Становище 14/2021 по проекта на решение за изпълнение на Европейската комисия съгласно Регламент (ЕС) 2016/679 относно адекватното ниво на защита на личните данни в Обединеното кралство

Прието на 13 април 2021 г.

СЪДЪРЖАНИЕ

Европейският комитет по защита на данните

като взе предвид член 70, параграф 1, буква т) от 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 (наричан по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство (ЕИП), и по-специално приложение XI и Протокол 37 към него, изменено с Решение на Съвместния комитет на ЕИП № 154/2018 от 6 юли 2018 г.[1],

като взе предвид членове 12 и 22 от своя Правилник за дейността,

ПРИЕ СЛЕДНОТО СТАНОВИЩЕ:

1. РЕЗЮМЕ

1. На 19 февруари 2021 г.[2] Европейската комисия одобри проекта си на решение за изпълнение (наричан по-нататък „проекторешението“) съгласно ОРЗД относно адекватното ниво на защита на личните данни от Обединеното кралство. След това Европейската комисия започна процедурата за официалното му приемане.

2. На същата дата Европейската комисия поиска становището на Европейския комитет по защита на данните (наричан по-нататък „ЕКЗД“)[3]. Оценката на ЕКЗД за адекватността на нивото на защита, осигурявано от Обединеното кралство, е направена въз основа на прегледа на самото проекторешение, както и на анализа на документацията, предоставена на разположение от Европейската комисия.

3. При извършването на оценката ЕКЗД насочи своето внимание както към общите аспекти на ОРЗД, заложени в проекторешението, така и към достъпа на държавните органи до лични данни, предавани от ЕИП за целите на правоприлагането и националната сигурност, включително към средствата за правна защита, достъпни за физическите лица от ЕИП. ЕКЗД оцени също така дали гаранциите, предвидени в правната уредба на Обединеното кралство, са налични и ефективни.

4. Като основен справочен източник ЕКЗД използва своя Референтен документ относно адекватното ниво на защита съгласно ОРЗД[4], приет през февруари 2018 г., и Препоръки 02/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение[5].

[1] Позоваванията на „държави членки“ в настоящото становище следва да се разбират като позовавания на „държавите членки на ЕИП“.

[2] Вж. съобщение за медиите на Европейската комисия, „Защита на данните: Европейската комисия открива процедура относно потоците от лични данни към Обединеното кралство“, 19 февруари 2021 г., https://ec.europa.eu/commission/presscorner/detail/bg/ip_21_661.

[3] Пак там.

[4] Вж. Работна група по член 29, Референтен документ относно адекватното ниво на защита, приет на 28 ноември 2017 г., преработен за последен път и приет на 6 февруари 2018 г., РД 254 ред.01 (одобрен от ЕКЗД, вж. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); наричан за краткост „*Референтен документ относно адекватното ниво на защита съгласно ОРЗД*“).

[5] Вж. Препоръки 02/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение, приети на 10 ноември 2020 г., https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_bg.

1.1. Области на сближаване

5. Основната цел на ЕКЗД е да представи на Европейската комисия становище относно адекватността на нивото на защита, осигурявано на физическите лица в Обединеното кралство. Важно е да се признае, че ЕКЗД не очаква правната уредба на Обединеното кралство да възпроизведе европейското законодателство за защита на данните.

6. ЕКЗД обаче припомня, че за да се смята, че дадена трета държава осигурява адекватно ниво на защита съгласно член 45 от ОРЗД и практиката на Съда на Европейския съюз (наричан по-нататък „Съд на ЕС“), се изисква нейното законодателство да бъде приведено в съответствие със същината на основополагащите принципи, залегнали в ОРЗД. Уредбата на Обединеното кралство за на защита на данните до голяма степен се основава на уредбата на ЕС в тази област (по-конкретно ОРЗД и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета , наричана по-нататък „Директива относно правоприлагането “ или „ДП“), което се дължи на факта, че до 31 януари 2020 г. Обединеното кралство беше държава членка на ЕС. Освен това в Закона на Обединеното кралство за защита на личните данни от 2018 г., който влезе в сила на 23 май 2018 г. и отмени Закона на Обединеното кралство за защита на данните от 1998 г., допълнително е уточнено прилагането на ОРЗД в правото на Обединеното кралство, заедно с транспонирането на Директивата на ЕС относно правоприлагането в областта на защитата на данните, като са предоставени правомощия и са наложени задължения на националния надзорен орган по защита на данните — Службата на комисаря за информацията на Обединеното кралство, (наричан по-нататък „СКИ“). Поради това ЕКЗД признава, че правната уредба на Обединеното кралство за защита на данните в по-голямата си част отразява ОРЗД.

7. **При анализа на правото и практиката на трета държава, която доскоро е била държава членка на ЕС, се вижда, че ЕКЗД е установил много аспекти, които са равностойни по същество.**

8. В областта на защитата на данните ЕКЗД отбелязва, че е налице солидна съгласуваност между уредбата на ОРЗД и правната уредба на Обединеното кралство по отношение на някои основни разпоредби, като понятийния апарат (например „лични данни“; „обработване на личните данни“; „администратор“); основанията за законосъобразно и добросъвестно обработване за легитимни цели; ограничение на целите; качество и пропорционалност на данните; съхраняване на данни, сигурност и поверителност на данните; прозрачността; специални категории данни; директен маркетинг; автоматизирано вземане на решения и профилиране.

1.2. Предизвикателства

9. Обединеното кралство до неотдавна беше държава членка на ЕС; затова при анализа на нейното право и практика ЕКЗД е установил много аспекти, които са равностойни по същество. Същевременно с оглед на ролята си в процеса по приемане на заключение относно адекватното ниво на защита на данните, но и с оглед на времевите ограничения, ЕКЗД взе решение да съсредоточи вниманието си върху онези аспекти, по отношение на които смята, че има нужда от по-внимателно разглеждане и по-подробен анализ.

10. Въпреки това продължават да съществуват предизвикателства и ЕКЗД смята, че следните въпроси следва да бъдат оценени допълнително, за да се гарантира постигането на равностойно по същество ниво на защита, и тяхното развитие в Обединеното кралство трябва да бъде наблюдавано внимателно от Европейската комисия.

1.2.1. Общи положения

11. Първото предизвикателство е общо и е свързано с наблюдението на промените в правната система на Обединеното кралство за защита на данните като цяло. В действителност правителството на Обединеното кралство е заявило намерението си да разработи отделни и независими политики за защита на данните, и евентуално желание за отклоняване от правото на ЕС за защита на данните. Тези политически декларации все още не са материализирани в правната уредба на Обединеното кралство. Това евентуално бъдещо **отклонение обаче би могло да създаде рискове за поддържането на нивото на защита, което се осигурява при предаването на лични данни от ЕС. Поради това, Европейската комисия се приканва от влизането в сила на нейното решение за адекватното ниво на защита да наблюдава внимателно тези промени и да предприеме необходимите действия, включително чрез изменение и/или спиране на прилагането на решението, ако е необходимо.**

1.2.2. Общи аспекти на защитата на данните

12. Първо, т.нар. „**изключение във връзка с имиграционния контрол**“, предвидено в **приложение 2 към Закона за защита на данните от 2018 г., част 1**, параграф 4, **съдържа „широка“ формулировка**. По-специално, то се прилага и когато лични данни не се събират с цел имиграционен контрол от администратор, а се предоставят от последния на друг администратор, който обработва такива лични данни за целите на имиграционния контрол.

13. ЕКЗД приканва Европейската комисия да провери текущото състояние на производството *Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)*, и тъй като това съдебно решение не е окончателно (*res judicata*), да провери дали то е потвърдено или е отхвърлено в решението на апелативния съд, вземайки предвид всяка актуализация в това отношение и посочвайки я в решението. **ЕКЗД приканва също така Европейската комисия да предостави в решението относно адекватното ниво на защита допълнителна информация относно изключението във връзка с имиграционния контрол[6], по-специално по отношение на необходимостта и пропорционалността на подобно широко прилагане на изключението в правото на Обединеното кралство, особено, когато се касае за физически лица..** Същевременно, ЕКЗД приканва Европейската комисия да изследва допълнително дали в правната уредба на Обединеното кралство съществуват или биха могли да бъдат предвидени допълнителни гаранции, например чрез правно обвързващи инструменти, които да допълнят изключението във връзка с имиграционния контрол, като повишат неговата предвидимост и гаранциите за субектите на данни, което ще даде възможност също така за по-добра и своевременна оценка, и наблюдение на изискванията за необходимост и пропорционалност.

14. Второ, въпреки че ЕКЗД признава, че Обединеното кралство е отразило в по-голямата си част глава V от ОРЗД в своята правна уредба за защита на данните, ЕКЗД установи определени аспекти **във връзка с последващото предаване**, които биха могли да подкопаят нивото на защита на трансферираните лични данни от ЕИП.

---

[6] Също като резултат от текущата проверка на използването на изключението във връзка с имиграционния контрол, посочено в т. 5 от Разяснителната рамка на правителството на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел Е3: приложение 2 „Ограничения“, 13 март 2020 г., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

15. В действителност член 44 от ОРЗД[7] предвижда, че последващото предаване на лични данни се осъществява само при условие че нивото на защита на физическите лица, осигурено от ОРЗД, не се подлага на риск. **Това означава, че не само законодателството на Обединеното кралство трябва да бъде „равностойно по същество“ на законодателството на ЕС във връзка с обработването на лични данни, предавани от Обединеното кралство съгласно бъдещото решение относно адекватното ниво на защита, но също така че правилата, приложими в Обединеното кралство във връзка с последващото предаване на тези данни на трети държави, трябва да гарантират продължаващото предоставяне на равностойно по същество ниво на защита.**

16. Въпреки че ЕКЗД отбелязва способността на Обединеното кралство съгласно неговата правна уредба да признава, че дадена територия предоставя адекватно ниво на защита на личните данни, ЕКЗД желае да подчертае, че към днешна дата, за тези територии може да не се прилага решение относно адекватното ниво на защита, издадено от Европейската комисия, и да не осигуряват ниво на защита, което е „по същество равностойно“ на гарантираното в ЕИП. Това би могло да доведе до потенциални рискове за защитата, осигурявана на предаваните от ЕИП лични данни, особено ако в бъдеще уредбата на Обединеното кралство за защита на данните се отклони от достиженията на правото на ЕС. В допълнение Обединеното кралство вече е признало за адекватни третите държави, за които има заключение, че предоставят адекватно ниво на защита на данните съгласно Директива 95/46/ЕО[8], като Европейската комисия скоро ще провери тези констатации, но изводите от проверката все още не са известни.

17. **В ситуации като горепосочените Европейската комисия следва да изпълнява своята роля, свързана с наблюдението, и в случай че равностойното по същество ниво на защита на предаваните от ЕИП лични данни не се запази, тя следва да обмисли изменение на решението относно адекватното ниво на защита, за да въведе конкретни гаранции за данните, предавани от ЕИП, и/или да спре прилагането на решението относно адекватното ниво на защита.**

18. **По отношение на международните споразумения, сключени между Обединеното кралство и трети държави,** Европейската комисия се приканва да проучи взаимодействието между уредбата на Обединеното кралство за защита на данните извън обхвата на Споразумението за достъп до електронни данни с цел противодействие на тежката престъпност, сключено между Обединеното кралство и Съединените американски щати (наричани по-нататък „САЩ“)[9] (наричано по-нататък „Споразумение между Обединеното кралство и САЩ във връзка със

[7] *„Предаване на лични данни, които се обработват или са предназначени за обработване след предаването им на трета държава или на международна организация, се осъществява само при условие че са спазени другите разпоредби на настоящия регламент, само ако администраторът и обработващият лични данни спазват условията по настоящата глава, включително във връзка с последващо предаване на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация. Всички разпоредби на настоящата глава се прилагат, за да се гарантира, че нивото на защита на физическите лица, осигурено от настоящия регламент, не е изложено на риск.“*

[8] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995 г., стр. 31).

[9] Вж. Споразумение между правителството на Обединеното кралство Великобритания и Северна Ирландия и правителството на Съединените американски щати относно достъпа до електронни данни с цел противодействие на тежката престъпност, Вашингтон, окръг Колумбия, САЩ, 3 октомври 2019 г., https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

Закона CLOUD“), по-специално, за да гарантира приемственост на нивото на защита, когато личните данни се предават от ЕС на Обединеното кралство въз основа на решението относно адекватното ниво на защита за Обединеното кралство, и след това се предават по-нататък на други трети държави; както и да извършва постоянно наблюдение и при необходимост да предприема действия, в случай че сключването на международни споразумения между Обединеното кралство и трети държави застрашава да подкопае нивото на защита на личните данни, предвидено в ЕС.

19. Освен това, Европейската комисия се приканва да наблюдава дали Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD предоставя подходящи допълнителни гаранции, отчитайки нивото на чувствителност на категориите засегнати данни и специфичните изисквания за прехвърляне на електронни доказателства пряко от доставчици на услуги, а не между органи, както и да оцени при какви обстоятелства може да се предоставят гаранции чрез подходящо прилагане на адаптирания вариант на рамковото споразумение между ЕС и САЩ[10].

20. Освен това ЕКЗД отбелязва, че последващо предаване може да се извършва също така от Обединеното кралство към трета държава въз основа на **инструменти за прехвърляне съгласно приложимото законодателство на Обединеното кралство в областта на защитата на личните данни**[11]. Проследявайки делото *Schrems II*[12], ЕКЗД приканва Европейската комисия да предостави уверения, в решението относно адекватното ниво на защита, за въвеждането на ефективни гаранции, отчитайки също така законодателството на приемащата трета държава.

21. Относно липсата **на защити, предвидени съгласно член 48 от ОРЗД** в законодателството на Обединеното кралство, ЕКЗД приканва Европейската комисия да представи допълнителни уверения и конкретни позовавания на законодателството на Обединеното кралство, с които се гарантира, че нивото на защита съгласно правната уредба на Обединеното кралство е по същество равностойно на нивото на защита, гарантирано в ЕИП.

22. По отношение на **процедурните и правоприлагащите механизми** ЕКЗД отбелязва, че съществуването и ефективното функциониране на независим надзорен орган; съществуването на система, която да гарантира добро ниво на съответствие; както и система за достъп до подходящи механизми за правна защита, осигуряващи средства на гражданите в ЕИП да упражняват правата си и да търсят правна защита, без да се сблъскват с обременителни бариери пред административната и съдебната защита, са основните елементи, които трябва да характеризират дадена уредба за защита на данните, която е съгласувана с европейската такава.

23. ЕКЗД признава, че Обединеното кралство е отразило в по-голямата част съответните разпоредби на ОРЗД в ОРЗД на Обединеното кралство и в Закона за защита на данните от 2018 г.; независимо от това Европейската комисия се приканва да наблюдава постоянно всички промени в правната уредба и в практиката на Обединеното кралство, които биха могли да доведат до вредоносни въздействия върху тези области.

[10] Вж. Споразумение между Съединените американски щати и Европейския съюз относно защитата на личната информация във връзка с предотвратяването, разследването, разкриването и наказателното преследване на престъпления, декември 2016 г. (наричано по-нататък „Рамково споразумение между ЕС и САЩ“),https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8.

[11] Вж. членове 46 и 47 от ОРЗД на Обединеното кралство.

[12] Вж. делото *Schrems II*.

1.2.3. Относно достъпа на публични органи до предадени данни на Обединеното кралство

24. ЕКЗД отбелязва съществените промени в правната уредба и в практиката на Обединеното кралство, приложими за агенциите за сигурност и разузнаване, особено по отношение на прихващането и събирането на комуникационни данни. ЕКЗД разбира, че тези промени са, *между другото*, в отговор на производството, образувано пред Съда на ЕС и пред Европейския съд за правата на човека (наричан по-нататък „ЕСПЧ“), и техните неотдавнашни съдебни решения в този контекст.

25. По-специално, ЕКЗД приветства факта, че Обединеното кралство е създало Трибунала с правомощия за разследване (наричан по-нататък „ТПР”). ТПР е компетентен да разглежда дела за упражняването на правомощия за разследване не само от страна на правоприлагащи органи, но и от разузнавателни служби. Поради това ЕКЗД смята, че ТПР функционира като надлежно създаден съд по смисъла на член 47 от Хартата на основните права на ЕС (наричана по-нататък „Хартата на ЕС“).

26. Освен това, ЕКЗД отбелязва като положително и важно подобрение въвеждането на „съдебни комисари“ в Закона за правомощията за разследване от 2016 г. (наричан по-нататък „ЗПР от 2016 г.“). Той разбира, че важна функция на съдебния комисар е в отделни случаи предварително да одобрява различни мерки за наблюдение, включително целенасочено прихващане и масово събиране на комуникационни данни (т.нар. процедура „с двойна защита“).

27. За да се оцени ефективността на това допълнително ниво на надзор обаче, ЕКЗД вижда необходимост от по-нататъшно поясняване на сценариите, в които е възможно законно прихващане без одобрение от комисаря с правомощия за разследване (наричан по-нататък „КПР“) или от съдебните комисари, и приканва Европейската комисия да оцени допълнително и да демонстрира, че дори в случаите, в които не се прилага процедурата с „двойна защита“, правната уредба на Обединеното кралство предвижда подходящи гаранции, включително чрез ефективен последващ надзор и възможности за правна защита на гражданите, осигурявайки по този начин ниво на защита, което е по същество равностойно на предоставяното в рамките на ЕС.

28. Освен това, ЕКЗД приканва Европейската комисия да оцени допълнително условията, при които може да се направи позоваване на спешност и да предостави пояснения относно възможните начини за упражняване на правата на засегнатите субекти на данни, и предоставените им възможни средства за правна защита при операциите, които водят до намеса в оборудването, особено в случай на дерогация от процедурата с двойна защита.

29. В допълнение ЕКЗД смята, че е необходимо допълнително пояснение и оценка относно масовото прихващане, по-конкретно във връзка с подбора и използването на съответните критерии, за да се изясни степента, до която достъпът до лични данни отговаря на прага, определен от Съда на ЕС, както и какви гаранции са предвидени за защита на основните права на гражданите, чиито данни са прихванати, включително сроковете за съхранение на данните. Независима оценка от компетентните надзорни органи на Обединеното кралство би била особено полезна. ЕКЗД подчертава също така, че вероятно е още по-съществено, че „свързаната с чужди държави комуникация“, която е в обхвата на практиките за масово прихващане, дава основание да се заключи, че данни могат да бъдат пряко прихванати и събрани в масив в рамките на ЕС от Обединеното кралство, включително и информация,

предавана транзитно между ЕС и Обединеното кралство, която би могла да попадне в обхвата на проекторешението. С оглед на значението на този аспект ЕКЗД приканва Европейската комисия да наблюдава внимателно развитието по този въпрос.

30. Освен това, ЕКЗД подчертава съгласуваната оценка на ЕСПЧ и Съда на ЕС по отношение на масовото прихващане и припомня изразените опасения във връзка с вторичните данни, за които би следвало да има въведени специални гаранции поради тяхната чувствителност. Поради това, Европейската комисия се приканва внимателно да прецени дали гаранциите, предвидени в правото на Обединеното кралство относно тази категория лични данни, осигуряват по същество ниво на защита, равностойно на гарантираното в ЕИП.

31. В тази връзка ЕКЗД е запознат с факта, че публичният доклад на Комисията по разузнаване и сигурност от 2016 г. относно използването на правомощия за създаване на масиви от данни[13] засяга практики, свързани с предишната правна уредба, която впоследствие беше заменена от ЗПР от 2016 г. Въпреки това, той вижда необходимост от допълнителна независима оценка и надзор на използването на инструменти за автоматизирана обработване от компетентните надзорни органи на Обединеното кралство и приканва Европейската комисия да направи допълнителна оценка на този въпрос и на гаранциите, които ще бъдат и/или биха могли да бъдат предоставени на субектите на данни в ЕИП.

32. ЕКЗД споделя възгледа, изразен от КПР, че са необходими допълнителни проверки и наблюдение, за да се гарантира, че се поддържат и ще продължат да се подобряват прилаганите на практика гаранции от компетентните органи в областта на националната сигурност и разузнаването за коригиране на несъответствия с прилагането на съответното законодателство. ЕКЗД приветства също така факта, че КПР извърши последваща проверка на своя подход за инспектиране на масовото прихващане през 2019 г., *„ което включваше внимателен преглед на технически сложните начини, по които на практика се извършва масовото прихващане*“, и се ангажира да включи „*подробно разглеждане на критериите за подбор и за търсене, за които се споменава по-горе от ЕСПЧ*“, при провеждането на проверките за масовото прихващане от 2020 г. нататък. Като се има предвид значението на този аспект, ЕКЗД се опасява, че все още не е извършено подробно разглеждане на критериите за подбор и на критериите за търсене от КПР, и призовава Европейската комисия да наблюдава внимателно случващото се, особено след като конкретният формат на този надзор предстои да бъде изяснен.

