се предвижда роля за съответния компетентен орган (която не съществува в случай на пряко сътрудничество между доставчик на услуги от Обединеното кралство и правоприлагащ орган в САЩ), се тълкуват *mutatis mutandis* като отнасящи се до определения орган (както е посочен в Споразумението между Обединеното кралство и САЩ) ([150]) на съответната страна.

(94) Например, що се отнася до уведомяването за инцидент, свързан със сигурността на информацията, по член 10 от Рамковото споразумение между ЕС и САЩ, съгласно който се изисква да бъде уведомен предаващият компетентен орган, Обединеното кралство обясни, че тази разпоредба се прилага *mutatis mutandis*, което означава, че уведомлението следва да бъде подадено до определения орган на страната, предала данните.

(95) Що се отнася до разрешението от страна на предаващия компетентен орган преди всяко последващо предаване на лична информация по член 7 от Рамковото споразумение, Обединеното кралство поясни, че ще прилага тази разпоредба *mutatis mutandis*, което означава, че определеният орган на страната, предала данните, ще трябва да даде разрешение за всяко последващо предаване.

(96) Що се отнася до задълженията по член 8 от Рамковото споразумение относно поддържането на качеството и целостта на информацията, ако разпоредбата се тълкува *mutatis mutandis*, това би означавало, че в случай на проблеми по отношение на качеството и целостта на данните определеният орган на страната, получаваща данните, ще бъде отговорен за осъществяването на връзка с доставчика, предал данните.

([147]) 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.

([148]) 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, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Член 9, параграф 1 от споразумението.

([150]) Съгласно член 1, параграф 8 от Споразумението между Обединеното кралство и САЩ „определен орган“ означава държавното образувание, определено за Обединеното кралство от министъра на вътрешните работи, а за Съединените щати — от главния прокурор.

(97) Що се отнася до защитата по съдебен ред, Обединеното кралство подчерта, че при предаването на данни по силата на Споразумението между Обединеното кралство и САЩ винаги ще участва определеният орган на всяка от страните. Когато САЩ са страната, получаваща данни от доставчици на услуги в Обединеното кралство, Министерството на правосъдието на САЩ ще изпълнява ролята на определен орган. Следователно според тълкуването на Обединеното кралство при всяко искане, издадено въз основа на Споразумението между Обединеното кралство и САЩ, Министерството на правосъдието ще участва като федерален орган, определен съгласно Закона за съдебната защита на САЩ, и по този начин съдебната защита може да бъде упражнена срещу Министерството на правосъдието в съответствие с член 19 от Рамковото споразумение. Освен това Обединеното кралство потвърди пред службите на Комисията, че Законът за съдебната защита не е единственият механизъм за търсене на правна защита. В зависимост от обстоятелствата и контекста на конкретния случай се предоставят алтернативни начини за търсене на съдебна защита по силата на други приложими закони на САЩ.

3.2.3. *Надзор и правна защита*

(98) 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 ЗПР от 2016 г.), надзорът над упражняването на тези правомощия продължава да се осигурява от различни органи, както е оценено в съображения 158—174 от Решение за изпълнение (ЕС) 2021/1772, и продължава да има механизми за правна защита съгласно част 3 от ЗЗД от 2018 г., съгласно ЗПР от 2016 г. и съгласно Закона за правата на човека от 1998 г., както е анализирано в съображения 250—269 от Решение за изпълнение (ЕС) 2021/1772.

(99) По отношение на надзора върху част 3 от ЗЗД от 2018 г. функциите и правомощията на Комисията по информацията са анализирани в съображения 158—160 и съображение 162 от Решение за изпълнение (ЕС) 2021/1772, като са взети предвид измененията, въведени със Закона за данните (използване и достъп), описани в раздел 2.3.1 и 2.3.2 от настоящото решение.