33. ЕКЗД подчертава, че що се отнася до разкриванията на данни в чужбина, прилагането на изключение относно националната сигурност съгласно правото на Обединеното кралство може да доведе до липсата на гаранции, осигуряващи спазването на принципите за ограничение на целите, необходимостта и пропорционалността, или предвиждащи предоставяне или зачитане на достатъчно права на гражданите, надзор и средства за правна защита в третата държава на местоназначение. Поради това, ЕКЗД препоръчва на Европейската комисия да разгледа допълнително всички гаранции, предвидени в законодателството на Обединеното кралство, свързано с разкриването на данни в чужбина, по-специално, по отношение на прилагането на изключенията относно националната сигурност.

[13] Вж. Доклад за проверка на правомощията относно прихващането на масиви от данни, представен от независимия оценител на законодателството за борба с тероризма, август 2016 г., https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

34. Накрая, ЕКЗД има опасения относно други форми на споделяне и оповестявания на информация въз основа на други инструменти, по-специално, различните международни споразумения, сключени от Обединеното кралство с други трети държави, особено когато тези инструменти остават недостъпни за обществеността, като например Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на комуникацията. Последиците от това споразумение биха могли да доведат до заобикаляне на установените гаранции във връзка с достъпа и използването на лични данни за целите на националната сигурност. ЕКЗД смята, че сключването на двустранни или многостранни споразумения с трети държави за целите на сътрудничеството в областта на разузнаването, с които се осигурява правно основание за пряко прихващане и придобиване на лични данни или за предаване на лични данни на тези държави, може значително да повлияе, и на условията за последващо използване на събраната информация, тъй като тези споразумения може да засегнат вече оценената правна уредба на Обединеното кралство в областта на защитата на личните данни.

1.3. Заключение

35. ЕКЗД смята, че оценката за адекватността на нивото на защита, осигурявано от Обединеното кралство, е уникална поради предишния статут на Обединеното кралство като държава членка на ЕС. Освен това тя ще е първото решение относно адекватното ниво на защита, включващо клауза за прекратяване на действието.

36. ЕКЗД признава наличието на много области на сближаване между правната уредба на Обединеното кралство за защита на данните и тази на ЕС. В същото време обаче и след внимателен анализ на проекторешението на Европейската комисия и на законодателството на Обединеното кралство в областта на защитата на данните бяха установени редица предизвикателства, които са разгледани подробно в настоящото становище. В тази връзка ЕКЗД желае да подчертае изключително важната роля на Европейската комисия за наблюдението на всички промени в Обединеното кралство.

37. Предвид гореизложеното, ЕКЗД препоръчва на Европейската комисия да намери решения на предизвикателствата, повдигнати в това становище. Европейската комисия също така се приканва да наблюдава внимателно всички промени в Обединеното кралство, които може да окажат влияние върху равностойното ниво на защита на личните данни, и да предприеме бързо подходящи действия, когато е необходимо.

2. ВЪВЕДЕНИЕ

2.1. Уредба на Обединеното кралство за защита на данните

38. Уредбата на Обединеното кралство за защита на данните до голяма степен се основава на уредбата на ЕС в тази област (по-конкретно ОРЗД и ДП), което се дължи на факта, че до 31 януари 2020 г. Обединеното кралство беше държава членка на ЕС. Освен това в Закона на Обединеното кралство за защита на личните данни от 2018 г., който влезе в сила на 23 май 2018 г. и отмени Закона на Обединеното кралство за защита на данните от 1998 г., допълнително е уточнено прилагането на ОРЗД в правото на Обединеното кралство, заедно с транспонирането на Директивата на ЕС относно правоприлагането в областта на защитата на данните, както и са предоставени правомощия и са наложени задължения на националния надзорен орган по защита на данните — Службата на комисаря по информацията на Обединеното кралство.

39. Както е посочено в съображение 12 от проекторешението на Европейската комисия, правителството на Обединеното кралство прие Закона от 2018 г. за оттеглянето от Европейския съюз, с който пряко приложимите законодателни актове на Съюза бяха включени в правото на Обединеното кралство. Съгласно този закон министрите на Обединеното кралство имат правомощието чрез нормативни актове да въвеждат вторично законодателство във връзка с въвеждането на необходимите изменения, с които да запази приложението на законодателството на Съюза след оттеглянето на Великобритания като се вземат предвид изискванията на националното право.

40. Вследствие на това правната уредба, приложима в Обединеното кралство след края на преходния период[14], се състои от:

- Общия регламент относно защитата на данните на Обединеното кралство (наричан по-нататък „ОРЗД на Обединеното кралство“), включен в правото на Обединеното кралство съгласно Закона от 2018 г. за оттеглянето от Европейския съюз и изменен с Наредбите от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС);

- Закона за защита на данните от 2018 г.(наричан по-нататък „ЗЗД от 2018 г.“), изменен с Наредбите от 2019 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) и Наредбите от 2020 г. за защита на данните, неприкосновеността на личния живот и електронните съобщения (изменения и т.н.) (Напускане на ЕС); както и

- ЗПР от 2016 г.

(наричани заедно „Уредба на Обединеното кралство за защита на данните“).

2.2. Обхват на оценката на ЕКЗД

41. Проекторешението на Европейската комисия е резултат от оценка на уредбата на Обединеното кралство за защита на данните, последвана от обсъждания с правителството на Обединеното кралство. В съответствие с член 70, параграф 1, буква т) от ОРЗД от ЕКЗД се очаква да предостави независимо становище по изводите на Европейската комисия, да посочи недостатъците в уредбата за осигуряване на адекватно ниво на защита, ако има такива, и да се опита да отправи предложения за отстраняването им.

42. Както е посочено в Референтния документ относно адекватното ниво на защита съгласно ОРЗД: *„предоставената от Европейската комисия информация следва да бъде изчерпателна и да дава възможност на ЕКЗД да извърши собствена оценка на нивото на защита на данните в третата държава“*[15].

43. Във връзка с това следва да се отбележи, че ЕКЗД получи своевременно само част от документите от значение за разглеждането на правната уредба на Обединеното кралство. Комитетът получи по-голямата част от законодателството на Обединеното кралство, упоменато в проекта на решение, чрез електронните препратки, посочени в него. Европейската

[14] Определено е преходният период да изтече на 31 декември 2020 г., като след тази дата правото на ЕС вече не се прилага в Обединеното кралство. „Междинният период“ е определено да приключи най-късно на 30 юни 2021 г. и се отнася за допълнителния период, през който прехвърлянето на лични данни от ЕИП към Обединеното кралство не се смята за предаване на лични данни.
[15] Вж. РД 254 ред.01, стр. 3.

комисия не беше в състояние да предостави писмени обяснения и ангажименти от страна на Обединеното кралство във връзка с обмена на информация между органите на Обединеното кралство и Европейската комисия във връзка с настоящото разглеждане[16].

44. С оглед на горното и поради ограничения срок (2 месеца), с който разполага ЕКЗД, за да приеме настоящото становище, ЕКЗД избра да се съсредоточи върху някои конкретни въпроси, представени в проекторешението, и да предостави своя анализ и становището си по тях.

45. При анализа на правото и практиката на трета държава, която доскоро е била държава членка на ЕС, се вижда, че ЕКЗД е установил много аспекти, които са равностойни по същество. С оглед на ролята си в процеса по приемане на заключенията относно адекватното ниво на защита на данните и на обема нормативни актове и практика, които трябва да бъдат анализирани, ЕКЗД взе решение да съсредоточи вниманието си върху онези аспекти, по отношение на които установи най-голяма потребност от по-внимателен анализ. В допълнение, в съответствие с практиката на Съда на ЕС много важна част от анализа касае правния режим за достъп на органи на националната сигурност до лични данни, предадени на Обединеното кралство, и националната им практика. Необходимо е обаче да се има предвид, че националната сигурност очевидно е област на правото и практиката, в която законодателството на държавите членки не е хармонизирано на равнище ЕС и затова може да има разлики.

46. ЕКЗД взе предвид приложимата европейска уредба в областта на защитата на личните данни, в т.ч. членове 7, 8 и 47 от Хартата на ЕС, с които се защитават съответно правото на зачитане на личния и семейния живот, правото на защита на личните данни и правото на ефективни правни средства за защита и на справедлив съдебен процес; както и член 8 от Европейската конвенция за правата на човека (наричана по-нататък „ЕКПЧ“), с който се защитава правото на зачитане на личния и семейния живот. В допълнение към горното ЕКЗД взе предвид изискванията на ОРЗД, както и съответната съдебна практика.

47. Целта на това разглеждане е да предостави на Европейската комисия становище за оценката на адекватността на нивото на защита в Обединеното кралство. Концепцията за „адекватно ниво на защита“, която вече съществуваше съгласно Директива 95/46/ЕО, е доразвита от Съда на ЕС. Важно е да се припомни стандартът, установен от Съда на ЕС в делото *Schrems I*, а именно

[16] По отношение на: член 48 от ОРЗД (бележка под линия 78 от проекторешението); засилени гаранции и мерки за сигурност, прилагани от администраторите, когато обработването се извършва в контекста на националната сигурност (бележка под линия 64 от проекторешението); изискването към администратора да прецени дали има нужда да се позовава на изключението за всеки отделен случай, дори когато е издадено удостоверение за национална сигурност (съображение 126 и бележка под линия 172 от проекторешението); факта, че защитата, предвидена в Рамковото споразумение между ЕС и САЩ ще се прилага за цялата създадена или получена лична информация по Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD, независимо от характера или вида на отправящия искането орган, по отношение на конкретното прилагане на гаранциите за защита на данните, които все още се обсъждат между Обединеното кралство и САЩ, потвърждението, че органите на Обединеното кралство ще се съгласят Споразумението да влезе в сила едва след като се убедят, че прилагането му отговаря на предвидените в него законови задължения, включително яснота по отношение на спазването на стандартите за защита на данните за всички данни, поискани съгласно Споразумението (съображение 153 от проекторешението); случаите, когато данните се предават от ЕС към Обединеното кралство в рамките на обхвата на настоящото проекторешение, както и факта, че винаги ще има „връзка с Британските острови“ и поради това всяка намеса в оборудването, обхващаща такива данни, подлежи на задължителното условие за наличие на заповед по член 13, параграф 1 от ЗПР от 2016 г. (съображение 206 от проекторешението); и представените примери на оперативни цели (съображение 216 и бележка под линия 369 от проекторешението).

че докато „степента на защита“ в третата държава трябва да бъде „по същество равностойна“ на гарантираната в ЕС*, то е възможно средствата, до които третата страна прибягва в това отношение, за да гарантира такава степен на защита, да са различни от прилаганите вътре в ЕС*“[17]. Ето защо целта не е да се отрази точка по точка европейското законодателство, а да се установят съществените и основните изисквания на разглежданото законодателство. Адекватно ниво на защита може да се постигне чрез комбинация от права за субектите на данни и задължения за лицата, които обработват данните или които упражняват контрол върху това обработване, и надзор от страна на независими органи. Правилата за защита на данните обаче са ефективни само ако се прилагат и се спазват на практика. Поради това е необходимо да се разгледа не само съдържанието на правилата, които са приложими за предаването на лични данни на трета държава или на международна организация, но също така въведената система за гарантиране на ефективността на тези правила. Ефикасните механизми за правоприлагане са от съществена важност за ефективността на правилата за защита на данните[18].

2.3. Общи коментари и опасения

2.3.1. Международни ангажименти, поети от Обединеното кралство

48. Съгласно член 45, параграф 2, буква в) от ОРЗД и Референтния документ относно адекватното ниво на защита на данните съгласно ОРЗД[19], когато оценява адекватността на нивото на защита на трета държава, Европейската комисия взема предвид, наред с другото, международните ангажименти, които съответната трета държава е поела, или други задължения, произтичащи от участието ѝ в многостранни или регионални системи, по-конкретно по отношение на защитата на личните данни, както и изпълнението на тези задължения. Освен това следва да се вземе предвид присъединяването на третата държава към Конвенцията на Съвета на Европа от 28 януари 1981 г. за защита на лицата при автоматизираната обработка на лични данни (наричана по-нататък „Конвенция № 108“)[20] и допълнителния протокол към нея[21].

49. **В това отношение ЕКЗД приветства факта, че Обединеното кралство се е придържало към ЕКПЧ и е под юрисдикцията на ЕСПЧ. Освен това Обединеното кралство се е придържало и към Конвенция № 108 и допълнителния протокол към нея и през 2018 г. е подписало Конвенция № 108+[22] и понастоящем работи по ратифицирането ѝ.**

2.3.2. Възможни бъдещи отклонения на уредбата на Обединеното кралство за защита на данните

50. Както се посочва в съображение 281 от проекта на решение, Европейската комисия трябва да вземе под внимание, че в края на преходния период, предвиден в Споразумението за

[17] Вж. решение на Съда на ЕС от 6 октомври 2015 г., C-362/14, *Maximilian Schrems/Data Protection Commissioner*, ECLI:EU:C:2015:650 (наричано по-нататък „*делото Schrems I*“), т. 73—74.

[18] Вж. РД 254 ред.01, стр. 2.

[19] Вж. РД 254 ред.01, стр. 2.

[20] Вж. Конвенция за защита на лицата при автоматизираната обработка на лични данни, Конвенция № 108, 28 януари 1981 г.

[21] Вж. Допълнителен протокол към Конвенцията за защита на лицата при автоматизирана обработка на лични данни, по отношение на надзорните органи и трансграничните информационни потоци, открит за подписване на 8 ноември 2001 г.

[22] Вж. Протокол за изменение на Конвенцията за защита на лицата при автоматизираната обработка на лични данни (наричана по-нататък „Конвенция 108+“), 18 май 2018 г.

оттегляне[23], Обединеното кралство управлява, прилага и изпълнява свой собствен режим за защита на личните данни и веднага щом спре да се прилага временната разпоредба по член FINPROV.10A от Споразумението за търговия и сътрудничество между ЕС и Обединеното кралство[24], това може да включва по-конкретно изменения или промени в уредбата в областта на защитата на личните данни, оценена в проекторешението, както и други свързани с това промени.

51. Поради това, Европейската комисия е решила да включи в своя проект на решение клауза за изтичане на срока на действие[25], като определи дата за изтичане на този срок четири години след влизането му в сила.

52. Важно е да се отбележи, че възможността министрите и държавният секретар на Обединеното кралство да въвеждат вторично законодателство след края на междинния период може в бъдеще да доведе до значително отклоняване на уредбата на Обединеното кралство за защита на данните от тази на ЕС.

53. В действителност правителството на Обединеното кралство е заявило намерението си да разработи отделни и независими политики за защита на данните, които биха могли да доведат до отклоняване от правото на ЕС за защита на данните[26]. Това намерение обхваща включването на аспекти на личните данни в търговски споразумения[27] — практика, която предполага риск

[23] Вж. Споразумение за оттеглянето на Обединеното кралство Великобритания и Северна Ирландия от Европейския съюз и Европейската общност за атомна енергия (ОВ L 029, 31.1.2020 г., стр. 7).

[24] Вж. Споразумение за търговия и сътрудничество между Европейския Съюз и Европейската общност за атомна енергия, от една страна, и Обединеното кралство Великобритания и Северна Ирландия, от друга страна (ОВ L 444, 31.12.2020 г., стр. 14).

[25] Вж. член 4 от проекторешението. Вж. също така съображение 282 от проекторешението.

[26] Националната стратегия на Обединеното кралство за данните (последна актуализация на 9 декември 2020 г., https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) включва следното като една от своите цели: *„Защита на международния поток от данни. Потокът от трансгранична информация захранва глобалните бизнес операции, веригите на доставки и търговията, засилвайки растежа в целия свят. Освен това той играе по-широка обществена роля. Предаването на лични данни гарантира, че заплатите на гражданите ще бъдат изплатени, и им помага да се свържат с близките си от далечни места. И както показа епидемията от коронавирус, споделянето на здравни данни може да подпомогне жизненоважни научни изследвания на заболяванията, като същевременно обединява държавите в техния отговор на извънредни ситуации, свързани със здравето в световен мащаб.* ***След като напусна Европейския съюз, Обединеното кралство ще отстоява ползите, които могат да му осигурят данните.*** *Ще насърчаваме националните най-добри практики и работата с международни партньори,* ***за да гарантираме, че данните няма да бъдат неподходящо ограничавани от националните граници и от разнородни регулаторни режими****, така че да могат да бъдат използвани в пълния си потенциал.*“ (подчертаването е допълнено).

[27] Пак там: *„Улесняване на трансграничните потоци от данни:* ***Ще работим глобално за премахване на пречките пред международните потоци от данни. Ще договорим амбициозни разпоредби относно данните в нашите търговски преговори*** *и ще използваме нашето ново независимо място в Световната търговска организация, за да влияем върху търговските правила за получаване на по-добри данни.* ***Ще премахнем пречките пред предаването на международни данни*** *в подкрепа на растежа и иновациите, включително чрез развиване на нова способност на Обединеното кралство, която да предоставя нови и иновативни механизми за международно предаване на данни. Ще работим също така с партньорите от Г20 за създаване на оперативна съвместимост между режимите на националните данни с цел намаляване на трудностите при предаването на данни между отделните държави“*. (подчертаването е допълнено).

от намаляване на нивото на защита на личните данни, предоставяно от Обединеното кралство[28].

54. И на последно място, след края на преходния период Обединеното кралство не само вече не е обвързано от съдебната практика на Съда на ЕС, но е вероятно и приетите дотогава решения на Съда на ЕС, които се смятат за запазена съдебна практика в правната уредба на Обединеното кралство, повече да не са задължителни за него, по-специално, тъй като Обединеното кралство има възможност да изменя запазеното право на ЕС след края на междинния период и неговият Върховен съд не е обвързан от запазената съдебна практика на ЕС[29].

55. **Като се вземат предвид рисковете, свързани с възможното отклонение на уредбата на Обединеното кралство за защита на данните от достиженията на правото на ЕС след края на междинния период, ЕКЗД приветства решението на Европейската комисия да въведе в проекторешението клауза за изтичане на срока му на действие след четири години. ЕКЗД обаче би искал да подчертае значението на ролята на Европейската комисия, свързана с наблюдението[30]. В действителност, Европейската комисия следва да наблюдава всички промени в Обединеното кралство, които може да окажат влияние върху равностойното ниво на защита на личните данни, предавани по силата на решението относно адекватното ниво на защита в Обединеното кралство, в текущ и постоянен порядък след влизането му в сила. В допълнение Европейската комисия следва да предприеме подходящи действия, като спре прилагането, измени или обжалва решението относно адекватното ниво на защита, въз основа на съответните обстоятелства, ако след приемането на решението относно адекватното ниво на защита установи признаци, че в Обединеното кралство вече не се осигурява адекватно ниво на защита.**

56. От своя страна ЕКЗД ще положи максимални усилия да информира Европейската комисия за всички действия, предприети от надзорните органи по защита на данните на държавите членки (наричани по-нататък „НОЗД“) в търговския или в публичния сектор, и по-специално във връзка с жалби, подадени от субекти на данни в ЕИП, свързани с предаването на лични данни от ЕИП към Обединеното кралство.

3. ОБЩИ АСПЕКТИ НА ЗАЩИТАТА НА ДАННИТЕ

3.1. Принципи, отнасящи се до съдържанието:

57. Глава 3 от Референтния документ относно адекватното ниво на защита съгласно ОРЗД е посветена на „Принципи, отнасящи се до съдържанието“. Системата на дадена трета държава трябва да ги включва, за да може нейното ниво на защита на личните данните да се смята за равностойно по същество на гарантираното в ЕС. ЕКЗД признава факта, че Обединеното

[28] Вж. Резолюция на Европейския парламент от 12 декември 2017 г. *„По пътя към цифрова търговска стратегия“* (2017/2065(INI)), раздел V, в който се подчертава, че *„Защитата на личните данни не подлежи на преговори в контекста на търговските споразумения с [ЕС]“*, на разположение на адрес: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_BG.pdf. Вж. също Резолюция на Европейския парламент от 25 март 2021 г. относно Доклада на Комисията за оценка на изпълнението на Общия регламент относно защитата на данните две години след неговото прилагане, параграф 28, който гласи: *„подкрепя практиката на Комисията за разглеждане на защитата на данните и потоците от лични данни отделно от търговските споразумения;* , https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_BG.html.

[29] Вж. член 6, параграфи 3—6 от Закона от 2018 г. за оттеглянето от Европейския съюз.

[30] Вж. член 45, параграф 4 от ОРЗД.

кралство не разполага с кодифицирана конституция, в смисъл на един-единствен документ, в който да се определят неговите ръководни основополагащи правила. Правото на зачитане на личния и семейния живот (и правото на защита на личните данни като част от него) и правото на справедлив съдебен процес[31] обаче са включени в Закона за правата на човека от 1998 г. и конституционната стойност на този закон е призната от съдилищата на Обединеното кралство. В действителност със Закона за правата на човека от 1998 г. са въведени правата, съдържащи се в ЕКПЧ[32]. В допълнение, в Закона за правата на човека от 1998 г. се провъзгласява, че всяко действие на публичните органи трябва да бъде съвместимо с ЕКПЧ [33].

58. С изключение на структурните и формалните разлики между законодателството на Обединеното кралство и това на ЕС, ЕКЗД отбелязва, че подходът на Обединеното кралство в областта на защитата на личните данни е подобен на този в ЕС, което се дължи на факта, че до 31 януари 2020 г. Обединеното кралство беше държава членка на ЕС. В резултат на това много принципи, отнасящи се до съдържанието, са съгласувани с ОРЗД; и следователно предоставят ниво на защита, което е по същество равностойно на гарантираното от ЕС. ЕКЗД реши да не развива допълнително анализа на тези принципи на съдържанието, които са съгласувани със законодателството на ЕС, и е удовлетворен от анализа на Европейската комисия, представен в нейния проект на решение. Такива принципи, отнасящи се до съдържанието, включват например следното: понятията (например „лични данни“; „обработване на личните данни“; „администратор“); основанията за законосъобразно и добросъвестно обработване за легитимни цели; ограничение на целите; качество и пропорционалност на данните; съхраняване на данни, сигурност и поверителност на данните; прозрачност; специални категории данни; директен маркетинг; автоматизирано вземане на решения и профилиране. ЕКЗД отбелязва също така, че ОРЗД на Обединеното кралство и ЗЗД от 2018 г. включват принципи, отнасящи се до съдържанието, които надхвърлят изискванията на Референтния документ относно адекватното ниво на защита съгласно ОРЗД, и отразяват принципите, включени в ОРЗД; с което повишават нивото на предоставяното в Обединеното кралство ниво на защита. Принципите, отнасящи се до съдържанието, са свързани например с уведомленията за нарушаване на сигурността на личните данни, длъжностното лице по защита на данните, оценките на въздействието върху защитата на данните или защитата на данните на етапа на изготвяне и по подразбиране.

59. Както е посочено във Въведението обаче, ЕКЗД желае да обърне специално внимание в настоящото становище на определени въпроси, по отношение на които има опасения и би искал да получи пояснения от Европейската комисия.

3.1.1. Правото на достъп, коригиране, изтриване и възражение

60. Така нареченото „изключение във връзка с имиграционния контрол“, предвидено в **приложение 2 към ЗЗД от 2018 г., част 1**, параграф 4, позволява на администраторите, участващи в „имиграционния контрол“, да не изпълняват определени права на субекти на данни, предвидени от ЗЗД от 2018 г., ако има вероятност това да *„накърни поддържането на ефективен имиграционен контрол“* или *„разследването или разкриването на дейности, които биха подкопали поддържането на ефективен имиграционен контрол“*.

[31] Вж. членове 6 и 8 от ЕКПЧ (приложение 1 към Закона за правата на човека от 1998 г.).
[32] За повече информация вж. съображения 8—10 от проекторешението.
[33] Вж. член 6 от Закона за правата на човека от 1998 г.

61. Както е потвърдено от Европейската комисия в нейното проектерешение[34] и както е посочено в Становището на Комисията по граждански свободи, правосъдие и вътрешни работи на Европейския парламент за сключването от името на Съюза на Споразумението за търговия и сътрудничество между ЕС и Обединеното кралство[35], това изключение е **„широко“ формулирано**. То се прилага по отношение на следните права: право на информиране; право на достъп; право на изтриване; право на ограничаване на обработването; и право на възражение.

62. Наред с това е важно да се отбележи, че това изключение се прилага и когато лични данни не са събрани с цел имиграционен контрол от администратор („администратор 1“), а са предоставени от последния на друг администратор („администратор 2“), който обработва такива лични данни за целите на имиграционния контрол (например Министерството на вътрешните работи на Обединеното кралство)[36].

---

[34] Вж. съображения 62—65 от проектерешението.

[35] Във връзка с това, относно **широката формулировка** на изключението във връзка с имиграционния контрол, вж. Становище на Комисията по граждански свободи, правосъдие и вътрешни работи на Европейския парламент за сключването от името на Съюза на 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, и на Споразумението между Европейския съюз и Обединеното кралство Великобритания и Северна Ирландия относно процедурите за сигурност при обмен и защита на класифицирана информация (2020/0382(NLE), 5 февруари 2021 г., https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_EN.pdf, т. 10: *„припомня във връзка с това резолюциите на Парламента от февруари и юни 2020 г., посочвайки **общото и широко изключение** по отношение на обработването на лични данни за имиграционни цели в Закона за защита на данните на Обединеното кралство“*, и т. 11: *„смята, че **общото и широко** изключение във връзка с обработването на лични данни за имиграционни цели на Закона за защита на данните на Обединеното кралство [...] трябва да бъде изменено, преди да се вземе валидно решение относно адекватното ниво на защита;“* (подчертаването е допълнено).

[36] Вж. примера, даден в „Насоки относно Общия регламент относно защитата на данни (ОРЗД)“ на СКИ, версия 01 от януари 2021 г., стр. 307 (подчертаването е допълнено): *„Частна организация (администратор 1) подава сигнал до Министерството на вътрешните работи на Обединеното кралство (администратор 2) за служител, за който смята, че е подал фалшиви документи, за да удостовери своята самоличност и квалификации, за да получи работа. Работодателят предоставя на Министерството на вътрешните работи съответната информация. Правото на лицето да бъде информирано, че личните му данни са предоставени на Министерството на вътрешните работи, е ограничено, доколкото привеждането му в сила би могло да накърни разследването.*
***Следователно работодателят няма задължение да информира лицето, че неговите лични данни са предадени на Министерството на вътрешните работи**, а на свой ред **Министерството на вътрешните работи** няма задължение да предостави на лицето уведомление за поверително третиране на личните му данни, за да го информира, че в момента обработва неговите лични данни. Изключението се отнася в еднаква степен и за двамата администратори.*
*Служителят обаче иска копие от своите лични данни от Министерството на вътрешните работи, което го разследва в момента. **Министерството на вътрешните работи може да се позове на изключението**, за да задържи част от неговите данни, ако има вероятност разкриването да накърни разследването. Ако служителят отправи подобно искане до **своя работодател, той също може да приложи изключението** в същата степен.“*
С други думи, както е пояснено на стр. 300: *„В повечето случаи Министерството на вътрешните работи или някоя от неговите агенции или изпълнители ще бъдат администраторите, които прилагат това изключение. Важно е да се отбележи обаче, че прилагането на това изключение не е ограничено до Министерството на вътрешните работи. То може да се прилага и от други администратори, като работодатели, университети и полицията, които се свързват с Министерството на вътрешните работи по имигрантски въпроси.“*

63. В делото *Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin) (03 октомври 2019 г.)* жалбоподателите оспорват законността на изключението във връзка с имиграционния контрол на основанието, че то противоречи на член 23 от ОРЗД и е несъвместимо с правата на неприкосновеност на личния живот и на защита на личните данни, гарантирани по членове 7 и 8 от Хартата на ЕС. Висшият съд на Англия и Уелс (наричан по-нататък „Висш съд“) разгледа въпроса дали изключението във връзка с упражняването на имиграционен контрол в точка 4 от част 1 от приложение 2 към ЗЗД от 2018 г. е законосъобразно и заключи в полза на неговата законосъобразност.

64. Висшият съд по-специално е сметнал, че:

- *„[…] изключението във връзка с имиграционния контрол очевидно е въпрос от „важен обществен интерес“ и преследва легитимна цел. […]“*, т. 30;

- *„изключението във връзка с имиграционния контрол отговаря на изискванията за това мярката да бъде „в съответствие със закона. […]“*, т. 38;

- *„На изключението във връзка с имиграционния контрол може да се прави позоваване само ако и доколкото съответствието с „посочените разпоредби на ОРЗД“* ***има вероятност да накърни*** *поддържането на ефективен имиграционен контрол или разследването, или разкриването на дейности, които биха подкопали поддържането на ефективен имиграционен контрол. Изразът „има вероятност да накърни“ в контекста на Закона за защита на данните от 1998 г. (който предшестваше ЗЗД от 2018 г.) е тълкуван като „много значима и сериозна възможност да бъде накърнен конкретният обществен интерес. Степента на риск трябва да бъде такава, че да е „твърде възможно“ да бъдат накърнени тези интереси, дори ако вероятността да настъпи рискът е по-скоро малка[…].“*, т. 39 (подчертаването е допълнено).

65. Следва да се отбележи, че доколкото е известно на ЕКЗД, горното съдебно решение не е окончателно и е било обжалвано.

66. Както е посочено в Насоките на ЕКЗД относно ограниченията съгласно член 23 от ОРЗД („член 23 от Насоките относно ограниченията“)[37] *„[...] в контекста на ОРЗД ограничения* ***се предвиждат чрез законодателна мярка*** *относно* ***ограничен брой права на субекти на данни и/или задължения на администратор****, посочени в член 23 от ОРЗД,* ***зачитане на същината*** *на разглежданите основни права и свободи****, която е необходима и пропорционална мярка*** *в едно демократично общество и защитава основанията, предвидени в член 23, параграф 1 от ОРЗД [...]“*.[38]

67. ЕКЗД припомня също така, че в съображение 41 от ОРЗД се посочва, че *„[к]огато в настоящия регламент се прави позоваване на* ***правно основание или законодателна мярка****, това не налага непременно приемането на законодателен акт от парламент, без с това да се засягат изискванията съгласно конституционния ред на съответната държава членка. Такова правно основание или законодателна мярка обаче следва да бъдат* ***ясни и точни и прилагането им следва да бъде предвидимо за лицата, за които се прилагат****, в*

[37] Вж. Насоки на ЕКЗД 10/2020 относно ограниченията съгласно член 23 от ОРЗД, версия 1.0, приети на 15 декември 2020 г., понастоящем в процес на приключване след обществена консултация, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/guidelines-102020-restrictions-under-article-23_bg.

[38] Вж. Насоки съгласно член 23 от ОРЗД, т. 9, стр. 5.

съответствие с практиката на Съда на Европейския съюз [...] и на Европейския съд по правата на човека“ (подчертаването е допълнено).

68. Въпреки че ЕСПЧ посочи, че *„[д]опълнително, що се отнася до думите „в съответствие със закона“ и „предписано от закона“, които се появяват в членове 8 до 11 от Конвенцията, [ЕСПЧ] отбелязва, че винаги е разбирал термина „закон“ в неговия „материален“ смисъл, а не в неговия „формален“ смисъл; той е включвал както „писан закон“, обхващащ приложенията на нормативни актове от по-нисък порядък и регулаторни мерки, предприемани от регулаторни органи с независими правомощия за разработване на правила, които са им делегирани от парламент, така и неписан закон. Под „закон“ трябва да се разбира както право, изразено в законодателен акт* ***, така и прецедентно „право“***[39], в Насоките съгласно член 23 от ОРЗД се припомня, че *„[с]ъгласно практиката на Съда на ЕС всяка* ***законодателна мярка****, приета въз основа на член 23, параграф 1 [от] ОРЗД, трябва по-специално* ***да отговаря на конкретните изисквания, посочени в член 23, параграф 2 от ОРЗД****. В член 23, параграф 2 от ОРЗД се посочва, че законодателните мерки налагат ограничения на правата на субектите на данни, а задълженията на администратора включват, когато е целесъобразно,* ***специални разпоредби относно няколко критерия, посочени по-долу****. По правило всички посочени по-долу изисквания* ***следва да бъдат включени в законодателната мярка*** *за налагане на ограничения съгласно член 23 [от] ОРЗД.“*[40]

69. Във връзка с това може да бъде отбелязано, че **самото изключение във връзка с упражняването на имиграционен контрол** не **включва следните елементи, посочени в член 23, параграф 2 от ОРЗД**:

- „гаранциите за предотвратяване на злоупотреби или незаконен достъп или предаване“ — г);

[39] Вж. ЕСПЧ, делото *Sanoma Uitgevers B.V./The Netherlands*, 14 септември 2010 г., EC:ECHR:2010:0914JUD003822403, т. 83 (подчертаването е допълнено).

[40] Вж. Насоки съгласно член 23 от ОРЗД, т. 45 и 46, стр. 11. Съгласно член 52, параграф 3 от Хартата на ЕС, *„Доколкото настоящата Харта съдържа права, съответстващи на права, гарантирани от Европейската конвенция за защита на правата на човека и основните свободи, техният смисъл и обхват са същите като дадените им в посочената Конвенция. Тази разпоредба не пречи на правото на Съюза да предоставя по-широка защита“*. По отношение на понятието „**предписан от закона**“ съгласно член 52, параграф 1 от Хартата на ЕС критериите, разработени от ЕСПЧ, следва да се използват съгласно предложеното в няколко становища на генералния адвокат на Съда на ЕС, вж. например Становищата в съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:572, т. 137—154, и по делото C-70/10, *Scarlet Extended*, ECLI:EU:C:2011:255, т. 88—114. Следователно може да се направи позоваване, наред с останалото, на решението на ЕСПЧ по делото *Weber and Saravia/Germany*, т. 84: *„Съдът потвърждава, че изразът „****в съответствие със закона****“ по смисъла на член 8, § 2 [от ЕКПЧ] изисква, на първо място, оспорената мярка да има някакво основание в* ***националното право****; той се позовава също така на* ***качеството на съответния закон****, като поставя изискването той да бъде достъпен за засегнатото лице, което освен това трябва да бъде в състояние да предвиди последиците му за себе си, както и да бъде съвместим с върховенството на закона.“* (подчертаването е допълнено).
Вж. също съображение 41 от ОРЗД: *„Такова [правно основание или] законодателна мярка обаче следва да бъдат* ***ясни*** *и* ***точни*** *и прилагането им следва да бъде* ***предвидимо за лицата,*** *за които се прилагат, в съответствие с практиката на Съда на Европейския съюз (...) и на Европейския съд по правата на човека“* (подчертаването е допълнено).

- „администратора или категориите администратори“ — д)[41];
- „рисковете за правата и свободите на субектите на данни“ — ж);
- „правото на субектите на данни да бъдат информирани за ограничаването, освен ако това би било в разрез с целта на ограничаването“ — з).

70. „Насоките относно Общия регламент относно защитата на данните (ОРЗД)“ на СКИ[42], включващи глава относно „изключението във връзка с имиграционния контрол“, дават пояснения за изключението във връзка с имиграционния контрол, но **не могат** *сами по себе си* да предоставят задължителни правила за допълването му. Освен това въпросът с „качеството на закона“ е особено значим предвид важността на ограничените права и разширяването на изключението[43].

---

[41] Вж. горепосоченото дело на Висшия съд, т. 54: *„Според мен няма нищо незаконно в това, че изключението във връзка с имиграционния контрол е приложимо **за всички администратори**, които обработват данни за посочените цели. Както посочват ответниците, без точки 4(3)—(4) изключението във връзка с имиграционния контрол би станало недействително в случаите, когато данните се получават от трети страни (например местен орган или агенция „Приходи и митници“ на Нейно Величество) за целите на поддържане на ефективен имиграционен контрол.“* (подчертаването е допълнено), с което се потвърждава **обобщеното** прилагане на ограниченията.

[42] „Насоки относно Общия регламент относно защитата на данните (ОРЗД)“ на СКИ, версия от 1 януари 2021 г., стр. 299—307.

[43] Вж. горепосоченото дело на Висшия съд, точка 57: *„Господин Найт ме информира, че Комисарят финализира насоките относно изключението, но те ще имат „задължителен“ характер само в смисъл, че ще бъдат издадени по силата на правомощията на Комисаря съгласно член 57, параграф 1 от ОРЗД. Те няма да имат правен статут съгласно ЗЗД от 2018 г..“*

Логиката на въвеждането на правно обвързващи насоки, подкрепени от СКИ, е разгледана по-специално в точки 56—60 от съдебното решение:

„56. Накрая се връщам към твърдението на Комисаря, че без придружаващи законови насоки за предоставяне на гаранции относно значението и прилагането на изключението във връзка с имиграционния контрол, то не би било пропорционално прилагане на член 23, параграф 1 от ОРЗД. Господин Найт заяви, че ако бъде допълнена с тези насоки, разпоредбата е пропорционална.

57. Господин Найт ме информира, че Комисарят финализира насоките относно изключението, но те ще имат „законов“ характер само в смисъл, че ще бъдат издадени по силата на правомощията на Комисаря съгласно член 57, параграф 1 от ОРЗД. Те няма да имат правен статут съгласно ЗЗД от 2018 г.. Разбирам също, че Министерството на вътрешните работи е разработило проект на вътрешни насоки за персонала относно изключението във връзка с имиграционния контрол (вж. [22] по-горе). На практика насоките, издадени от Комисаря, оказват влияние, независимо от правната основа. Комисарят обаче няма правомощие да издава „задължителни“ насоки от типа, който Върховният съд е имал предвид в делото Christian Institute (в [101] и [107]). Изглежда, че е необходимо да се въведе първично законодателство, ако се прецени, че такова е нужно, за да може насоките относно изключението във връзка с имиграционния контрол да имат същия статут като кодекси на добрите практики, предвидени в параграфи 121—124 от ЗЗД от 2018 г.

58. В своя довод относно законовите насоки г-н Найт твърди, че контекстът, в който ще се наложи използването на изключението във връзка с имиграционния контрол, е неизменно свързан с опасенията относно необходимостта и пропорционалността на съществуването и използването му. Той обръща внимание специално на два въпроса в правния контекст. Първо, за личните данни, за които се прилага изключението във връзка с имиграционния контрол, е вътрешно присъщо да включват специална категория данни по смисъла на член 9, параграф 1 от ОРЗД (т.е. данни, „разкриващи расов или етнически произход“). Такива данни са идентифицирани в ОРЗД, тъй като те изискват по-висока мярка на защита (Становище 1/15 [2019] 3 C.M.L.R. 25 в [141]). Второ, основна предпоставка на закона за защита на данните е, че по-специално правото на достъп на субекта е

71. *Дори още повече* „**тестът за накърняване**“ не предвижда гаранции за предотвратяване на злоупотреба или незаконен достъп или предаване, както и неговото приложение от Министерството на вътрешните работи.

72. Предвид гореизложено ЕКЗД отбелязва, че са необходими допълнителни пояснения относно прилагането на изключението във връзка с имиграционния контрол.

73. Освен това ЕКЗД отбелязва липсата на правно обвързващ акт, който да пояснява изключението във връзка с имиграционния контрол, така че то да се разглежда като равностойно по същество на член 23 от ОРЗД и членове 7 и 8 от Хартата на ЕС. Същевременно ЕКЗД смята, че необходимостта и пропорционалността на широкия обхват, по отношение на лицата и страните, на изключението във връзка с имиграционния контрол трябва да бъдат заявени допълнително от Европейската комисия и подкрепени с доказателства.

74. **В заключение ЕКЗД приканва Европейската комисия да провери текущото състояние на производството *Open Rights Group & Anor, R (ищци)/Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin)*, цитирано по-горе, и тъй като съдебното решение не е окончателно (*res judicata*), да провери дали е потвърдено или отхвърлено обжалваното решение, да вземе предвид всяка актуална информация и да я посочи в решението относно адекватното ниво на защита. ЕКЗД приканва също така Европейската комисия да предостави допълнителна информация относно необходимостта и пропорционалността на изключението във връзка с имиграционния контрол, по-специално във връзка с широкия обхват на прилагане *по отношение на лицата и страните*.**

75. **Същевременно ЕКЗД приканва Европейската комисия да изследва допълнително дали в правната уредба на Обединеното кралство съществуват или биха могли да бъдат предвидени допълнителни мерки, например, чрез правно обвързващи инструменти, които да допълнят изключението във връзка с имиграционния контрол, като повишат неговата**

от голямо значение, тъй като дава възможност за упражняване на другите предоставени на субектите на данни права (вж. дело YS/Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 в [44]).

59. Господин Найт откроява четири основни въпроса от практическо естество. Първо, когато администраторите не обясняват на субектите на данни, че са се позовали на законово изключение, нито дават обширно обобщение на причините за това, субектът на данни няма да узнае за прилагането на изключението и в резултат на това няма да бъде в състояние да го оспори ефективно. Второ, субектите на данни ще разчитат особено много на администраторите да прилагат изключението внимателно и само доколкото им е необходимо. Въпреки че всеки субект на данни има право да подава жалба до Комисаря относно прилагането на изключението или да открие съдебно производство пред съдилищата, има вероятност субектът на данни да не познава правата си и да няма финансови средства да предприеме правни действия в обстоятелства, в които е нужно своевременно и точно спазване на правата за защита на данните. Трето, като имигрант субектът на данни е вероятно да бъде в уязвимо положение. Четвърто, това не е абстрактен въпрос в контекста на доказателствата на ответниците относно използването на изключението във връзка с имиграционния контрол (вж. [4] по-горе).