(100) По отношение на използването на тези правомощия след приемането на Решение за изпълнение (ЕС) 2021/1772 комисарят по информацията е обработил множество жалби ([151]), провел е редица разследвания и е предприел принудителни мерки във връзка с обработването на данни от правоприлагащи органи. Между 2021 г. и 2025 г. комисарят по информацията проведе разследвания и издаде официални предупреждения срещу различни полицейски органи за различни видове неизпълнение на задълженията им за защита на данните, например при отговаряне на искания за достъп до данни, при въвеждане на мерки за сигурност за данни от видеонаблюдение, при работа с чувствителна информация от регистри за съдимост, при обединяване на данни на различни лица или при разкриване на лични данни на трети страни ([152]). Освен това комисарят по информацията издаде насоки, становища и документи с указания, например относно правото на достъп или относно това как да се обработват явно неоснователни или прекомерни искания съгласно част 3 от ЗЗД от 2018 г. ([153]).

(101) Що се отнася до използването на правомощия за разследване съгласно ЗПР от 2016 г., независимият и съдебният надзор продължават да се осъществяват от комисаря по правомощията за разследване (IPC), подпомаган от други съдебни комисари, които заедно се наричат съдебни комисари ([154]). В тази област със Закона за правомощията за разследване (изменения) от 2024 г. са направени само ограничени и целеви промени, които не засягат независимостта, задачите и правомощията на съдебните комисари, а са насочени към укрепване на функционирането на практика на съществуващия режим за надзор, по-специално чрез въвеждането на заместници на IPC, на които IPC може да делегира специфични правомощия, когато не е в състояние или не е на разположение да изпълнява функциите си. Тези заместници на IPC трябва да бъдат съдебни комисари и се назначават от IPC ([155]).

([151]) Например в периода 2023—2024 г. Комисията по информацията е получила 1 890 жалби въз основа на ОРЗД и/или ЗЗД от 2018 г. относно организации в подсекторите „Полицейски органи“, „Полицейски сили“ и „Полицейски комисари“. Вж. също годишния доклад и финансовите отчети на комисаря по информацията за 2023—2024 г., достъпни на следния линк: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Допълнителна информация можете да намерите на следния адрес: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) На разположение на следния адрес: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ и https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Вж. съображение 250 от Решение за изпълнение (ЕС) 2021/1772.

([155]) Член 227 от ЗПР от 2016 г., въведен с член 7 от Закона за правомощията за разследване (изменение).

3.3. **Съответни промени във връзка с достъпа и използването от публични органи на Обединеното кралство за целите на националната сигурност**

(102) Що се отнася до правомощията за разследване, упражнявани в контекста на националната сигурност, със ЗПР от 2016 г. продължава да се осигурява правната рамка за упражняването на тези правомощия. В допълнение към измененията, отнасящи се до целевите правомощия за разследване, които при специални условия могат да се използват и от някои правоприлагащи органи, както е описано в съображения 77—85 от настоящото решение, със Закона за правомощията за разследване (изменение) от 2024 г. са въведени изменения и в едно от правомощията, предвидени по силата на ЗПР от 2016 г., които могат да се упражняват масово.

(103) По-конкретно със Закона за правомощията за разследване (изменение) от 2024 г. в новата част 7A от ЗПР от 2016 г. беше въведен специфичен режим за съхраняване и преглед на конкретна подгрупа масиви от лични данни ([156]), т.е. за масивите от данни, при които лицата, за които се отнасят личните данни, могат да имат само ниски (или никакви) разумни очаквания за поверителност във връзка с данните ([157]). Дали масив от лични данни е част от такава конкретна подгрупа набори от данни, се определя от ръководителя на разузнавателна служба въз основа на всички обстоятелства, по-специално i) естеството на данните, ii) степента, до която данните са били направени обществено достояние от лицата или лицата са дали съгласие данните да бъдат направени обществено достояние, iii) ако данните са били публикувани — степента, до която са били публикувани под редакторски контрол или от лице, действащо в съответствие с професионални стандарти, iv) ако данните са били публикувани или по друг начин са били направени обществено достояние — степента, до която те са широко известни, и v) степента, до която данните вече са били използвани в общественото пространство ([158]).

(104) Важно е да се отбележи, че за съхраняването и прегледа на масиви от лични данни, които не попадат в тази категория, т.е. тези, които са по-чувствителни и следователно са свързани с разумни очаквания за поверителност, остава в сила режимът, оценен в съображения 239 и 240 от Решение за изпълнение (ЕС) 2021/1772, по-специално необходимостта от заповед, одобрена първо от министъра, а след това от съдебния комисар, при спазване на изискванията за необходимост и пропорционалност на мярката, както е предвидено в част 7 от ЗПР от 2016 г. ([159]).