60. Господин Найт предполага, че има тесен паралел между настоящото оспорване на изключението във връзка с имиграционния контрол и аргументацията на Съда по делото Christian Institute [2016] UKSC 51. Както в делото Christian Institute, той твърди, че изключението във връзка с имиграционния контрол е широко, по отношение на него се използват неопределени термини, прилага се нисък праг, подлежи на контрол, който не е виден от разпоредбата, и е приложимо за много широк контекст и права. За разлика от делото Christian Institute, по отношение на изключението във връзка с имиграционния контрол няма обществено достъпни насоки, то все още няма законов статут, който трябва да бъде спазван.”

предвидимост и гаранциите за субектите на данни, което ще даде възможност също така за по-добра и своевременна оценка, и наблюдение на изискванията за необходимост, и пропорционалност.

3.1.2. Ограничения за последващото предаване на данни

76. Член 44 от ОРЗД предвижда, че предаване и последващ трансфер на лични данни се осъществява само при условие че нивото на защита на физическите лица, осигурено от ОРЗД, не се излага на риск. Поради това предаваните лични данни от ЕИП към Обединеното кралство въз основа на решението относно адекватното ниво на защита трябва да имат ниво на защита, което по същество е равностойно на нивото, осигурено от правната уредба на ЕС за защита на личните данни. **Това означава, че законодателството на Обединеното кралство трябва не само да бъде „по същество равностойно“ на законодателството на ЕС във връзка с обработването на личните данни, предавани на Обединеното кралство съгласно проекторешението, но и че правилата, приложими в Обединеното кралство във връзка с последващото предаване на тези данни на трети държави, трябва да гарантират продължаващото предоставяне на равностойно ниво на защита.**

77. Във връзка с това е важно всяко последващо предаване на лични данни от ЕИП от страна на Обединеното кралство към друга трета държава да бъде надлежно защитено с гаранции или да се извършва в съответствие с правилата за дерогациите[44], за да се гарантира непрекъснатостта на защитата, предоставена от законодателството на ЕС. **В действителност ако не може да бъде предоставена такава защита, не следва да се извършва последващо предаване на лични данни на ЕИП.**

78. ЕКЗД признава, че в по-голямата част Обединеното кралство е отразило глава V от ОРЗД в ОРЗД на Обединеното кралство (членове 44—49) и в ЗЗД от 2018 г[45]. **ЕКЗД обаче е установил определени аспекти от правната уредба на Обединеното кралство във връзка с последващо предаване, които биха могли да подкопаят нивото на защита на предаваните лични данни от ЕИП.**

79. **Първото предизвикателство, установено от** ЕКЗД, е свързано с признаването от страна на Обединеното кралство, след изпълнение на процедурата, описана подробно в ЗЗД от 2018 г., на трети държави, международни организации или територии[46] като адекватни получатели. В действителност последващото предаване на лични данни от ЕИП може да се извършва от Обединеното кралство към други трети държави въз основа на бъдещ евентуален регламент на Обединеното кралство относно адекватното ниво на защита[47].

80. По-специално, както е пояснено в съображение 77 от проекта на решение, държавният секретар на Обединеното кралство има правомощието да признае, че трета държава (или територия или сектор в рамките на трета държава), международна организация или описание на такава държава, територия, сектор или организация гарантира адекватно ниво на защита на личните данни, след консултация със СКИ[48]. Когато оценява адекватността на нивото на

[44] Вж. член 49 от ОРЗД на Обединеното кралство.
[45] Вж. членове 17A, 17B, 17C и 18 ЗЗД от 2018 г.
[46] Вж. член 17A от ЗЗД 2018 от 2018 г.
[47] Еквивалентът на Обединеното кралство на решението относно адекватното ниво на защита съгласно ОРЗД.
[48] Вж. член 182, параграф 2 от ЗЗД от 2018 г. Вж. също Меморандума за разбирателство относно ролята на СКИ във връзка с новите оценки на Обединеното кралство относно адекватното ниво на защита,

защита, държавният секретар на Обединеното кралство трябва да вземе предвид същите елементи, които Европейската комисия е длъжна да оцени съгласно член 45, параграф 2, букви а)—в) от ОРЗД, тълкувани във връзка със съображение 104 от ОРЗД, и запазената съдебна практика на ЕС. Това означава, че когато се оценява адекватното ниво на защита на трета държава, съответният стандарт трябва да бъде дали въпросната трета държава осигурява ниво на защита „по същество равностойно“ на това, което е гарантирано в рамките на Обединеното кралство. Въпреки че ЕКЗД отбелязва качеството на Обединеното кралство да признава, съгласно неговото ОРЗД, че дадени територии предоставят адекватно ниво на защита на личните данни, той желае да подчертае, че към днешна дата тези територии може да не се ползват от решение относно адекватното ниво на защита, издадено от Европейската комисия, признаващо ниво на защита, което е „по същество равностойно“ на това, гарантирано в ЕС. Това би могло да доведе до потенциални рискове за осигуряваната защита на предаваните от ЕИП лични данни, особено ако в бъдеще уредбата на Обединеното кралство за защита на данните се отклони от достиженията на правото на ЕС. Следва да се отбележи, че през юли 2020 г. в резултат на ключовото дело *Schrems II* пред Съда на ЕС[49] решението относно Щита за личните данни беше обявено за невалидно, тъй като според Съда на ЕС не може да се смята, че правната уредба на САЩ осигурява по същество равностойно ниво на защита в сравнение с нивото на ЕС. Въпреки това вече приетите решения на Съда на ЕС, които се смятат за запазена съдебна практика в правната уредба на Обединеното кралство, може повече да не го обвързват, тъй като Обединеното кралство има възможност да изменя запазеното право на ЕС след края на междинния период и неговият Върховен съд не е задължен да се води от запазената съдебна практика на ЕС[50].

81. **ЕКЗД приканва Европейската комисия да наблюдава внимателно процеса на оценка на адекватното ниво на защита и критериите на органите на Обединеното кралство по отношение на други трети държави, по-специално на тези, за които ЕС не е признал, че осигуряват адекватно ниво на защита съгласно ОРЗД. Когато Европейската комисия установи, че третата държава, смятана от Обединеното кралство за притежаваща адекватно ниво на защита, не осигурява ниво на защита, по същество равностойно на това, гарантирано в рамките на ЕС, ЕКЗД приканва Комисията да предприеме всички необходими стъпки, като например изменение на решението относно адекватното ниво на защита на Обединеното кралство, за да въведе конкретни гаранции за личните данни, предавани от ЕИП, и/или да спре прилагането на решението относно адекватното ниво на защита на Обединеното кралство, когато лични данни, предавани от ЕИП във Великобритания, подлежат на последващо предаване към въпросната трета държава, позовавайки се на признато адекватно ниво на защита.**

82. **Второто предизвикателство** е свързано с предстоящия преглед на вече съществуващите решения относно адекватното ниво на защита, издадени от Европейската комисия съгласно Директива 95/46/ЕО. След този преглед Европейската комисия може да реши, че определени държави, които до момента са прилагали съответното решение относно адекватното ниво на защита, вече не предоставят ниво на защита, което е „по същество равностойно“ на актуалното законодателство на ЕС и на последната съдебна практика. Както е предвидено в параграф 4, приложение 21 към ЗЗД от 2018 г. обаче, Обединеното кралство вече е признало, че тези

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.

[49] Вж. делото *Schrems II*.

[50] Вж. член 6, параграфи 3—6 от Закона от 2018 г. за оттеглянето от Европейския съюз.

държави осигуряват адекватно ниво на защита. Въпреки че държавният секретар на Обединеното кралство трябва да извърши преглед на тези заключения относно адекватното ниво на защита в срок от четири години, Европейската комисия отбелязва в своето проекторешение, че тези констатации относно адекватното ниво на защита няма да престанат да съществуват автоматично, ако държавният секретар на Обединеното кралство не извърши предвидената проверка в рамките на определения срок от четири години[51].

83. **ЕКЗД приканва Европейската комисия да наблюдава дали след приключването на прегледа на вече съществуващи решения относно адекватното ниво на защита, държава, за която се смята, че вече не осигурява адекватно ниво на защита, все още се счита за такава от Обединеното кралство. Ако това е така, ЕКЗД приканва Европейската комисия въз основа на съображения 277—280 от проекта на решение да предприеме подходящи мерки за коригиране на положението, например чрез изменение на решението относно адекватното ниво на защита, за да въведе конкретни изисквания за личните данни, предавани от ЕИП, и/или да спре прилагането на решението относно адекватното ниво на защита, когато лични данни, предавани от ЕИП в Обединеното кралство, подлежат на последващо предаване към въпросната трета държава. ЕКЗД приканва Европейската комисия да продължи наблюдението относно срока на действие на решението относно адекватното ниво на защита в Обединеното кралство.**

84. **Третото предизвикателство** е свързано с последващото предаване на лични данни от ЕИП към държави, които не предоставят адекватно ниво на защита въз основа на инструментите за предаване, предвидени в членове 46 и 47 от ОРЗД на Обединеното кралство. Въпреки че ОРЗД на Обединеното кралство предвижда същите инструменти за предаване като предвидените от ОРЗД, ЕКЗД подчертава необходимостта да се гарантира, че съдържащите се в тях мерки осигуряват ефективна защита в третата държава, особено като се има предвид съдебното решение по делото *Schrems II*.

85. След съдебното решение по делото *Schrems II*, в което Съдът на ЕС напомня, че осигурената защита на личните данни в ЕС трябва да се движи заедно с данните, където и да отидат те, ЕКЗД вече е приел първоначални препоръки относно допълващите мерки[52], за да подпомогне износителите, когато е необходимо, да гарантират, че субектите на данни се ползват с ниво на защита, което по същество е равностойно на гарантираното в ЕС.

86. Според Съда на ЕС износителите на данни имат отговорност да проверяват за всеки отделен случай и когато е целесъобразно — в сътрудничество с вносителя на данни в третата държава, дали законът или практиката на третата страна засягат ефективността на подходящите гаранции, съдържащи се в инструментите за предаване съгласно член 46 от ОРЗД[53]. Когато това е така, износителите на данни следва да прилагат допълващи мерки, които да запълват тези пропуски в защитата, и да я издигат до нивото, което се изисква от правото на ЕС.

87. **ЕКЗД приканва Европейската комисия, с цел да се гарантира непрекъснатост на защитата, да въведе в проекторешението уверения, че когато инструментите за предаване, предвидени в**

[51] Вж. съображение 82 от проекторешението.

[52] Вж. Препоръки 01/2020 на ЕКЗД относно мерките, които допълват инструментите за предаване, за да се гарантира спазването на защита на личните данни на равнище ЕС, приети на 10 ноември 2020 г., които към момента са в процес на приключване след обществена консултация, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_bg.pdf.

[53] Вж. делото *Schrems II*, т. 134.

членове 46 и 47 от ОРЗД, се използват от износители на данни в Обединеното кралство за последващо предаване към други трети държави на прехвърлени от ЕИП данни, тези износители на данни преценяват във всеки отделен случай уредбата за защита на данните на третата държава; и ако е необходимо, предприемат подходящи мерки с цел да се гарантира ефективното спазване на мерките, съдържащи се в избрания инструмент за предаване, за да осигурят по същество равностойно ниво на защита като гарантираното в ЕС. Без тези уверения ЕКЗД подчертава, че има риск по същество равностойното ниво на защита като гарантираното в ЕС да бъде намалено чрез последващо предаване, което се извършва от Обединеното кралство.

88. **Четвъртото предизвикателство**, свързано с последващо предаване, се отнася за международни споразумения, които са сключени или които предстои да бъдат сключени в бъдеще от Обединеното кралство, и възможния пряк достъп до лични данни от ЕИП на органите от трета(и) държава(и), страна(и) по такива споразумения. В действителност ЕКЗД има силни опасения във връзка с вече сключеното Споразумение между Обединеното кралство и САЩ по Закона CLOUD и Европейската комисия потвърждава това предизвикателство, като подчертава, че *„евентуалното влизане в сила на споразумението може да окаже въздействие върху нивото на защита, оценено в настоящото решение“*[54]. В действителност въз основа на това споразумение, след като то влезе в сила, предадените от ЕИП лични данни в Обединеното кралство съгласно проекторешението след това ще бъдат предмет на разпоредбите на това споразумение, в които се предвиждат условия за пряк достъп на органите на САЩ, засягайки уредбата на Обединеното кралство за защита на данните, включително разпоредбите за последващо предаване. В резултат на това, нивото на защита, което се осигурява на предаваните от ЕИП данни, може да бъде засегнато съществено от разпоредбите на сключеното със САЩ споразумение. ЕКЗД отбелязва, че Европейската комисия се позовава на обяснения, дадени от органите на Обединеното кралство в съображение 153 от своето решение, без да цитира или да предостави конкретно писмено уверение или ангажимент и без да посочи конкретни правни разпоредби в правото на Обединеното кралство, които биха дали възможност за прилагането на тези обяснения.

89. ЕКЗД беше изразил тези свои опасения в писмо, адресирано до Европейския парламент от 15 юни 2020 г[55]. ЕКЗД беше подчертал, че въз основа на *„достиженията на правото на ЕС в областта на защитата на данни, и по-специално ОРЗД и директивата за правоприлагането“* има резерви дали гаранциите в споразумението за достъп до лични данни в Обединеното кралство ще се прилагат при определени обстоятелства, които предвиждат задължения за разкриването им на САЩ, както и дали тези мерки са достатъчни предвид заложените стандарти на ЕС, така че да не подкопаят нивото на защита.

90. Освен това, разпоредбите на Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD може да засегнат съществено материалноправните и процесуалните условия, въз основа на които лични данни, държани от администратори или обработващи данни в Обединеното кралство, могат да бъдат пряко достъпвани от органи на САЩ, което ще повлияе върху нивото на защита, гарантирано от правото на Обединеното кралство. За да се осигури ниво на защита, което по същество е равностойно на гарантираното от правото на ЕС,

[54] Вж. съображение 153 от проекторешението.

[55] Вж. отговор на ЕКЗД на членовете на парламента Sophie in't Veld и Moritz Körner относно Споразумението между Обединеното кралство и САЩ във връзка със Закона Cloud, приет на 15 юни 2020 г.https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

например *„е от съществено значение гаранциите по такова споразумение да включват задължително предварително съдебно разрешение като основна мярка за достъпа до метаданни и данни за съдържанието. Въз основа на своята предварителна оценка ЕКЗД, като отбелязва, че споразумението се отнася за прилагането на националното законодателство, не можа да установи ясно разписана разпоредба в споразумението, сключено между Обединеното кралство и САЩ“*[56].

91. Европейската комисия подчертава, че получените данни по това споразумение ще се ползват от защита, равностойна на специфичните гаранции, предоставени по така нареченото „Рамково споразумение между ЕС и САЩ“, но ЕКЗД има опасения за това дали въвеждането на тези гаранции в Споразумението между Обединеното кралство и САЩ съгласно Закона CLOUD единствено чрез позоваване и прилагане на принципа *по подразбиране* би изпълнило критериите за ясни, прецизни и достъпни правила във връзка с достъпа до лични данни или дали в него ще бъдат заложени достатъчно гаранции, които да подлежат на изпълнение, и да дават основание за съдебно преследване съгласно законодателството на Обединеното кралство.

92. **Поради това ЕКЗД препоръчва на Европейската комисия да поясни как и въз основа на кой правен инструмент еквивалентните защити на специалните мерки, предоставени от Рамковото споразумение между ЕС и САЩ ще бъдат приведени в действие и ще имат обвързващ характер съгласно правото на Обединеното кралство.**

93. ЕКЗД отбелязва, че разпоредбите на Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD съгласно член 3 от Закона CLOUD на САЩ[57] повдигат въпроси относно действителното прилагане на предлаганите гаранциите по споразумението за достъп от правоприлагащите органи на САЩ до лични данни в Обединеното кралство, обработвани от доставчици на електронни комуникационни услуги или от доставчици на дистанционни компютърни услуги (наричани по-нататък „ДКУ“), попадащи под юрисдикцията на САЩ. В действителност, ако ДКУ, който се намира в Обединеното кралство, е обект на правото на САЩ (например поради това, че е дъщерно дружество на дружество от САЩ), остава да се удостовери дали органите на САЩ ще трябва да се позоват на Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD, за да получат такива данни. Тъй като Европейската комисия посочва, че *„[о]собено внимание ще се обърне на прилагането и адаптирането на защитите, предвидени в Рамковото споразумение, към конкретния вид предаване на данни, обхванато от Споразумението между Обединеното кралство и САЩ“,* ЕКЗД подчертава, че въз основа на направената предварителна оценка не е ясно дали гаранциите, заложени в Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD, и следователно мерките по Рамковото споразумение между ЕС и САЩ, ще се прилагат за всички искания за достъп до данни в Обединеното кралство, ако има такива, направени от органите на САЩ във връзка със Закона CLOUD на САЩ.

94. В бъдеще, Обединеното кралство може да сключи други международни споразумения или ангажименти с трети държави, а това се отнася и за предаваните от ЕИП към Обединеното кралство лични данни съгласно проекторешението[58]. В зависимост от разпоредбите на тези международни споразумения и прилагането на специфични клаузи за гаранции в тях, те могат да засегнат съществено също така материалноправните и процесуалните условия за достъп до

[56] Вж. гореспоменатото писмо на ЕКЗД.
[57] Вж. Закона CLOUD на САЩ, https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.
[58] Вж. раздел 2.3.3 по-горе.

лични данни в Обединеното кралство от органи на трети държави. Такъв по-конкретно е случаят с проекта на втори допълнителен протокол към Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство (наричана по-нататък „Конвенцията от Будапеща“), който се договаря понастоящем между страните по тази конвенция, които включват няколко държави извън ЕС. В действителност, проектът на протокол включва клаузи, които могат да бъдат активирани по преценка на страните, например относно разрешаването на достъп до данни за съдържанието. Всички държави членки ще активират клаузите в съответствие с правилата за защита на данните, но по отношение на Обединеното кралство не са предоставени гаранции, а то може да се отклони съществено от нивото на защита, което ще бъде предоставено в рамките на ЕС. Друг пример за представените по-горе въпроси е Споразумението между Обединеното кралство и Япония за всеобхватно икономическо партньорство[59] („CEPA“), първата търговска сделка на Обединеното кралство след Брекзит, която влезе в сила на 1 януари 2021 [60] и която включва разпоредби относно личните данни[61]. В допълнение ЕКЗД отбелязва, че Обединеното кралство обяви официално на 1 февруари 2021 г. своето искане за присъединяване към Всеобхватното и прогресивно споразумение за транстихоокеанско партньорство („CPTPP“), което включва Споразумението за транстихоокеанско партньорство „TPP“)[62].

95. ЕКЗД отбелязва, че освен Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD споменатите по-горе международни споразумения не са разгледани в проекторешението.

96. **ЕКЗД приканва Европейската комисия:**

- **да разгледа взаимодействието между уредбата на Обединеното кралство за защита на данните и неговите международни ангажименти, извън Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD, по-специално, да гарантира непрекъснатост на нивото на защита, когато личните данни, предадени от ЕИП на Обединеното кралство, се предават на други трети държави въз основа на решение на Обединеното кралство относно адекватното ниво на защита; както и да извършва постоянно наблюдение и при необходимост да предприема действия по отношение на сключването на други международни споразумения между Обединеното кралство и трети държави, което излага на риск нивото на защита на личните данни, предоставено в ЕС;**

- **да предостави на ЕКЗД писмени ангажименти от органите на Обединеното кралство и да посочи конкретни разпоредби съгласно правото на Обединеното кралство във връзка**

[59] Вж. Обединено кралство/Япония: Споразумение за всеобхватно икономическо партньорство [CS Japan No.1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Вж. Насоки на правителството на Обединеното кралство относно търговските споразумения с държави извън ЕС, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Съгласно член 8.80, параграф 5 от CEPA страните се ангажират да стимулират разработването на механизми за насърчаване на съвместимостта между своите различни правни подходи за защита на (личните) данни. Съгласно член 8.84 страните се ангажират да не забраняват или да не ограничават трансграничното предаване на информация чрез електронни средства, включително лична информация, когато тази дейност е с цел извършване на бизнес от обезпечено лице по смисъла на CEPA.

[62] Съгласно член 14.11, параграф 2 от TPP всяка страна позволява трансграничното предаване на информация чрез електронни средства, включително лична информация, когато тази дейност е с цел извършване на бизнес от обезпечено лице.

с разяснението относно евентуалното прилагане и изпълнение на Споразумението между Обединеното кралство и САЩ съгласно Закона CLOUD, както е посочено в съображение 153 от проекторешението.

- **Да наблюдава в този контекст дали Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD освен гаранциите, които могат да бъдат предоставени чрез подходящо изпълнение на адаптирането на Рамково споразумение между ЕС и САЩ, предоставя и подходящи допълнителни гаранции, отчитайки нивото на чувствителност на категориите засегнати данни и специфичните изисквания за пряко прехвърляне на електронни доказателства от ДКУ, а не между органи.**

- **Да оцени въздействието и потенциалните рискове на разпоредбите за личните данни, съдържащи се в международни споразумения, сключени неотдавна от Обединеното кралство, като CEPA.**

97. **Петото установено предизвикателство** е свързано с прилагането на дерогации за предаванията на лични данни на трета държава. Въпреки че съществуващите дерогации съгласно ОРЗД на Обединеното кралство са същите като предвидените в ОРЗД, важно е СКИ да прилага и да продължи да прилага тълкуване при използването на тези дерогации, което е съгласувано с това на ЕКЗД. Ако случаят не е такъв или ако Обединеното кралство се отклони от това тълкуване в бъдеще, ще възникне риск от накърняване на нивото на защита на данните, предавани от ЕИП към трети държави през Обединеното кралство.

98. **ЕКЗД приканва Европейската комисия, като част от своята задача за наблюдение, специално да провери, дали тълкуването на Обединеното кралство относно използването на дерогации остава съгласувано с това на ЕС. Ако обаче Обединеното кралство е следвало различно тълкуване относно използването на дерогации, което излага на риск нивото на защита, от съществено значение е Европейската комисия да предприеме необходимите стъпки чрез изменение на решението относно адекватното ниво на защита на личните данните, за да гарантира, че нивото на защита на личните данните, които се предават от ЕИП към Обединеното кралство, няма да бъде изложено на риск, когато тези данни бъдат предадени след това от Обединеното кралство на трети държави.**

99. **Шестото предизвикателство,** което е последното в този раздел, е свързано с липсата на защитите, предвидени в член 48 от ОРЗД, в уредбата на Обединеното кралство за защита на данните.

100. В действителност Европейската комисия разяснява в своя проект на решение, че при липсата на разпоредби относно адекватното ниво на защита или на подходящи гаранции предаването може да се извърши само въз основа на дерогации, посочени в член 49 от ОРЗД на Обединеното кралство, *„с изключение на член 48 от Регламент (ЕС) 2016/679, който Обединеното кралство е избрало да не включва в ОРЗД на Обединеното кралство.“*[63] Липсата на разпоредба, равностойна по същество на член 48 от ОРЗД, в уредбата на Обединеното кралство за защита на данните във връзка с предавания и оповестявания, след решение на съд или трибунал, или решение на административен орган от друга трета държава, може да породи правна несигурност дали е засегнато съществено нивото на защита на личните данни, предавани от ЕИП към Обединеното кралство.

[63] Вж. бележка под линия 78 в проекторешението.

101. В своя Референтен документ относно адекватното ниво на защита съгласно ОРЗД ЕКЗД посочва, че когато става въпрос за последващо предаване, „*последващо предаване на личните данни от първоначалния получател на първоначалното предаване на данни следва да бъде разрешено само когато следващият получател също е обвързан с правила, осигуряващи подходящо ниво на защита, и при спазване на съответните указания, когато данните се обработват от името на администратора*“[64]. Освен това ЕКЗД подчертава, че „*първоначалният получател на данните, които се предават от ЕС, следва да носи отговорност за осигуряването на подходящи гаранции за последващото предаване на данните, ако не е издадено решение относно адекватното ниво на защита. Такова последващо предаване на данни следва да се извършва само за ограничени и определени цели и доколкото са налице правни основания за такова обработване*“[65]. Като част от глава V от ОРЗД, член 48 трябва да бъде взет предвид напълно при извършването на оценка за това дали правната уредба на Обединеното кралство гарантира по същество равностойно ниво на защита[66].

102. ЕКЗД подчертава практиката на Съда на ЕС във връзка с риска от злоупотреба или неправомерен достъп и използване на данни, като твърди по-конкретно, че „*що се отнася до гарантираната в рамките на Съюза степен на защита на основните права и свободи, съгласно постоянната практика на Съда съответната правна уредба на Съюза, в която се предвижда намеса в гарантираните с членове 7 и 8 от Хартата основни права, трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито лични данни са били засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на техните лични данни срещу рискове от злоупотреби, както и срещу всякакъв незаконен достъп или използване на тези данни. Необходимостта от такива гаранции е още по-голяма, когато личните данни са подложени на автоматизирано обработване и когато има значителен риск от неправомерен достъп до такива данни.*“[67].

103. ЕКЗД отбелязва, че въз основа на наличната информация в проекта на решение в уредбата на Обединеното кралство за защита на данните не се предвижда ясно, че всяко решение на съд или трибунал и на административен орган на трета държава, с което от администратор или обработващ се изисква да предаде или разкрие лични данни, могат да бъдат признати или да подлежат на изпълнение по какъвто и да било начин само, ако се основават на международно споразумение, което е в сила между третата държава, отправила искането, и Обединеното кралство. Член 48 от ОРЗД е разпоредба относно равностойното по същество ниво на защита в съответствие с глава V от ОРЗД, тъй като изисква при предаване или оповестяване на лични данни след съдебно решение или решение на съд от трета държава/трибунал, или административен орган, последното да може да бъде признато или да подлежи на изпълнение само, ако се основава на международно споразумение, което е в сила между третата държава, отправила искането, и Съюза или държава членка, без да се нарушават други основания за прехвърлянето по глава V от ОРЗД. В действителност ЕКЗД припомня, че „*искане от чуждестранен орган само по себе си не представлява правно основание за предаване на*

[64] Вж. РД 254 ред.01, стр. 6.
[65] Вж. РД 254 ред.01, стр. 6.
[66] Вж. член 44 от ОРЗД, последно изречение, по-специално: „*Всички разпоредби на настоящата глава се прилагат, за да се направи необходимото нивото на защита на физическите лица, осигурено от настоящия регламент, да не се излага на риск.*“
[67] Вж. делото *Schrems I*, т. 91.

данни. Заповедта може да бъде призната само ако се основава на международно споразумение, като договор за взаимна правна помощ, който е в сила между третата държава, отправила искането, и Съюза или държава членка"[68]. Следователно от съществено значение е в правото на Обединеното кралство да могат да бъдат установени разпоредби относно равностойно по същество ниво на защита на личните данни.

104. В своето проекторешение Европейската комисия посочва разяснения от органите на Обединеното кралство, според които съгласно общото право и законите чуждестранно съдебно решение, с което се искат данни, не подлежи на изпълнение в Обединеното кралство без международно споразумение и за всяко предаване на данни по искане на чуждестранен съд или административен орган се изисква инструмент за предаване, като разпоредба, осигуряваща адекватното ниво на защита или подходящи гаранции, освен ако не се прилага една от дерогациите в член 49 от ОРЗД на Обединеното кралство. На ЕКЗД обаче не е предоставена кореспонденцията между Европейската комисия и органите на Обединеното кралство[69], поради което ЕКЗД не е в състояние да анализира и да оцени самостоятелно дали предоставените от органите на Обединеното кралство гаранции са достатъчни, за да се гарантира по същество равностойно ниво на защита по отношение на мерките, съдържащи се в член 48 от ОРЗД.

105. **ЕКЗД приканва Европейската комисия да представи допълнителни уверения и конкретни позовавания на законодателството на Обединеното кралство, с които се гарантира, че нивото на защита съгласно правната уредба на Обединеното кралство е по същество равностойно на нивото на защита, гарантирано в ЕИП. Комитетът подканва Европейската комисия да представи писмени разяснения и ангажименти от органите на Обединеното кралство във връзка с прилагането на защити, които са по същество равностойни на тези, предвидени в член 48 от ОРЗД.**

106. **ЕКЗД смята, че установяването на разпоредби в правото на Обединеното кралство, които да гарантират по същество равностойно ниво на защита във връзка с мерките, съдържащи се в член 48 от ОРЗД, е още по-важно в светлината на вече изразените опасения относно исканията за достъп до данни в Обединеното кралство, направени от органите на САЩ или на други трети държави, и като се има предвид, че съгласно решението относно адекватното ниво на защита, личните данни биха могли да бъдат предавани от ЕИП към Обединеното кралство без допълнителна гаранция или обвързващ ангажимент от страна на получателя при отправянето на искания за достъп до данни от органите на други трети държави.**

3.2. Процедурни механизми и механизми за правоприлагане:

107. Въз основа на критериите, определени в Референтния документ относно адекватното ниво на защита съгласно ОРЗД, ЕКЗД е анализирал следните аспекти на уредбата на Обединеното кралство за защита на данните, обхванати в проекторешението: съществуването и ефективното функциониране на независим надзорен орган; съществуването на система, която да гарантира добро ниво на съответствие; както и система за достъп до подходящи механизми за правна защита, осигуряващи средства на гражданите в ЕИП да упражняват правата си и да търсят

[68] Вж. приложението към Съвместния отговор на ЕКЗД-ЕНОЗД на Комисията по граждански свободи, правосъдие и вътрешни работи на Европейския парламент относно въздействието на Закона Cloud на САЩ върху европейската правна уредба за защита на личните данни, приет на 10 юли 2019 г., https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_bg.

[69] Вж. бележка под линия 78 в проекторешението.

правна защита, без да се сблъскват с обременителни бариери пред административната и съдебната защита.

3.2.1 Компетентен независим надзорен орган

108. ЕКЗД приветства усилията на Европейската комисия да разгледа всеобхватно създаването, функционирането и правомощията на надзорния орган на Обединеното кралство от глава 2.6 от проекта на решение. В Обединеното кралство комисарят по информацията („наричан по-нататък „КИ“) е натоварен със задачата да упражнява надзор и да следи за спазването на ОРЗД на Обединеното кралство и на ЗЗД от 2018 г. Съгласно приложение 12 от ЗЗД от 2018 г. КИ е „Corporation Sole“, т.е. отделен правен субект, учреден като едноличен орган, подпомаган от служба — СКИ.

109. Във връзка с независимостта на КИ, ЕКЗД подчертава, че член 51 от ОРЗД на Обединеното кралство не съдържа изрично пояснение, че КИ е независим държавен орган, както е посочено в член 51 от ОРЗД по отношение на надзорния орган за защита на данните (НОЗД). Независимо от това ЕКЗД потвърждава, че ОРЗД на Обединеното кралство отразява в своя член 52 по подобен начин съответстващите правила във връзка с независимостта, определени в член 52, параграфи 1—3 от ОРЗД.

110. Освен това, ЕКЗД изтъква, че в член 52 от ОРЗД на Обединеното кралство не са предвидени задължения, съответстващи на член 52, параграфи 4—6 от ОРЗД, с което изрично да се гарантира, че на съответния НО са предоставени необходимите ресурси за ефективно изпълнение на неговите задачи и за упражняване на неговите правомощия. ЕКЗД обаче признава, че ЗЗД от 2018 г. съдържа разпоредби, предназначени да осигурят подходящо финансиране на СКИ[70], както и обстоятелството, че Службата понастоящем е един от най-големите НОЗД в сравнение с другите органи в рамките на ЕС/ЕИП. Тъй като текущото разпределение на подходящи ресурси, особено по отношение на персонала и бюджета[71], е задължително, за да се гарантира надлежното функциониране на НОЗД по изпълнение на възложените му задачи и наскоро от Европейския парламент беше обърнато внимание, че това е от основно значение[72], ЕКЗД смята, че е изключително важно да се обърне специално внимание на бъдещите промени в тази област.

111. **Поради това ЕКЗД приканва Европейската комисия да наблюдава промените във връзка с разпределението на ресурси към СКИ, които биха имали пагубно въздействие върху надлежното изпълнение на задачите.**

3.2.2. Съществуване на система, която да гарантира добро ниво на съответствие

112. В проекта на решение се разглеждат всеобхватно правомощията, предоставени на СКИ по член 58 от ОРЗД на Обединеното кралство и по ЗЗД от 2018 г., за да се гарантира наблюдението и прилагането на законодателството. ЕКЗД потвърждава, че ОРЗД на Обединеното кралство отразява в своя член 58 по подобен начин съответстващите правила във връзка с правомощията на НОЗД, както са заложени в член 58 от ОРЗД. Относно правомощието за налагане на административни глоби в зависимост от обстоятелствата на всеки отделен случай в член 83 от ОРЗД на Обединеното кралство се съдържат подобни разпоредби и са предвидени

[70] Вж. членове 137, 138, 182 и точка 9 от приложение 12 към ЗЗД от 2018 г.

[71] Вж. РД 254 ред.01, стр. 7.

[72] Резолюция на Европейския парламент от 25 март 2021 г. относно Доклада на Комисията за оценка на изпълнението на Общия регламент относно защитата на данните две години след неговото прилагане, параграф 15,https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_BG.html.

максимални суми като определените в член 83 от ОРЗД. Затова ЕКЗД смята, че правната уредба на Обединеното кралство в тази област понастоящем е в съответствие със стандартите, определени в съответното законодателство на ЕС. В същото време ЕКЗД подчертава, че съществуването на *ефективни* санкции играе важна роля, за да се осигури спазването на правилата[73].

113. **Предвид гореспоменатото, ЕКЗД приканва Европейската комисия да наблюдава ефективността на санкциите и съответните средства за правна защита в уредбата на Обединеното кралство за защита на данните.**

3.2.3. Системата за защита на данните трябва да осигурява подпомагане и помощ за отделните субекти на данни при упражняването на техните права, както и подходящи механизми за съдебна защита

114. Ефективният надзорен механизъм, който позволява независимо разследване на жалби, за да се установят и санкционират нарушения на правата на субектите на данни в практиката, както и ефективните средства за административна и съдебна защита (включително обезщетение за понесени вреди от субекта на данни в резултат от неправомерно обработване на личните му данни) са основни елементи на оценката за това, дали системата за защита на данните осигурява адекватно ниво на защита.

115. ЕКЗД приветства факта, че СКИ предоставя всеобхватна информация и насоки на своя уебсайт с цел повишаване на осведомеността на администраторите и обработващите данни във връзка с техните задължения и отговорности, както и с цел подпомагане на субектите на данни да се информират за своите права по отношение на личните данни и да търсят своите индивидуални права съгласно ОРЗД на Обединеното кралство и ЗЗД от 2018 г.

116. **Независимо от настоящото положение, ЕКЗД приканва Европейската комисия постоянно да наблюдава нивото на подкрепа, предоставяна от СКИ специално на гражданите, чиито лични данни са предадени от Обединеното кралство съгласно решението относно адекватното ниво на защита, за да им помогне да упражнят правата си по режима за защита на данните в Обединеното кралство.**

4. ДОСТЪП И ИЗПОЛЗВАНЕ НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ ОТ ЕС, ОТ ПУБЛИЧНИ ОРГАНИ В ОБЕДИНЕНОТО КРАЛСТВО

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

4.1.1. Правни основания и приложими ограничения/гаранции

117. По отношение на оценката, извършена от Европейската комисия и документирана в съображения 132 и следващи от проекторешението, **относно достъпа за целите на правоприлагането**, Европейската комисия предоставя нюансирана и подробна информация и обикновено прави ясни заключения. Затова ЕКЗД се въздържа от възпроизвеждане на фактическата констатация и оценките в настоящото становище. Има обаче определени случаи,

[73] Вж. РД 254 ред.01, стр. 7.

в които описанието на фактите или разяснението на изводите не е достатъчно, за да може ЕКЗД да ги възприеме.

4.1.1.1. Използването на съгласие

118. ЕКЗД отбелязва, че в бележка под линия 184 от проекторешението[74] Европейската комисия твърди, че **използването на съгласие** не се смята за уместно в сценарий за адекватно ниво на защита, тъй като при ситуации на предаване на данни те не се събират от правоприлагащ орган на Обединеното кралство пряко от субекта на данни въз основа на съгласие. Следователно използването на съгласие като правно основание при полицейски действия не е преценено от Европейската комисия.

119. Във връзка с това ЕКЗД припомня, че в член 45, параграф 2, буква а) от ОРЗД се изисква оценката на широк спектър от елементи, които не се ограничават до ситуации, свързани с предаване, в т.ч. „*върховенството на закона, спазването на правата на човека и основните свободи, съответното законодателство — както общо, така и секторно, включително в областта на [...] наказателното право*“.

120. ЕКЗД отбелязва, въз основа и на информацията, предоставена от Европейската комисия в съображение 38 от нейния проект на решение за изпълнение съгласно Директива (ЕС) 2016/680 на Европейския парламент и на Съвета относно адекватната защита на лични данни от Обединеното кралство (наричано по-нататък „проекторешение относно адекватното ниво на защита съгласно ДП“), че използването на съгласие, както е формулирано в режима на Обединеното кралство, винаги ще изисква да се разчита на правно основание. Това означава, че дори ако полицейската служба разполага със законови правомощия да обработва данните с цел разследване, при определени конкретни обстоятелства (например събиране на ДНК проба) тя може да прецени за уместно да поиска съгласието на субекта на данни.

121. **ЕКЗД приканва Европейската комисия да включи в решението относно адекватното ниво на защита неговия анализ на възможното използване на съгласие в контекста на правоприлагането, предвидено в проекта на решение относно адекватното ниво на защита съгласно ДП**.

4.1.1.2. Заповеди за обиск и заповеди за предоставяне

122. Въпреки че ЕКЗД няма коментари по принцип относно извличането на доказателства от полицията чрез заповеди за обиск и заповеди за предоставяне, от съображение 136 от проекторешението следва, че Европейската комисия е съсредоточила своите съображения за достъп на правоприлагащите органи до полицията и че обработването на лични данни от други правоприлагащи агенции е по-малко изследвано.

123. Например в Обяснителната рамка на Обединеното кралство за обсъждане на адекватното ниво на защита, раздел F: Правоприлагане[75], на страница 11 се посочва, че **Националната агенция за противодействие на престъпността** (наричана по-нататък „НАПП“) може да бъде правоприлагаща агенция от особен интерес, която *между другото* има по-широки функции за извършване на криминално разузнаване. НАПП описва своята мисия като обединяване на

[74] Вж. точка 37 от проекторешението.

[75] Вж. Обяснителната рамка на правителството на Обединеното кралство за обсъждане във връзка с адекватното ниво на защита, раздел F: Правоприлагане, 13 март 2020 г., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

разузнавателни данни от редица източници за предоставяне на най-добрите възможности за анализ, оценка и тактически действия, включително от прихващане на комуникация с технически средства, от партньори в областта на правоприлагането в Обединеното кралство и в чужбина, агенции за сигурност и разузнаване[76]. Освен това НАПП е един от основните събеседници на международните партньори в областта на правоприлагането и играе ключова роля в обмена на разузнавателни данни за престъпността[77].

124. ЕКЗД освен това отбелязва факта, че Правителствената централа за комуникации (*Government Communications Headquarters*), наричана по-нататък „ПЦК“), чиято дейност обичайно попада в обхвата на част 4 от ЗЗД от 2018 г., т.е. националната сигурност, поема също така активна роля за намаляване на обществените и финансовите вреди, които тежката и организираната престъпност причинява на Обединеното кралство, като работи в тясно сътрудничество с министерството на вътрешните работи, НАПП, Кралската данъчна и митническа служба (HM Revenue and Customs или „КДМС“) и други държавни ведомства[78]. Неговите дейности са свързани с противодействие на сексуалното насилие над деца; измами; други видове икономическа престъпност, включително изпирането на пари; престъпно използване на технологии; киберпрестъпления; организирана имигрантска престъпност, включително трафик на хора; и наркотици, огнестрелни оръжия и други незаконни контрабандни дейности.