(105) В част 7A от ЗПР от 2016 г. се предвиждат два вида разрешения: индивидуално разрешение и разрешение за категория. Съхраняването или съхраняването и прегледът на всеки масив от лични данни, съхраняван съгласно част 7A, трябва да бъдат разрешени по силата на едно от тези разрешения. И за двете разрешения по принцип ([160]) се изисква разрешение от ръководителя на разузнавателната служба (или от лице, действащо от негово име) и одобрение от независим съдебен комисар ([161]). Индивидуалното разрешение се издава от ръководителя на разузнавателна служба при условията, посочени в член 226B, параграф 4 от ЗПР от 2016 г., и след предварително одобрение от съдебните комисари. Съдебният комисар трябва да преразгледа заключенията на лицето, което е издало разрешението, във връзка с това дали член 226A, т.е. изискването за ниски или никакви разумни очаквания за поверителност, се прилага за описания в разрешението масив от лични данни ([162]).

([156]) Със заповедите за масиви от лични данни, издадени съгласно член 200 от ЗПР от 2016 г., разузнавателните агенции се оправомощават да съхраняват и преглеждат набори от данни, които съдържат лични данни, свързани с редица лица, и естеството на данните е такова, че по-голямата част от лицата не представляват и е малко вероятно да представляват интерес за разузнавателната служба при упражняване на нейните функции, и които се съхраняват в електронен вид от разузнавателната служба и се държат за анализ при упражняването на нейните законоустановени функции (вж. също член 199 от ЗПР от 2016 г.).

([157]) Член 226A, параграф 1 от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение) от 2024 г.

([158]) Член 226A, параграф 3 от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение) от 2024 г.

([159]) Със Закона за правомощията за разследване (изменение) от 2024 г. беше изменен член 213 от ЗПР от 2016 г. така, че заповедите за масиви от лични данни престават да бъдат валидни 12 месеца след издаването им. Преди това подобни заповеди трябваше да се подновяват на всеки 6 месеца. Вж. член 3 от Закона за правомощията за разследване (изменение) от 2024 г.

([160]) Индивидуално разрешение може да бъде предоставено без предварително съдебно одобрение само i) ако лицето, издаващо индивидуалното разрешение, счита, че въпросният масив от лични данни попада в обхвата на съществуващо разрешение за категория, или ii) при спешни случаи, вж. член 226B, параграф 6 от ЗПР от 2016 г. Във втория случай решението за предоставяне на спешно индивидуално разрешение трябва да бъде преразгледано от съдебен комисар в срок от три работни дни след деня на издаването му, вж. член 226BC от ЗПР от 2016 г.

([161]) Член 226B, параграф 1 от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение).

([162]) Член 226BB, параграф 1, буква a) от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение) от 2024 г.

(106) С разрешението за категория се разрешават съхраняването или съхраняването и прегледът на описана в разрешението категория масиви от лични данни.

(107) Решението за предоставяне на разрешение за категория се взема от ръководителя на разузнавателната служба, когато той счита, че член 226A се прилага за всеки набор от данни в рамките на категорията и когато решението за предоставяне на разрешение е одобрено от независим съдебен комисар ([163]). Последният трябва да провери дали член 226A, т.е. изискването за ниски или никакви разумни очаквания за поверителност, се прилага за всеки набор от данни, който попада в рамките на описаната в разрешението категория набори от данни ([164]).

(108) Важно е да се отбележи, че когато одобрява решение за предоставяне на индивидуално разрешение или разрешение за категория, съдебният комисар трябва „да прилага същите принципи, каквито биха били приложени от съда във връзка с молба за съдебен контрол“ ([165]), и да разглежда тези въпроси с достатъчна степен на грижа, за да гарантира, че спазва задълженията, наложени съгласно член 2 от ЗПР от 2016 г. (общите задължения във връзка с неприкосновеността на личния живот) ([166]). Освен това издаването на разрешения подлежи на строг последващ надзор, по-специално чрез годишно отчитане пред министъра и Комисията по разузнаване и сигурност на Парламента ([167]), и чрез редовни инспекции на Службата на IPC ([168]).

(109) По отношение на съответните промени в областта на надзора Службата на IPC публикува годишни доклади за 2021 г., 2022 г. и 2023 г., в които е предоставена подробна статистика и информация относно упражняването на правомощията за разследване от страна на разузнавателните служби и правоприлагащите органи в Обединеното кралство ([169]). Освен това в докладите са описани одитите и разследванията на службата, както и констатациите от тях, с което се потвърждава, че IPC продължава да изпълнява своята много важна надзорна функция съгласно режима за правомощията за разследване на Обединеното кралство. Например през 2023 г. службата прегледа обосновките за необходимостта и пропорционалността при упражняването на правомощията за масово прихващане (както е оценено в съображения 218—225 от Решение за изпълнение (ЕС) 2021/1772) от страна на Правителствената централа за комуникации, като заключи, че по-голямата част от получените твърдения имат основателна обосновка, макар и в някои случаи пропорционалността да не е добре обоснована. Тези констатации бяха обсъдени с екипа по съответствие на централата, който пое ангажимент да заяви допълнително вътрешно обучение за повишаване на осведомеността, за да се справи с този проблем ([170]).

(110) Освен това Трибуналът за правомощията за разследване публикува публичен доклад за своята дейност и съдебна практика за периода 2021—2023 г. ([171]). В доклада се посочва, че броят на получените от трибунала дела се е увеличил повече от два пъти от 2017 г. насам, като през 2023 г. са били получени над 400 дела ([172]). Повечето

([163]) Член 226BA от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение).

([164]) Член 226BB, параграф 1, буква b) от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение).

([165]) Член 226BB, параграф 2, буква a) от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение) от 2024 г.

([166]) Член 226BB, параграф 2, буква b) от ЗПР от 2016 г., въведен с член 2 от Закона за правомощията за разследване (изменение) от 2024 г. В съответствие с общите задължения във връзка с неприкосновеността на личния живот, както са определени в член 2 от ЗПР от 2016 г., публичният орган трябва да вземе предвид а) 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, б) 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, в) обществения интерес от целостта и сигурността на далекосъобщителните системи и пощенските услуги, г) и всички други аспекти на обществения интерес от защитата на правото на неприкосновеност на личния живот.

([167]) Членове 226DA и 226DB от ЗПР от 2016 г., въведени с член 2 от Закона за правомощията за разследване (изменение) от 2024 г.

([168]) Вж. годишния доклад на комисаря по правомощията за разследване за 2023 г., достъпен на следния адрес: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, стр. 3.

([169]) Годишните доклади са на разположение на следния адрес: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Вж. параграфи 6.39—6.43 от годишния доклад за 2023 г., достъпен на следния адрес: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) Доклад на Трибунала за правомощията за разследване за периода 2021—2023 г., достъпен на следния адрес: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

([172]) Доклад на Трибунала за правомощията за разследване за периода 2021—2023 г., стр. 5.

жалби са били срещу правоприлагащи органи, следвани непосредствено от органи в областта на сигурността и разузнаването ([173]). Важно е да се отбележи, че през 2022 г. и 2023 г. трибуналът е постановил решения по дела, получени от него преди 2021 г., в които е установил, че публични органи на Обединеното кралство (съответно полицията на Шотландия (Police Scotland) ([174]), полицията на Голям Манчестър (Greater Manchester Police) ([175]), полицията на Съри (Surrey Police) ([176]), МИ5 и министърът на вътрешните работи (Home Secretary) ([177]) са действали незаконосъобразно. Що се отнася до средствата за правна защита, Трибуналът за правомощията за разследване, наред с другото, е разпоредил унищожаването на всички незаконно получени материали, а в един случай и плащането на сума от 12 000 британски лири като справедливо обезщетение за установените нарушения. Следователно с годишния доклад се потвърждава, че Трибуналът за правомощията за разследване ефективно изпълнява важната си роля за гарантирането на надзора и правната защита в областта на наказателното правоприлагане и достъпа до лични данни за целите на националната сигурност.