125. **ЕКЗД призовава Европейската комисия да допълни своя анализ с анализ на агенциите, осъществяващи дейност в областта на правоприлагането, за които, изглежда, събирането и анализът на данни, включително лични данни, са ядрото на всекидневните им операции, и по-специално НАПП. В допълнение ЕКЗД приканва Европейската комисия да разгледа по-внимателно агенциите като ПЦК, чиито дейности попадат в обхвата както на правоприлагането, така и на националната сигурност, както и приложимата за тях правна уредба относно обработването на лични данни.**

---

[76] Вж. уебсайта на Националната агенция по престъпността, Intelligence: enhancing the picture of serious organised crime affecting the UK (Разузнаването: осигуряване на по-ясна картина на тежката организирана престъпност, засягаща Обединеното кралство), https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[77] Въпреки че не всички разузнавателни данни, обработвани от НАПП, са лични данни, значителна част може да представлява лични данни и описаните тук дейности се различават от класическата полицейска работа, така че оценката на достъпа до лични данни от страна на правоприлагащите органи в Обединеното кралство би била непълна без задълбочено разглеждане на дейността на НАПП. Изглежда разумно да се гарантира, че на принципите на защита на данните се отдава еднакво значение във всички съответни правоприлагащи органи, и следователно да се хвърли светлина върху агенции като НАПП, чиято работа в особена степен зависи от данните. В допълнение, „с поглед към бъдещето“, разяснението продължава с *„[н]ие непрекъснато търсим нови възможности за набиране, изграждане и подобряване на традиционния капацитет с цел увеличаване на количеството и качеството на разузнавателните данни, които са на разположение за използване както в Обединеното кралство, така и в чужбина.“ „Като част от това ние разработваме новия Национален капацитет за експлоатация на данни, използвайки правомощията, вменени на агенцията от Закона за престъпността и съдилищата (Crime and Courts Act), за да свързваме заедно, да осъществяваме достъп и да използваме данните, съхранявани на различни места в държавната администрация*.“ [...] *„Всичко това ще повиши бързината и гъвкавостта на нашите ответни действия срещу новите заплахи и способността ни да работим проактивно, да събираме и анализираме информация и разузнавателни данни за нововъзникващи заплахи, за да можем да предприемаме действия, преди заплахите да бъдат осъществени*.“

[78] Вж. уебсайта на ПЦК, Mission, Serious and Organised Crime, (Мисия. Тежки престъпления и организирана престъпност) https://www.gchq.gov.uk/section/mission/serious-crime.

4.1.1.3. Правомощия за разследване за целите на правоприлагането

126. Съгласно глава 4 от Референтния документ относно адекватното ниво на защита съгласно ОРЗД „Основни гаранции в трети **държави с цел правоприлагане** и национална сигурност с оглед на ограничаването на намесите в основните права“ ЕКЗД напомня, че *„[в] този контекст съдът също така отбелязва критично, че предходното решение за „сферата на неприкосновеност на личния живот“ „не съдържа каквато и да било констатация относно наличието в Съединените щати на правила с етичен характер, предназначени за ограничаване на евентуалната намеса, засягаща основните права на лицата, чиито данни се прехвърлят от Европейския съюз към Съединените щати**, **която намеса държавните структури на тази страна имат право да извършват, ако преследват законосъобразни цели**, като например осигуряване на националната сигурност*.“[79]. В този Референтен документ ЕКЗД заявява, че **четирите европейски основни гаранции за достъпа до данни**[80] **трябва да бъдат спазвани — както за целите на** националната сигурност, така и **с цел правоприлагане — от всички трети държави, за да се смятат за адекватни,** по-специално **трябва да се обосновават необходимостта и пропорционалността във връзка с преследваните законосъобразни цели.**

127. В този раздел на проекторешението Европейската комисия заключава (съображение 139): *„тъй като целевите правомощия за разследване, предоставени съгласно ЗПР от 2016 г., са същите като тези, с които разполагат службите за национална сигурност, условията, ограниченията и гаранциите, приложими за такива правомощия, са разгледани подробно в раздела относно достъпа и използването на лични данни от публичните органи на Обединеното кралство за целите на националната сигурност*“. От практиката на Съда на ЕС обаче следва, че при прилагането на теста за необходимост и пропорционалност към законодателството на държавите членки, позволяващо задържане и достъп до лични данни от публични органи, законосъобразните цели, като национална сигурност или борба с тежката престъпност, се различават и затова по отношение на едната може да е възможно да се обоснове определен вид намеса, докато за другата това да не е възможно[81].

128. **Затова ЕКЗД би приветствал конкретна оценка в рамките на решението за необходимостта и пропорционалността на условията, ограниченията и гаранциите, описани в съображения 174 и следващи — раздел, посветен на мерките, с които се преследват цели на националната сигурност, — когато се стигне до прилагане на тези условия, ограничения и гаранции по отношение на предприетата мярка за целите на правоприлагането. Затова ЕКЗД приканва Европейската комисия да разясни допълнително дали описаното съхраняване на лични данни и достъпът до тях за целите на правоприлагането са ограничени в достатъчна степен, за да се гарантира ниво на защита, което е равностойно по същество на гарантираното в ЕС.**

[79] Вж. РД 254 ред.01, стр. 9.

[80] Вж. Препоръки 02/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение.

[81] Вж. решение на Съда на ЕС, съединени дела C-511/18, C-512/18 и C-520/18, *La Quadrature du Net и други*, 6 октомври 2020 г., ECLI:EU:C:2020:791.

4.1.2. По-нататъшно използване на събраната информация за целите на правоприлагането (съображения 140—154)

129. ЕКЗД отбелязва, че уредбата на Обединеното кралство за защита на данните предвижда подобни гаранции и ограничения като предвидените в правото на ЕС във връзка с по-нататъшното използване на събраната информация за целите на правоприлагането.

4.1.2.1. По-нататъшно използване за други цели на правоприлагането

130. В ЗЗД от 2018 г. се предвижда, че личните данни, събирани от компетентен орган с цел правоприлагане, могат да бъдат обработвани по-нататък (независимо дали от първоначалния администратор или от друг администратор) за всяка друга цел на правоприлагането, при условие че администраторът е оправомощен по закон да обработва данни за другата цел и че обработването е необходимо и пропорционално за тази друга цел. Европейската комисия отбелязва, че всички гаранции, предвидени в част 3 от ЗЗД от 2018 г., се прилагат за обработването, извършвано от получаващия орган. ЕКЗД подчертава обаче, че съгласно част 3 от ЗЗД от 2018 г. в член 44, параграф 4, член 45, параграф 4, член 48, параграф 3 и член 68, параграф 7 се предвижда възможност за ограничаване на правата на субекта на данни, а в член 79 се предвижда възможност за издаване на сертификати, с които се удостоверява, че ограничението е необходима и пропорционална мярка за защита на националната сигурност. **Затова ЕКЗД препоръчва на Европейската комисия да оцени допълнително възможното въздействие на тези ограничения върху нивото на защита на личните данни във връзка с по-нататъшното използване на събраната информация. По подобен начин следва да се предостави разяснение и във връзка с правната уредба на Обединеното кралство, позволяваща последващо споделяне, по-специално във връзка със Закона за цифровата икономика от 2017 г. (Digital Economy Act 2017), както и със Закона за престъпността и съдилищата от 2013 г. (Crime and Courts Act 2013), които позволяват споделянето на информация с НАПП.**

4.1.2.2. По-нататъшно използване за цели, различни от правоприлагането, в рамките на Обединеното кралство

131. В ЗЗД от 2018 г. се предвижда също така, че лични данни, събрани за целите на правоприлагането, могат да бъдат обработвани за цел, различна от правоприлагането, когато обработването е разрешено от закона. В този случай правното основание за подобно споделяне е член 19 от Закона за борба с тероризма (*Counter-Terrorism Act*) от 2008 г. Във връзка с това ЕКЗД отбелязва, че обхватът и разпоредбите на член 19 от Закона за борба с тероризма не са изцяло разгледани в оценката на Европейската комисия и може да предполагат по-нататъшно използване от по-широк характер, по-специално, по отношение на член 19, параграф 2, в който се предвижда, че *„[и]нформация, получена от някоя от разузнавателните служби във връзка с упражняването на някоя от нейните функции, може да бъде използвана от тази служба във връзка с упражняването на която и да е от нейните други функции“*.

132. ЕКЗД отбелязва също така, че позоваването от страна на Европейската комисия на факта, че компетентните органи са публични органи, които трябва да действат в съответствие с ЕКПЧ, включително с член 8 от нея, за да гарантират, че споделянето на всички данни между правоприлагащите органи и разузнавателните служби съответства на законодателството в областта на защитата на данните и на ЕКПЧ, може да бъде подкрепено допълнително чрез установяване на съответните актове и закони съгласно правния ред на Обединеното кралство, в които се определят ясно и точно такива ограничения.

4.1.2.3. По-нататъшно използване при последващо предаване извън Обединеното кралство

133. Докато Европейската комисия се е позовала на факта, че Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD може да повлияе на последващото предаване на данни към САЩ от ДКУ в Обединеното кралство, ЕКЗД подчертава също така, че влизането в сила на това споразумение може да повлияе и на последващото използване на информацията, събрана чрез последващо предаване от правоприлагащите органи в Обединеното кралство, особено във връзка с издаването и предаването на заповеди съгласно член 5 от Споразумението между Обединеното кралство и САЩ във връзка със Закона CLOUD.

134. Като цяло, ЕКЗД смята, че сключването на бъдещи двустранни споразумения с трети държави за целите на сътрудничеството в областта на правоприлагането, с които се осигурява правно основание за предаването на лични данни на тези държави, също може да повлияе значително на условията за последващо споделяне на събраната информация, тъй като тези споразумения може да засегнат вече оценената правна уредба на Обединеното кралство за защита на данните. Съответно ЕКЗД препоръчва на Европейската комисия да оцени допълнително този въпрос, като установи наличието на международни споразумения, и да разясни дали разпоредбите на тези споразумения могат да засегнат прилагането на правото на Обединеното кралство в областта на защитата на личните данни и да доведат до допълнителни ограничения или изключения във връзка с по-нататъшното използване и разкриване в чужбина на информация, събрана за целите на правоприлагането. ЕКЗД смята, че такава информация и оценка са от съществено значение, за да може да се направи пълен преглед на нивото на защита, осигурявано от законодателната уредба и практиките на Обединеното кралство във връзка с разкриването и по-нататъшното използване на данни в чужбина.

4.1.3. Надзор

135. ЕКЗД отбелязва, че надзорът над правоприлагащите органи в областта на наказателното право се осигурява, освен от СКИ и от комбинация от различни комисари. В заключенията, направени в проекта на решение относно адекватното ниво на защита са посочени КПР, комисарят по въпросите на съхранението и използването на биометричен материал, както и комисарят относно камерите за наблюдение. В този смисъл трябва да се отбележи, че Съдът на ЕС многократно е подчертавал необходимостта от независим надзор. КПР играе особено важна роля по отношение на въпросите за достъпа до лични данни, предавани в Обединеното кралство. Разбирането на ЕКЗД е, че КПР е т.нар. „съдебен комисар“, подобно на други съдебни комисари, до когото да се отнасят въпроси, както е заложено в главата за националната сигурност, и че тези съдебни комисари се ползват от независимостта на съдиите и когато изпълняват функция на комисари. Що се отнася до Службата на КПР, Европейската комисия обяснява в съображение 245 от проекта на решение, че тя функционира независимо в качеството си на т.нар. „пряк орган“, като същевременно се финансира от Министерството на вътрешните работи.

136. ЕКЗД не е открил допълнителни насоки в проекторешението за оценка на независимостта на комисаря по въпросите на съхранението и използването на биометричен материал, както и на комисаря относно камерите за наблюдение.

137. **Европейската комисия се приканва да извърши допълнителна оценка на независимостта на съдебните комисари също и за случаите, в които комисарят (вече) не изпълнява функцията на съдия, както и да извърши преценка на независимостта на комисаря по въпросите на съхранението и използването на биометричен материал и на комисаря относно камерите за наблюдение.**

4.2. Обща правна уредба на защитата на данните в областта на националната сигурност

4.2.1. Удостоверения за национална сигурност

138. Съгласно член 111 от ЗЗД от 2018 г. администраторите могат да кандидатстват за удостоверения за национална сигурност, издадени от министър, член на кабинета, главния прокурор или генералния адвокат за Шотландия, с които се удостоверява, че изключването от задълженията и правата, залегнали в части 4—6 от ЗЗД от 2018 г., е необходима и пропорционална мярка за защита на националната сигурност. Тези удостоверения са предназначени да дадат на администраторите по-голяма правна сигурност и ще бъдат убедително доказателство, че националната сигурност е приложима при обработването на лични данни. Следва да се отбележи обаче, че тези удостоверения не се изискват, за да се използват за позоваване на изключения относно националната сигурност, а вместо това са мярка за прозрачност[82].

139. ЕКЗД разбира от членове 17 и 18 на приложение 20 към ЗЗД от 2018 г., че срокът на действие на удостоверенията за национална сигурност, издадени съгласно Закона за защита на данните от 1998 г. (наричани по-нататък „старо удостоверение“) за целите на обработването на лични данни съгласно ЗЗД от 2018 г., е удължен до 25 май 2019 г. До тази дата, освен ако не бъдат заменени или отменени, старите удостоверения са третирани така, сякаш са издадени съгласно ЗЗД от 2018 г.

140. Въпреки това, когато няма изрично определена дата на изтичане на удостоверението за национална сигурност, издадено съгласно Закона за защита на данните от 1998 г., ЕКЗД разбира, че то ще продължи да има действие по отношение на обработването съгласно Закона за защита на данните от 1998 г., освен ако не бъде отнето или отменено[83]. Въпреки че защитата, осигурявана чрез тези стари удостоверения, се ограничава до обработването на лични данни съгласно Закона за защита на данните от 1998 г., ЕКЗД отбелязва факта, че е заложена възможността за издаване на нови удостоверения за национална сигурност за лични данни, които са били обработвани съгласно Закона за защита на данните от 1998 г.[84]

141. **За по-голяма изчерпателност ЕКЗД приканва Европейската комисия да поясни в своя проект на решение относно адекватното ниво на защита дали все още могат да бъдат издавани удостоверения за национална сигурност съгласно Закона за защита на данните от 1998 г. Освен това, ЕКЗД приканва Европейската комисия да опише в своето проекторешение механизмите за правна защита и за надзор по отношение на удостоверенията, издадени съгласно Закона за защита на данните от 1998 г. И накрая, ЕКЗД приканва Европейската**

[82] Вж. Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020 (Министерство на вътрешните работи на Обединеното кралство, Закон за защита на данните от 2018 г., Насоки за удостоверенията за национална сигурност), август 2020 г., параграф 4, стр. 3, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

[83] Вж. Home Office, The Data Protection Act 2018, National Security Certificates Guidance (Министерство на вътрешните работи на Обединеното кралство, Закон за защита на данните от 2018 г., Насоки за удостоверенията за национална сигурност), август 2020 г., стр. 5.

[84] Вж. Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020 (Министерство на вътрешните работи на Обединеното кралство, Закон за защита на данните от 2018 г., Насоки за удостоверенията за национална сигурност), август 2020 г., параграф 8, стр. 5.

комисия да включи броя на съществуващите удостоверения, издадени съгласно Закона за защита на данните от 1998 г., и да наблюдава внимателно този аспект.

4.2.2. Право на коригиране и изтриване

142. Във връзка с правото на коригиране и изтриване ЕКЗД отбелязва факта, че съгласно член 100 и член 149 от ЗЗД от 2018 г. субектите на данни имат възможност да се обърнат към Висшия съд (или както е в Шотландия- Върховен граждански съд) за издаване на разпореждане, с което администраторът се задължава да коригира или да заличи данните им без ненужно забавяне.

143. **ЕКЗД подчертава, че ефективното упражняването на правата на субектите на данни трябва да бъде гарантирано; затова приканва Европейската комисия да опише в своето проекторешение как се прилага на практика член 100 от ЗЗД от 2018 г. и да наблюдава внимателно използването на този член.**

4.2.3. Изключения, свързани с националната сигурност

144. ЕКЗД би искал да обърне внимание на член 110 от ЗЗД от 2018 г., и по-специално на приложение 11, в което се посочват конкретните цели, поради които разузнавателните служби могат да се отклонят от определени принципи на защита на данните, включително във връзка с права на субектите на данни, без да имат задължение да съобщават на СКИ за нарушения на сигурността на личните данни[85].

145. **ЕКЗД призовава Европейската комисия да разясни допълнително обхвата на изключенията, тъй като не е наясно дали всички изключения, предвидени в приложение 11 към ЗЗД от 2018 г., са от значение за работата на разузнавателните служби и дали осигуряват равностойно ниво на защита съгласно принципа на необходимостта и пропорционалността** . По-специално, **ЕКЗД приканва Европейската комисия да предостави повече пояснения при какви обстоятелства дадена разузнавателна служба би могла да се позове на член 10 от приложение 11 от ЗЗД от 2018 г., който гласи, че *„[п]осочените разпоредби не се прилагат за лични данни, които включват записи на намеренията на администратора във връзка с преговори със субекта на данни, доколкото прилагането на посочените разпоредби има вероятност да създаде риск за преговорите.“***

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

146. Като обща забележка ЕКЗД потвърждава, че на държавите е предоставена широка свобода на преценка по въпросите на националната сигурност, която се признава и от ЕСПЧ. ЕКЗД напомня също така, че както е подчертано в неговите актуализирани препоръки относно европейските основни гаранции при прилагане на мерки за наблюдение[86], член 6, параграф 3 от Договора за Европейския съюз установява, че основните права, залегнали в ЕКПЧ, представляват общи принципи на правото на ЕС. Съдът на ЕС обаче напомня в своята практика, че ЕКПЧ не

[85] Тези цели са предотвратяването и разкриването на „престъпление“, „информация, която трябва да бъде разкрита по закон и т.н. или във връзка със съдебни производства“, „парламентарна привилегия“, „съдебни производства“, „кралска чест и достойнство“, „въоръжени сили“, „икономическо благополучие“, „правна професионална привилегия“, „преговори“, „поверителни позовавания, направени от администратор“, „писмени изпитни работи и оценки“, „изследвания и статистика“ и „архивиране в обществен интерес“.

[86] Вж. Препоръки 02/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение.

представлява правен инструмент, включен официално в правото на ЕС, доколкото ЕС не се е присъединил към него[87]. Затова нивото на защита на основните права, което се изисква съгласно член 45 от ОРЗД, трябва да бъде определено въз основа на разпоредбите на този регламент, тълкуван от гледна точка на основните права, залегнали в Хартата на ЕС. В този смисъл, съгласно член 52, параграф 3 от Хартата на ЕС, съдържащите се в нея права, които съответстват на правата, гарантирани от ЕКПЧ, трябва да имат същото значение и обхват като предвидените в ЕКПЧ. Следователно, както се напомня от Съда на ЕС, трябва да бъде взета предвид практиката на ЕСПЧ относно правата, които са предвидени и в Хартата на ЕС, като минимален праг на защита при тълкуването на съответните права в Хартата на ЕС[88]. Съгласно последното изречение от член 52, параграф 3 от Хартата на ЕС обаче *„[m]ази разпоредба не пречи на правото на Съюза да предоставя по-широка защита*."

147. Следователно в становището си по-долу ЕКЗД е взел предвид практиката на ЕСПЧ, доколкото Хартата на ЕС според тълкуването на Съда на ЕС не предвижда по-високо ниво на защита, което предполага различни изисквания.

4.3.1. Правни основания, ограничения и гаранции — правомощия за разследване, упражнявани във връзка с националната сигурност

4.3.1.1. Общи бележки

148. ЕКЗД напомня, че ЗПР от 2016 г. е наскоро приет закон, с който се изменят няколко разпоредби в Закона за разузнавателните служби от 1994 г. Той определя степента, до която определени правомощия за разследване могат да бъдат използвани за намеса в правото на неприкосновеност на личния живот[89]. Въпреки двата доклада на КПР, които предоставят полезна информация относно прилагането на тази нова правна уредба, все още не е направена проверка на определени аспекти, по-специално относно използваните критерии за подбор и за търсене.

149. Като обща забележка относно ЗПР от 2016 г. и неговия обхват на приложение ЕКЗД насочва вниманието към следните четири основни точки:

150. Във връзка с **първата основна точка** относно характеристиките на закона, ЕКЗД би искал да подчертае два аспекта:

151. Първо, ЕКЗД отбелязва, че законодателството касае общи цели относно използването на процедурите, предвидени в ЗПР от 2016 г., а не категориите граждани, които може да са засегнати от събирането на данни въз основа на части 2 и 7 от закона. Във връзка с това ЕКЗД напомня, че би следвало да има връзка между категориите граждани, които могат да бъдат обект на мерки за наблюдение, и целите, преследвани от законодателството за определяне на персоналния обхват на закона.

152. Освен това ЕКЗД подчертава също така, че определенията за „оператор на далекосъобщителна мрежа", „далекосъобщителна услуга" и „далекосъобщителна система", които определят обхвата на закона, са също много широки и неясни до известна степен. Освен това ЕКЗД подчертава също така, че тези понятия в областта на ЗПР от 2016 г. следва да се разбират в много по-широк смисъл от законодателствата за далекосъобщенията, както например е

[87] Вж. делото *Schrems II*, т. 98.
[88] Вж. решение на Съда на ЕС, съединени дела C-511/18, C-512/18 и C-520/18, *La Quadrature du Net и други*, 6 октомври 2020 г., ECLI:EU:C:2020:791, т. 124.
[89] Вж. член 1 от ЗПР от 2016 г.

определено в Европейския кодекс за електронните съобщения[90]. ЕКЗД отбелязва, че определенията за „далекосъобщителна услуга“ и „далекосъобщителна система“ в Закона преднамерено са формулирани в по-широк смисъл, за да продължават да бъдат от значение и за новите технологии. По подобен начин определението за „оператор на далекосъобщителна мрежа“ също е много общо и би могло например да включва видеоигри с елемент на чат, или други онлайн уебсайтове, които включват единствено такива чатове[91].