(111) Освен това в доклада се подчертават и важни събития, като например решение на Европейския съд по правата на човека, в което съдът постановява, че физически лица навсякъде по света могат да предявят пред Трибунала за правомощията за разследване иск във връзка с функционирането на режима на Обединеното кралство за масово прихващане, ако въпросното поведение е извършено от публичен орган на Обединеното кралство и е осъществено в Обединеното кралство ([178]).

4. ЗАКЛЮЧЕНИЕ

(112) Комисията счита, че ОРЗД на Обединеното кралство и ЗЗД от 2018 г., изменени със Закона за данните (използване и достъп), продължават да гарантират ниво на защита на личните данни, предавани от Европейския съюз, което по същество е равностойно на гарантираното от Регламент (ЕС) 2016/679.

(113) Комисията счита освен това, че като цяло механизмите за упражняване на надзор и възможностите за правна защита, предвидени от правото на Обединеното кралство, продължават да 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.

(114) 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, продължава да бъде ограничена до строго необходимото за постигане на въпросната законна цел, и че съществува ефективна правна защита срещу подобна намеса.

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

(116) Това заключение се основава както на съответния вътрешен режим на Обединеното кралство, с промените след приемането на Решение за изпълнение (ЕС) 2021/1772, така и на международните му ангажименти, по-специално на непрекъснатото спазване на Европейската конвенция за правата на човека и непрекъснатото признаване на юрисдикцията на Европейския съд по правата на човека от страна на Обединеното кралство. Следователно продължаващото спазване на такива международни задължения е особено важен елемент от оценката, на която се основава настоящото решение.

([173]) Доклад на Трибунала за правомощията за разследване за периода 2021—2023 г., стр. 12.
([174]) Wilson/Police Scotland [2022] UKIPTrib 5.
([175]) Pendlebury/Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill/Metropolitan Police Service & Independent Office For Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International/Security Service and Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) *Wieder и Guarnieri/UK*, [2023] ECHR 668, вж. също Доклад на Трибунала за правомощията за разследване за периода 2021—2023 г., стр. 6.

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

(117) 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.

(118) 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, през периода на прилагане на Решение за изпълнение (ЕС) 2021/1772, изменено с настоящото решение, предаването на данни от администратор или обработващ лични данни в Европейския съюз към администратори или обработващи лични данни в Обединеното кралство може да се извършва, без да е необходимо допълнително разрешение.

(119) 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 I* ([179]), 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, от която може да се изисква да отправи преюдициално запитване до Съда на ЕС ([180]).

6. **НАБЛЮДЕНИЕ**

(120) Съгласно член 45, параграф 4 от Регламент (ЕС) 2016/679 Комисията трябва да осъществява постоянно наблюдение на съответното развитие в Обединеното кралство, за да прецени дали то все още осигурява по същество равностойно ниво на защита. Това наблюдение е особено важно, тъй като Обединеното кралство ще прилага и привежда в изпълнение изменен режим за защита на данните. Освен това с изменената уредба за защита на данните на Обединеното кралство на министъра се предоставя правомощието да доуточнява тази уредба чрез вторично законодателство. В това отношение следва да се обърне специално внимание на тези допълнителни уточнения, както и на прилагането на практика на изменените правила на Обединеното кралство относно предаването на лични данни на трети държави; на ефективността на упражняването на индивидуалните права, включително всяко съответно развитие на законодателството и практиката по отношение на нововъведените изключения или ограничения, свързани с тези права, както и функционирането на преструктурирания орган на комисаря по информацията, включително по отношение на разглеждането на жалби и упражняването на корективни правомощия, както и на спазването на ограниченията и гаранциите по отношение на правителствения достъп, по-специално във връзка с нововъведената част 7А от ЗПР от 2016 г. Наред с други елементи, развитието на съдебната практика и надзорът от страна на комисаря по информацията и други независими органи следва да се използват за наблюдението от страна на Комисията.

(121) За да се улесни това наблюдение, 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 Решение за изпълнение (ЕС) 2021/1772, изменено с настоящото решение, както и за всяко развитие на практиките, свързани с обработването на личните данни, оценени в Решение за изпълнение (ЕС) 2021/1772, изменено с 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 развитието по отношение на елементите, посочени в съображение 120.