153. В допълнение, въпреки че по принцип се предвиждат процедури и надзор относно оценката на необходимостта и пропорционалността на събирането и достъпа до данни, критериите за преминаване към такава оценка не са определени в самия закон. Допълнителни елементи може да се открият в други документи, като кодексите за добрите практики.

154. Както обаче се напомня в Препоръки 02/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение, Съдът на ЕС е посочил, че *„изискването всяко ограничение на упражняването на основни права да бъде предвидено в закон, означава, че самото правно основание, позволяващо намеса в тези права, трябва да определя обхвата на ограничението при упражняване на съответното право “*[92]. По-точно Съдът на ЕС пояснява, че *„[з]а да изпълни изискването за пропорционалност, правната уредба трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито данни са засегнати, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на тези лични данни срещу рискове от злоупотреби. Законодателството трябва в частност да бъде правно обвързващо съгласно националното право, и по-специално да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на такива данни, като по този начин гарантира ограничаване на намесата до строго необходимото*.“[93]

155. ЕСПЧ също подчертава важността на поясняването на правните норми, за да се предостави на гражданите *„адекватно посочване на обстоятелствата и условията, при които публичните органи са упълномощени да прибягват до такива мерки“*[94].

156. **Затова ЕКЗД приканва Европейската комисия допълнително да оцени точността, яснотата и изчерпателността на съответния закон и да представи допълнителни елементи, за да покаже, че той осигурява ниво на защита, което е по същество равностойно на гарантираното**

---

[90] Вж. член 2, параграф 5 от Европейския кодекс за електронните съобщения, в който „междуличностна съобщителна услуга“ се определя като *„услуга, предоставяна обикновено по възмезден начин, която дава възможност за пряк междуличностен и интерактивен обмен на информация по електронни съобщителни мрежи между определен брой лица, като лицата, започващи или участващи в комуникацията, определят адресата (адресатите) ѝ, и не включва услугите, които дават възможност за междуличностна и интерактивна комуникация само като незначителен допълнителен елемент, пряко свързан с друга услуга*“.

[91] Вж. Home Office, Code of practice on the interception of communications (Министерство на вътрешните работи на Обединеното кралство, Практически кодекс за прихващане на комуникация), март 2018 г., параграфи 2.5 и следващи, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf.

[92] Вж. делото *Schrems II*, т. 175; и цитираната съдебна практика, както и решение на Съда на ЕС, дело C-623/17, *Privacy International/Secretary of State for Foreign and Commonwealth Affairs и други*, 6 октомври 2020 г., ECLI:EU:C:2020:790 (наричано по-нататък „Privacy International“), т. 65.

[93] Вж. дело *Privacy International*, т. 68.

[94] Вж. решение на ЕСПЧ, *Zakharov/Russia*, 4 декември 2015 г., CE:ECHR:2015:1204JUD004714306, т. 229.

в рамките на ЕС във връзка с характеристиките на закона. ЕКЗД също подчертава, че трябва да бъдат преценени също така и широко формулираните определения от гледна точка на пропорционалността на мерките за прихващане.

157. В допълнение, въпреки че в няколко вътрешни кодекса на компетентните органи от разузнавателната общност тези елементи са частично разгледани, например относно оценката на необходимостта и пропорционалността на събирането на данни, ЕКЗД подчертава, че изискванията на Съда на ЕС във връзка с характера на закона означават, че основните елементи, включително възможността гражданите да могат да се позоват на тях като част от средствата за правна защита, трябва да бъдат предвидени в законодателството като например права за завеждане на иск[95]. В действителност в приложение 7, параграф 6 от ЗПР от 2016 г. се споменава фактът, че съдилищата (и надзорните органи) „*вземат предвид неспазването от страна на лице на кодекс при решаването на въпрос в такова производство*“, без да се пояснява дали лицата могат да претендират за нарушение на кодексите пред съдилищата (или надзорните органи). Освен това предвидените досега елементи в проекторешението са свързани или с признаването от ЕСПЧ на предвидимостта на правилата, залегнали[96] в тези кодекси, а не толкова с тяхната „искова сила“ пред съда, както се изисква от Съда на ЕС, или с факта, че съдилищата на Обединеното кралство по някои дела са се позовали на кодексите, но нито едно от посочените дела не илюстрира възможността гражданите да предявят права, произтичащи от кодексите. **Ако се стигне до заключението, че правото на Обединеното кралство не посочва в достатъчна степен обстоятелствата и условията, при които може да бъде приета мярка, и че тези елементи в действителност са разписани във вътрешните кодекси на органите на разузнавателната общност**, **ЕКЗД би призовал Европейската комисия да оцени допълнително дали ограниченията и гаранциите за защита на данните, предвидени в различните вътрешни кодекси на органите на разузнавателната общност, могат да бъдат предявени от гражданите пред съд и изпълнени.**

158. **Втората основна точка** засяга факта, че разпоредбите, свързани, от една страна, с целевото събиране и задържане на комуникационни данни, и от друга — със събирането на масиви от данни в ЗПР от 2016 г. или в други закони, като Закона за разузнавателните служби от 1994 г. или Закона за уреждане на правомощията за разследване от 2000 г., ще се прилагат също така за данни, предадени от ЕС към Обединеното кралство. Относно събирането на масиви от данни ЕКЗД подчертава, че съответните разпоредби в правото на Обединеното кралство позволяват да се събират данни извън Обединеното кралство; така че биха могли да включват транзитни данни, предавани от ЕИП към Обединеното кралство въз основа на решението относно адекватното ниво на защита[97]. Освен това ЕКЗД отбелязва, че Европейската комисия посочва, че „*[с]ледва да се отбележи, че задържането и събирането на комуникационни данни*

[95] В връзка с това Съдът на ЕС разгледа например, че Президентският изпълнителен указ 28 в САЩ не отговаря на изискванията, въпреки че съдържа някои ограничения във връзка със събирането на масиви от данни, вж. делото *Schrems II*, т. 181.

[96] Вж. решението на ЕСПЧ, *Big Brother Watch и други/the United Kingdom*, 13 септември 2018 г., ECLI:CE:ECHR:2018:0913JUD005817013 (наричано по-нататък „Big Brother Watch“), т. 325: „*Тъй като Кодексът за идентификационни кодове (IC Code) е публичен документ, който подлежи на одобрение от парламента, той трябва да бъде взет предвид както от тези, които изпълняват задължения по прихващане, така и от съдилищата и трибуналите, които оценяват предвидимостта на режима на Закона за уреждане на правомощията за разследване (ЗУПР)*.“

[97] Вж. член 183 и следващи от делото *Schrems II* относно оценката на законодателството, предвиждащо достъп до данни, които се прехвърлят между ЕС и трета държава във връзка с прието решение относно адекватното ниво на защита.

обикновено не засяга лични данни на субекти на данни от ЕС, които се предават по настоящото решение към Обединеното кралство. Задължението за съхраняване или разкриване на комуникационни данни съгласно части 3 и 4 от ЗПР от 2016 г. обхваща данни, които се събират от оператори на далекосъобщителни мрежи в Обединеното кралство директно от потребителите на далекосъобщителна услуга.[98]“ Независимо от това ЕКЗД подчертава липсата на яснота относно факта, че само подразделения на тези оператори, които се намират в Обединеното кралство, могат да получават искания от компетентните органи на Обединеното кралство, тъй като определението за оператор на далекосъобщителна мрежа в член 261, параграф 10 от ЗПР от 2016 г. изисква „операторът на далекосъобщителната мрежа да е лице, което предлага или предоставя далекосъобщителна услуга на лица в Обединеното кралство*, или лице, което контролира или предоставя далекосъобщителна система, която (изцяло или частично) се намира в Обединеното кралство или се контролира от Обединеното кралство*“. Следователно, лични данни на субекти на данни от ЕИП биха могли в действителност да бъдат засегнати, например в случай на данни, събирани или генерирани от подразделение на оператор на далекосъобщителна мрежа в Обединеното кралство, което се намира в ЕИП, предавани на подразделение на същия този оператор, което се намира в Обединеното кралство, въз основа на решението относно адекватното ниво на защита (за търговски цели) и след това събирани в рамките на Великобритания от компетентните публични органи.

159. **Поради това ЕКЗД е на мнение, че оценката на тези разпоредби е валидна и за оценката на нивото на адекватност на правната уредба на Обединеното кралство, и приканва Европейската комисия да поясни този аспект и да оцени допълнително до каква степен това е така. По-конкретно, ЕКЗД приканва Европейската комисия да поясни своето разбиране за обхвата на това законодателство, включително какво обхваща понятието „потребители на далекосъобщителни услуги“ и дали биха могли да бъдат поискани данни от подразделения на операторите на далекосъобщителна мрежа извън Обединеното кралство, доколкото са засегнати субекти на данни от ЕИП, предвид много широкото определение на операторите на далекосъобщителни мрежи.**

160. **Третата основна точка** засяга процедурата с „двойна защита“. ЕКЗД отбелязва, че в ЗПР от 2016 г. е въведена нова процедура с „двойна защита“. Независимо от това ЕКЗД разбира също така, че дори ако по принцип събирането и достъпът до данни за целите на националната сигурност или разузнаването може да се осъществи само със заповед, одобрена от съдебен комисар, в ЗПР от 2016 г. се предвижда, че *„в конкретни ограничени случаи е възможно законното прихващане да се извърши без заповед, като се изисква единствено предварителното разрешение от самите компетентни органи от РО[вж. раздела за Надзор по-долу], включително за прихващания в съответствие с искания на чужди държави (член 52 от ЗПР от 2016 г.).*“ Както е подчертано по-долу, това се отнася и за опасенията на ЕКЗД особено по отношение на разкритията в чужди държави. В допълнение ЕКЗД отбелязва също така, че по отношение на намесата в оборудването, както за определена цел, така за обработване на масиви от данни, също е възможна дерогация от процедурата с двойна защита и че съдебният комисар има право да одобрява само подновяване на заповеди за обработване на масиви от данни, след първоначален период от 6 месеца. **ЕКЗД призовава Европейската комисия да оцени допълнително и да демонстрира, че дори в случаите, когато не е приложима процедурата с двойна защита, правната уредба на Обединеното кралство предвижда подходящи гаранции, включително чрез възможности за ефективен *последващ***

[98] Вж. съображение 196 от проекторешението.

надзор и средства за правна защита, които се предоставят на гражданите, с което се гарантира ниво на защита, равностойно по същество на предоставяното в рамките на ЕС (вж. също раздел 4.3.3 относно надзора).

161. Освен това, въпреки че ЗПР от 2016 г. в действителност предвижда процедурата с „двойна защита“, ЕКЗД продължава да има опасения относно някои елементи от новото законодателство. След предоставянето на съответните раздели от проекторешението, ЕКЗД анализира следните видове събиране и достъп до данни в същата последователност, в която бяха представени от Европейската комисия. Последователността на оценените елементи по-долу не отразява йерархията по отношение на степента на загриженост на ЕКЗД.

4.3.1.2. Целево събиране и съхраняване на комуникационни данни

162. ЕКЗД отбелязва, че две длъжностни лица могат да дават целеви разрешения за получаване на комуникационни данни: разрешаващият служител в Службата за предоставяне на разрешения за комуникационни данни (наричан по-нататък „КПР“), определен висш служител (лице, заемащо разписана длъжност или ранг в съответен публичен орган), в допълнение към одобрението от съдебен комисар в определени случаи. За ЕКЗД обаче остава неясно, съгласно закона и съответния кодекс, кой точно служител разрешава кой вид целево събиране на комуникационни данни и до каква степен определеният служител ще бъде достатъчно независим[99].

163. **С оглед на това ЕКЗД приканва Европейската комисия да оцени допълнително този аспект и да представи по-ясна информация по тези елементи.**

164. Относно известието, което изисква съхраняването на комуникационни данни, ЕКЗД отбелязва също така, че такива известия биха могли да бъдат адресирани към „описание на операторите“. Това понятие изглежда означава, че съхраняването на данни за съобщения може да бъде поискано едновременно от няколко оператора. В действителност целевият характер на придобиването не е свързан с броя на операторите, а с имената или описанието на лицата, организациите, местонахожденията или групата от лица, които представляват „целта“, описание на характера на разследването и на дейностите, за които се използва оборудването. Поради това, ЕКЗД подчертава, че в зависимост от броя на операторите, засегнати от това „описание на оператори“, известието може да изисква съхраняването на повече данни, отколкото изглежда са заложените съгласно съдържанието на процедурата за целево съхранение. **ЕКЗД приканва Европейската комисия да оцени допълнително този аспект и да предостави уверения, че независимо дали известията са адресирани до няколко оператора, те остават ограничени до строго необходимото и пропорционалното.**

4.3.1.3. Намеса в оборудването

165. ЕКЗД отбелязва, че „намесата в оборудването“ може да се отклони от процедурата с двойна защита в случай на спешност[100]. Поради това ЕКЗД се опасява, че целите, за които се изисква такава намеса в оборудването, може да са прекалено обширни, а критериите за спешност (в този случай не се изисква от съдебния комисар да даде предварително разрешение след извършена оценка на необходимостта и пропорционалността на намесата в оборудването) остават неясни. Тъй като в последната ситуация „заповедта престава да има действие и не

[99] Вж. също по-долу относно оценката на процедурата с двойна защита и независимостта на съдебния комисар.

[100] Вж. член 109 от ЗПР от 2016 г.

може да бъде подновена“ в случай че съдебният комисар в последствие не одобри намесата в оборудването, ЕКЗД разбира, че междувременно събраните данни продължават да бъдат законно събрани. За да бъдат заличени тези данни, може да бъде издадена специална заповед от съдебния комисар[101].

166. **ЕКЗД приканва Европейската комисия да оцени допълнително условията, при които може да се направи позоваване на спешност, и да предостави разяснения относно възможните начини за упражняване на правата на засегнатите субекти на данни и предоставените им възможни средства за правна защита при операциите по намеса в оборудването, особено когато това се случва поради спешност, водеща до дерогация от процедурата с двойна защита.**

4.3.1.4. Масово прихващане на данни от носители

167. Както е описано в доклада за прегледа на правомощията[102] *„[п]рихващането на масиви от данни по принцип включва събирането на комуникация, докато тя преминава през определени носители (комуникационни връзки)*.“ Официалната справка за ЗПР от 2016 г. описва „масовото прихващане“ като „*процесът на събиране на обем от комуникация, след което се избира комуникация за изчитане, преглеждане или прослушване, когато това е необходимо и пропорционално*.“ ЕКЗД отбелязва, че „масовото прихващане“ означава събирането на данни още преди филтрирането им по критерии за подбор (или просто при наблюдението на вече известни лица, които представляват заплаха, или комплексно при идентифицирането на нови заплахи и на неизвестни досега лица, представляващи интерес).

168. Придобиването на масиви от комуникационни данни беше също така един от въпросите, разгледани от Съда на ЕС по делото Privacy International, което приключи с решение на голям състав, издадено на 6 октомври 2020 г. (в допълнение на това дали такова събиране на данни е извършено в контекста на правото на ЕС, дори за целите на националната сигурност). ЗПР от 2016 г. замени законодателството, което беше предмет на това съдебно решение.

169. ЕКЗД отбелязва, че с въвеждането на ЗПР от 2016 г. в правото на Обединеното кралство сега се изисква заповед за прихващане на масиви от данни. Процесът на издаване на такава заповед се позовава на определението за „оперативни цели“. Списъкът на тези оперативни цели се съставя от ръководителите на разузнавателните служби и се одобрява от държавния секретар. Самото решение се одобрява от независим съдебен комисар, който трябва да провери дали заповедта е необходима и пропорционална на оперативните цели. ЕКЗД разбира, че съдебният комисар няма правомощие да оценява самите оперативни цели, а дали заповедта е необходима и пропорционална на посочените в нея оперативни цели. На Парламентарната комисия по разузнаване и сигурност се предоставя копие от списъка на всеки три месеца, а министър-председателят проверява списъка на тези оперативни цели най-малко веднъж годишно.

170. Въз основава на елементите, предоставени от Европейската комисия в проекторешението обаче, изглежда трудно да се оцени обхватът на оперативните цели, посочени в списъка, както и дали събирането на данни, което се позволява във връзка с тях, отговаря на прага, определен

[101] Вж. член 110, параграф 3, буква b) от ЗПР от 2016 г.

[102] Вж. Доклад за преглед на правомощията относно прихващането на масиви от данни, представен от независимия оценител на законодателството за борба с тероризма, август 2016 г.

от Съда на ЕС (например ограничаването на събирането на данни до географски район може да е стеснено до няколко улици, както и събирането на данни от ЕИП като цяло).

171. В допълнение ЕКЗД подчертава, че данни, събрани за създаване на масиви от данни, може да бъдат съхранявани за дълги периоди от време (за да бъдат на разположение при последващ достъп за разглеждане). В действителност ЕКЗД отбелязва, че в член 150, параграфи 5 и 6 от ЗПР от 2016 г. се предвижда единствено унищожаването на копията на събраните данни и само, ако съхраняването им не е необходимо или няма вероятност да стане необходимо в интерес на националната сигурност или на други основания, попадащи в обхвата на член 138, параграф 2 от ЗПР от 2016 г., или ако съхраняването им не е необходимо по няколко други причини[103]. ЕКЗД подчертава, че тези основания изглеждат много общи и във всеки случай се споменават само копия на получените данни.

172. Освен това ЕКЗД отбелязва, че ЗПР от 2016 г. позволява също така в спешни случаи заповедите да бъдат изменени без предварителното одобрение на съдебен комисар и че в този случай, ако след последващото сезирането на съдебния комисар, което трябва да стане в рамките на три работни дни, той откаже да одобри изменението, заповедта следва да породи действие все едно не е било направено изменение, но междувременно събраните данни продължават да бъдат законно събрани[104]. За да бъдат заличени тези данни, може да бъде издадена специална заповед от съдебния комисар[105].

173. **Затова ЕКЗД приканва Европейската комисия към допълнителни пояснения и оценка на масовите прихващания, по-конкретно, във връзка с избора и прилагането на критерии за подбор по отношение на процедурите за масово прихващане, за да се изясни степента, до която достъпът до лични данни отговаря на прага, определен от Съда на ЕС (вж. също по-долу раздел 4.3.1.7., по-конкретно относно надзора върху критериите за подбор), както и какви гаранции са предвидени за защита на основните права на гражданите, чиито данни са прихванати, включително сроковете за съхранението на данните. Независима оценка от компетентните надзорни органи на Обединеното кралство би била особено полезна.**

174. **ЕКЗД подчертава също така, че изглежда още по-важно, че „свързаните с чужди държави съобщения“, които са в обхвата на практиките за масово прихващане, дават основание да се заключи, че данните могат да бъдат масово пряко прихванати и събрани в рамките на ЕИП от Обединеното кралство, включително по отношение на данни, които се предават транзитно между ЕИП и Обединеното кралство, които биха попаднали в обхвата на проекторешението (вж. по-долу раздел 4.3.2. относно последващото използване на събраната информация за целите на националната сигурност и разкриването ѝ в чужбина).**

4.3.1.5. Защита и гаранции за вторични данни

175. В допълнение ЕКЗД се опасява, че съответното законодателство на Обединеното кралство, свързано с масовото прихващане на информация, не предвижда същото ниво на защита на всички комуникационни данни. „Вторични данни“, които могат да бъдат получени със заповед за създаване на масив от данни съгласно член 137 от ЗПР от 2016 г., са „данни за системи“, „*които се състоят, са включени като част от или са прикрепени или логично свързани с комуникация (от изпращача или по друг начин)*“ и „идентифициращи данни“, „*които се състоят, са включени като част от или са прикрепени или логично свързани с комуникация*

[103] Вж. член 150, параграфи 3 и 6 от ЗПР от 2016 г.
[104] Вж. член 147 от ЗПР от 2016 г. (част 6, глава I).
[105] Вж. член 181,параграф 3, буква b) от ЗПР от 2016 г.

(от изпращача или по друг начин), която може да бъде логически отделена от останалата част на комуникацията, и ако бъде отделена, не би разкрила нещо, което основателно може да се счита за смисъл (ако има такъв) на комуникацията, независимо от всеки смисъл, свързан с факта на комуникацията, или с данни, свързани с предаването на комуникацията"[106].

176. ЕКЗД отбелязва, че тези „вторични данни", известни също като „метаданни"[107], събирани групово, изглежда, не се ползват със същите гаранции като данните, събрани с целева заповед, но също и като данни за съдържание, събрани групово. В действителност ЕКЗД отбелязва, че изборът за обработване на всяко прихванато съдържание се ползва от повече гаранции[108] в сравнение с избора на вторични данни[109].