(122) 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 относими действия, предприети от националните органи за 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.

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

([180]) Решение по дело *Schrems I*, т. 65: „В това отношение националният законодател трябва да предвиди правни способи, позволяващи на съответния национален надзорен орган да изложи твърденията за нарушения, които счита 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.“

(123) Когато наличната информация, по-специално информацията, получена в резултат на наблюдението на Решение за изпълнение (ЕС) 2021/1772, изменено с настоящото решение, или предоставена от органите на Обединеното кралство или на държавите членки, показва, че нивото на защита, осигурявано от Обединеното кралство, може вече да не е адекватно, Комисията следва своевременно да информира за това компетентните органи на Обединеното кралство и да поиска предприемането на подходящи мерки в определен срок, който не може да надвишава три месеца. При необходимост този срок може да бъде удължен за определен период от време, като се вземе предвид естеството на разглеждания въпрос и/или мерките, които трябва да бъдат предприети. 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.

(124) 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 или отмяна на настоящото решение.

(125) 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.

(126) 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. ПРЕГЛЕД, СРОК НА ДЕЙСТВИЕ И ПОДНОВЯВАНЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(127) В приложение на член 45, параграф 3 от Регламент (ЕС) 2016/679 и с оглед на факта, че нивото на защита, осигурявано от правната уредба на Обединеното кралство, може да се промени, след приемането на настоящото решение Комисията следва периодично да проверява дали констатациите във връзка с адекватното ниво на защита, осигурявано от Обединеното кралство, са все още фактически и правно обосновани, като взема предвид елементите, изброени в член 45, параграф 2 от Регламент (ЕС) 2016/679. Подобни оценки следва да се извършват най-малко на всеки четири години и следва да обхващат всички аспекти на функционирането на настоящото решение, включително функционирането на съответните механизми за надзор и правоприлагане.

(128) За да извърши преразглеждането, Комисията следва да се срещне със съответни представители на органите на Обединеното кралство, включително с Комисията по информацията. В тази среща следва да могат да участват представители на членовете на Европейския комитет по защита на данните. В рамките на прегледа Комисията следва да поиска от Обединеното кралство да предостави изчерпателна информация по всички аспекти, които са от значение за установяването на адекватно ниво на защита. Комисията следва също така да потърси обяснения във връзка с всяка получена от нея информация, която е от значение за настоящото решение, включително от Европейския комитет по защита на данните, отделни органи за защита на данните, групи на гражданското общество, публични или медийни доклади или всякакви други налични източници на информация.

(129) Въз основа на прегледа Комисията следва да изготви публичен доклад, който се представя на Европейския парламент и на Съвета.

(130) Комисията трябва също така да вземе предвид, че уредбата за защита на данните, оценена в настоящото решение и в Решение за изпълнение (ЕС) 2021/1772, може да претърпи допълнителни промени.

(131) Поради това е целесъобразно да се предвиди настоящото решение да се прилага за срок от шест години, считано от влизането му в сила.

(132) 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**

(133) Европейският комитет по защита на данните публикува становище ([181]), което бе взето предвид при изготвянето на настоящото решение.

(134) Мярката, предвидена в настоящото решение, е в съответствие със становището на комитета, създаден по силата на член 93 от Регламент (ЕС) 2016/679.

(135) Поради това Решение за изпълнение (ЕС) 2021/1772 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Член 1, параграф 2 от Решение за изпълнение (ЕС) 2021/1772 се отменя.

Член 2

Член 4 от Решение за изпълнение (ЕС) 2021/1772 се заменя със следното:

„*Член 4*

Срокът на действие на настоящото решение изтича на 27 декември 2031 г., освен ако не бъде удължен в съответствие с процедурата, посочена в член 93, параграф 2 от Регламент (ЕС) 2016/679.“

Член 3

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 19 декември 2025 година.

За Комисията
Michael MCGRATH
Член на Комисията

([181]) Становище 26/2025 относно проекта на Решение за изпълнение на Европейската комисия съгласно Регламент (ЕС) 2016/679 относно адекватното ниво на защита на личните данни от страна на Обединеното кралство, достъпно на следния адрес: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.