177. Освен това ЕКЗД подчертава, че както ЕСПЧ[110], така и Съдът на ЕС[111] са поставили под съмнение факта, че тези данни са по-малко чувствителни от други данни, и по-специално от данните за съдържанието. В действителност Кодексът на добрите практики относно прихващанията представя примери за „вторични данни" (както „данни за системи", като профили за конфигуриране на рутери, адреси на електронна поща или идентификатори на потребители, така и алтернативни идентификатори на профили, както и „идентифициращи данни", като мястото на среща в календара за ангажименти, фотографска информация, като час, дата и място на заснемане). **Затова ЕКЗД подчертава единната оценка на ЕСПЧ и Съда на ЕС, и припомня изразените опасения във връзка с вторичните данни, за които би следвало да има въведени специални гаранции поради тяхната чувствителност. Поради това ЕКЗД приканва**

---

[106] Определенията на „данни за системи" и „идентифициращи данни" са дадени в член 263 от ЗПР от 2016 г.

[107] Вж. Доклад за преглед на правомощията относно прихващането на масиви от данни, представен от независимия оценител на законодателството за борба с тероризма, август 2016 г.

[108] Вж. член 152, параграф 1, буква c), член 152, параграф 3 и следващите от ЗПР от 2016 г.

[108] Вж. член 152, параграф 1, буква c), член 152, параграф 3 и следващите от ЗПР от 2016 г.

[109] Вж. член 152, параграф 1, букви a и b) от ЗПР от 2016 г.

[110] Вж. решение на ЕСПЧ, *Big Brother Watch*, т. 357, по сезиране на голям състав: „*Следователно, въпреки че Съдът не се съмнява, че приведените комуникационни данни са съществен инструмент за разузнавателните служби в борбата им с тероризма и тежката престъпност, не смята, че органите са постигнали справедлив баланс между спорещите публични и частни интереси, като изцяло са го лишили от гаранциите, които са приложими за търсенето и разглеждането на съдържание. Въпреки че Съдът не предлага свързаните комуникационни данни да бъдат достъпни само с цел да се определи дали дадено лице се намира на Британските острови или не, тъй като в този случай това би изисквало прилагането на по-стриктни стандарти за свързаните комуникационни данни от тези, които се прилагат за съдържанието, независимо от това би следвало да има въведени достатъчно гаранции, за да се гарантира, че изключването на тези свързани комуникационни данни от изискванията на член 16 от ЗУПР е ограничено само до необходимата степен за определяне на това дали дадено лице към момента се намира на Британските острови.*"

[111] Вж. решение на Съда на ЕС, *Privacy International*, т. 71: „*Произтичащата от предаването на службите за сигурност и разузнавателните служби на данни за трафик и на данни за местонахождение намеса в правото, закрепено в член 7 от Хартата, трябва да се смята за особено тежка най-вече предвид чувствителния характер на информацията, която тези данни могат да предоставят, и по-специално предвид възможността чрез тях да се установи профилът на съответните лица — информация, която е също толкова чувствителна, колкото и самото съдържание на комуникацията. Освен това тя може да породи усещане в съзнанието на съответните лица, че личният им живот е обект на постоянно наблюдение (вж. по аналогия решенията от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 27 и 37 и от 21 декември 2016 г., Tele2, C-203/15 и C-698/15, EU:C:2016:970, т. 99 и 100)*."

Европейската комисия внимателно да прецени дали гаранциите, предвидени в правото на Обединеното кралство относно тази категория лични данни, осигуряват по същество равностойно ниво на защита на гарантираното в ЕС ниво.

4.3.1.6. Автоматизирано обработване на комуникационни данни

178. ЕКЗД отбелязва, че органите на разузнавателната общност не само че използват прости или сложни критерии за подбор при филтриране на придобитите масиви от данни, но могат да разчитат също така на други инструменти за автоматизирано обработване за анализ на *„големи обеми от информация, която дава възможност на агенциите да открият връзки, модели, асоциации и поведения, които биха могли да докажат наличието на сериозна заплаха, която изисква разследване“*, съгласно доклада от 2015 г. на комисията по разузнаване и сигурност[112]. **ЕКЗД е запознат с факта, че този публичен доклад се отнася за практиките по предишната правна уредба, която впоследствие беше заменена от ЗПР от 2016 г. Въпреки това той вижда необходимост от допълнителна независима оценка и надзор на използването на инструменти за автоматизирано обработване от компетентните надзорни органи на Обединеното кралство и приканва Европейската комисия да направи допълнителна оценка на този въпрос, и на гаранциите, които ще бъдат и/или биха могли да бъдат предоставени на субектите на данни в ЕИП**.

4.3.1.7. Рискове от несъответствие и несъответстващи практики на компетентните органи на разузнавателната общност

179. ЕКЗД отбелязва, че има налични подробни доклади за извършен надзор. Те предоставят ценни елементи за това, което се оценява като положителни съответстващи практики, както и за установените рискове от несъответствие и несъответстващи практики.

180. Във връзка с това, съгласно КПР в доклада му за 2019 г., няколко елемента относно прилагането на правната уредба от различните компетентни органи разкриват някои (рискове от) несъответствия от компетентните органи.

181. Първо, ЕКЗД е забелязал, че критериите за класифициране на набор от данни като масиви от лични данни или като целеви данни сякаш не са винаги ясни за самите МИ5 и ШИС, особено за МИ5, което може да доведе до липсата на прилагане на подходящи гаранции за защита на данните[113]. В своя доклад за 2019 г. КПР припомня, че *„този въпрос следва да бъде разрешен*

---

[112] Вж. Intelligence and Security Committee of Parliament, Privacy and Security: A modern and transparent legal framework (Парламентарна комисия по неприкосновеност на личния живот и сигурност: модерна и прозрачна правна уредба), 2015 г., параграф 18, стр. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

[113] Вж. Годишен доклад на Комисаря за правомощията за разследване за 2019 г., 15 декември 2020 г., точка 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: *„Отбелязваме положителното развитие на Състава за надзор на масивите от данни (BOP) и неговото въздействие върху управлението на вътрешното съответствие. Продължаваме да се стремим към по-голяма яснота относно използвания от МИ5 процес за извършване на първоначални проверки на нови набори от данни, за да разберем по-добре решенията за класифициране на набор от данни като масиви от лични данни (BPD) или например като целеви данни. Имахме опасения поради едно нерешено действие по протокола на BOP относно разрешаването на несъответствия между разпределени BPD между МИ5 и ШИС. Възможно е поради различните употреби на данните и различните части от данни, които се съхраняват, при двете агенции да се намира един и същ набор от данни или версии от него, които законно да бъдат категоризирани като масив от данни от едната агенция и като целеви данни от другата агенция.*

приоритетно“[114]. Във връзка с масивите от лични данни ЕКЗД отбелязва също така, че според ПЦК, въпреки че класификацията на масивите от лични данни изглежда удовлетворителна (но предстои да бъде проверена от КПР) през март 2019 г., вътрешната проверка за съответствие на заповедите от специализирания екип е изразила сериозни опасения, тъй като 50 % от обосновките за получаване на заповеди за масово събиране, проверени от екипа на ПЦК за проверка на съответствието, не са отговаряли на изисквания стандарт. Според КПР екипът за проверка на съответствието е започнал работа по разследването на проблема и по ново обучение на персонала с цел подобряване на стандарта. Новото обучение относно разпоредбите на ЗПР от 2016 г. и допълнителното обучение, предоставено от мрежите за политики и съответствие (наричани по-нататък „МПС“), са допринесли за подобряване на съответствието на GCHQ в тази област. КПР не очаква да има отклонение от стандарта при бъдещи проверки, но ще продължи да наблюдава тази област внимателно[115]. **Поради това ЕКЗД споделя мнението, че са необходими допълнителна проверка и наблюдение на посочените елементи от страна на Европейската комисия като част от оценката на нивото на защита, за да се гарантира подобряване на този стандарт, както се подчертава в доклада на КПР, и напомня, че изпълнението и конкретното прилагане на правната уредба също трябва да бъдат взети предвид, както се посочва в член 45 от ОРЗД, при оценката на равностойното ниво на защита на дадена трета държава.**

182. В по-широк план ЕКЗД подчертава основните точки, споделени от КПР, относно „търсения, основани на задачи“, извършвани от офицерите на МИ5, при които на разследващия е позволено да извърши повече от едно търсене в масиви от лични данни, които са на негово разположение, и „*сериозните рискове за съответствието, свързани с определени технологични среди, които се използват от МИ5*“, относно мястото на съхранение на данните в средата, кой има достъп до тях, степента, до която са копирани или споделени, приложените процеси по изтриването им, както и относно сроковете за съхранение. Независимо че КПР посочва, че са взети мерки и са въведени гаранции, някои от тях все още не са автоматизирани и се водят от отделни лица, затова той подчертава, че е от съществено значение „*МИ5 да продължи да поддържа тези нови процеси и да предвиди достатъчно ресурси за тяхното ефективно функциониране. Ако МИ5 установи нарастване на случаите на несъответстващо поведение*“[116]. КПР очаква те да бъдат представени на неговото внимание във възможно най-кратък срок. **Поради това ЕКЗД приканва Европейската комисия да наблюдава внимателно тези аспекти в бъдеще**.

183. Относно ПЦК, ЕКЗД разбира също така от доклада на КПР, че за операциите, извършвани по заповедите за обработване на масиви от данни, „*качеството на заявленията за вътрешно одобрение е променливо и забелязахме, че има какво да се подобри в начина, по който се формулират тези заявления*“[117], и че по отношение на целевата намеса в оборудването поясненията за използването на общите дескриптори понякога са твърде общи и непрецизни[118]. ЕКЗД забеляза също така, че по отношение на масовата намеса в оборудването КПР препоръчва „*в заявленията да се посочва последователно и изрично връзката между*

Има риск, ако една от агенциите неправилно е категоризирала държаните данни като целеви, тези данни да бъдат държани без подходяща заповед и спрямо тях да не се прилагат подходящи гаранции.“

[114] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 8.39.

[115] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.48.

[116] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 8.52.

[117] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.2.

[118] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.16 и 10.17.

целта и предвидената от закона цел и разузнавателните изисквания“[119], *„във всички заявления да се посочва ясно възможността за съпътстващо проникване и съответни мерки за смекчаване при оценката на пропорционалността*“[120], като подчертава, че въпреки напредъка “*все още има какво да се подобри*“[121] и ще бъде необходимо да се обърне допълнително внимание на тези аспекти в бъдеще.

184. Във връзка с режима на масово прихващане съгласно Закона за уреждане на правомощията за разследване от 2000 г. (наричан по-нататък „ЗУПР от 2000 г.“), който след това беше заменен от разпоредби в ЗЗД от 2016 г., ЕКЗД напомня, че недостатъчният надзор както върху избора на интернет носители за прихващане и филтриране, така и върху търсенето и подбора на прихванатата комуникация за проверка, е един от основните аспекти, които ЕСПЧ е сметнал за несъответстващ на член 8 от ЕКПЧ по отношение на предишната правна уредба на правомощията за разследване на органите на Обединеното кралство в сферата на националната сигурност по делото *Big Brother Watch*, отнесено понастоящем към голям състав. **ЕКЗД приканва Европейската комисия да провери текущото състояние на производството, да вземе тези елементи предвид и да ги посочи в решението относно адекватното ниво на защита, в случай че го приеме.**

185. В този случай ЕСПЧ: „*не беше убеден, че гаранциите, уреждащи подбора на носители за прихващане и подбора на прихванат материал за проверка, са достатъчно надеждни, за да могат да осигурят достатъчно гаранции срещу злоупотреба. Най-голяма загриженост буди обаче липсата на надежден независим надзор върху критериите за подбор и критериите за търсене, които се използват за филтриране на прихванатата комуникация*.“[122] Както е подчертано от КПР*, „тази констатация отразява подобна препоръка в доклада на Комисията за разузнаване и сигурност относно неприкосновеността на личния живот и сигурността: съвременна и прозрачна правна уредба от март 2015 г.“*[123]. **ЕКЗД приветства също така факта, че впоследствие КПР извърши проверка на своя подход за инспектиране на масовото прихващане през 2019 г., „*която включваше внимателен преглед на технически сложните начини, по които на практика се извършва масовото прихващане*“[124], и се ангажира да включи „*подробно разглеждане на критериите за подбор и на критериите за търсене, за които се споменава по-горе от ЕСПЧ*“[125] в инспекциите на масовото прихващане от данни от 2020 г. нататък. Като се има предвид значението на този аспект, ЕКЗД се опасява, че все още не е извършено подробно разглеждане на критериите за подбор и на критериите за търсене от КПР, и призовава Европейската комисия да наблюдава внимателно промените в това отношение, особено след като конкретният формат на този надзор предстои да бъде изяснен[126].**

[119] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.23.
[120] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.23.
[121] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.23.
[122] Вж. решение на ЕСПЧ, *Big Brother Watch*, т. 347.
[123] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.28.
[124] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.28.
[125] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., т. 10.28.
[126] Вж. Годишен доклад на комисаря за правомощията за разследване за 2019 г., точка 10.28: „точният формат на тази проверка предстои да бъде съгласуван“.

4.3.2. Последващо използване на събраната информация за целите на националната сигурност и разкриването ѝ в чужбина

186. Що се отнася до последващото използване на събраната информация за целите на националната сигурност, Европейската комисия се позовава в своята оценка на член 87, параграф 1 от ЗЗД от 2018 г., който предвижда, че „*така събраните лични данни не трябва да бъдат обработвани по начин, който е несъвместим с целта, за която са събрани*“. ЕКЗД обаче посочва, че тази разпоредба може да подлежи на изключения, свързани с националната сигурност, съгласно член 110 от ЗЗД от 2018 г. Освен това ЕКЗД отбелязва, че по отношение на целевото прихващане и разглеждане, целевото събиране и съхраняване на комуникационни данни, целевата намеса в оборудването или по отношение на масовото прихващане и масовата намеса в оборудването, законодателството предвижда възможността за т.нар. „разкриване в чужбина“.

4.3.2.1. Последващо използване, разкриване в чужбина и приложима правна уредба в Обединеното кралство

187. Европейската комисия се е запознала с част 4 от ЗЗД от 2018 г., и по-специално член 109 от нея, като съответни разпоредби, в които се определят конкретни изисквания за последващото използване на събраната информация, и особено относно международното предаване на лични данни от разузнавателните служби към трети държави или международни организации. ЕКЗД отбелязва обаче, че в член 110 от ЗЗД от 2018 г. се предвижда изключение във връзка с националната сигурност, посочвайки че определени разпоредби от ЗЗД от 2018 г. не се прилагат, ако се изисква изключение от тези разпоредби с цел да се гарантира националната сигурност. Съответните разпоредби, които може да не се прилагат, включват глава 2 от част 4 от ЗЗД от 2018 г., която е свързана с принципите за защита на личните данни, включително ограничение на целите, както и глава 3 от част 4 от ЗЗД от 2018 г., която се отнася до правата на субектите на данни. Член 109 от ЗЗД от 2018 г. във връзка с член 110 от ЗЗД от 2018 г. и условията, при които се прилага, може да доведат до случаи, в които международното предаване на лични данни от разузнавателни служби към трети държави се извършва, без да се прилагат разпоредбите, свързани с принципите за защита на личните данни и с правата на субектите на данни.

188. Както е установено от Европейската комисия, това изключение трябва да бъде оценено за всеки отделен случай и може да се използва само доколкото прилагането на конкретна разпоредба би имало отрицателни последици за националната сигурност. В действителност издаването на национално удостоверение на разузнавателните служби на Обединеното кралство има за цел да удостовери, че е необходимо изключение по отношение на определени лични данни, които се обработват с оглед гарантиране на националната сигурност. ЕКЗД обаче отбелязва, че в своите насоки относно издаването на удостоверение за национална сигурност съгласно ЗЗД от 2018 г. Министерството на вътрешните работи на Обединеното кралство пояснява, че „*[е] важно да се отбележи от самото начало, че не се изисква удостоверение за позоваване на изключението, свързано с националната сигурност; всъщност в повечето случаи администраторите ще определят сами дали е приложимо изключението, свързано с националната сигурност*.“ [127] Освен това Министерството на вътрешните работи на Обединеното кралство отбелязва, че „*удостоверенията за национална*

[127] Вж. Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020 (Министерство на вътрешните работи на Обединеното кралство, Закон за защита на данните от 2018 г., Насоки за удостоверенията за национална сигурност), август 2020 г., параграф 3, стр. 3.

сигурност може да се прилагат за лични данни, които могат да бъдат конкретно удостоверени или които обхващат по-широка категория лични данни. Те може да са превантивни, както и ретроспективни.“ [128] Следователно изключението във връзка с националната сигурност може да се прилага при международно предаване на лични данни от разузнавателни служби на трети държави при отсъствие на удостоверение за национална сигурност.

189. ЕКЗД освен това отбелязва, че например удостоверението за национална сигурност DPA/S27/Security Service[129] предвижда, че до 24 юли 2024 г. обработените лични данни „ *за, от името на, по искане на или с помощта на Службата за сигурност или* “ и „*когато това обработване е необходимо за улесняване на надлежното изпълнение на функциите на Службата за сигурност, описани в член 1 от Закона за Службата за сигурност (Security Service Act)*“ от 1989 г. са освободени от съответните разпоредби в правото на Обединеното кралство, свързани с глава V от ОРЗД във връзка с предаванията на лични данни на трети държави или на международни организации. Докато другите публично достъпни удостоверения за национална сигурност не предвиждат изключение от разпоредбите на член 109 от ЗЗД от 2018 г., следва да се напомни, че някои или всички текстове на удостоверението може да не бъдат публикувани, ако има вероятност това да е в разрез с интересите на националната сигурност, би противоречало на обществения интерес или би могло да застраши безопасността на съответното лице.

190. По принцип, при оценката на проекта на решение във връзка с тези разпоредби, ЕКЗД отбелязва, че гаранциите за тези оповестявания включват единствено условието получателят на данните да спазва изискванията относно сигурността на данните, степента на оповестяването да е ограничена до необходимата, съхраняването на данните и ограничаването на достъпа до данни до ограничен брой лица. Затова **ЕКЗД подчертава, че що се отнася до разкриванията в чужбина, прилагането на изключението относно националната сигурност, предвидено в правото на Обединеното кралство, може да доведе до ситуации, в които гаранциите за спазването на принципите за ограничение на целите, необходимостта и пропорционалността, както и за спазването на правата на гражданите, надзора и средствата за правна защита в третата държава на местоназначение няма да бъдат напълно осигурени или зачетени. Поради това, ЕКЗД препоръчва на Европейската комисия да разгледа допълнително всички гаранции, предвидени в законодателството на Обединеното кралство в областта на разкриването в чужбина, по-специално при прилагането на изключенията относно националната сигурност.**

4.3.2.2. Разкриване в чужбина и споделяне на разузнавателни данни във връзка с международното сътрудничество

191. ЕКЗД отбелязва също така, че Европейската комисия не е взела предвид като част от своята оценка на адекватността съществуващите международни споразумения, сключени между Обединеното кралство и трети държави или международни организации, които може да

[128] Вж. Home Office, The Data Protection Act 2018, National Security Certificates Guidance, August 2020 (Министерство на вътрешните работи на Обединеното кралство, Закон за защита на данните от 2018 г., Насоки за удостоверенията за национална сигурност), август 2020 г., параграф 5, стр. 4.

[129] Вж. DPA/S27/Security Service, член 27 от ЗЗД от 2018 г., Удостоверение на министъра на вътрешните работи, 24 юли 2019 г., https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf

съдържат конкретни разпоредби относно международното предаване на лични данни от разузнавателните служби към трети държави.

192. ЕКЗД подчертава също така, че оценката на Европейската комисия се позовава основно на оценката на част 4 от ЗЗД от 2018 г., но ЕКЗД има сериозни опасения, че в ЗПР от 2016 г. се уреждат „искания“ за обмен на разузнавателна информация с чуждестранни партньори, но не се разглеждат други форми на споделяне на разузнавателна информация. Във връзка с това Комитетът отбелязва, че проекта на решение на Европейската комисия не се позовава или не прави оценка на съгласуването между правната уредба на Обединеното кралство и Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на комуникацията („Споразумение между Обединеното кралство и САЩ относно разузнаването в областта на комуникацията“). В неотдавнашно изявление за отбелязване на 75-ата годишнина от това споразумение Националната агенция за сигурност на САЩ (наричана по-нататък „НАС“) се казва, че това партньорство позволява *„да се споделя информация между двете агенции в максималната възможната степен, с минимални ограничения*“ и че въз основа на този *„паметен документ са създадени политиките и процедурите на професионалистите на САЩ и Обединеното кралство относно споделянето на комуникация, превода, анализа и информацията за разбиване на кодове*.“[130] Това споразумение също така стана основа за други партньорства с Австралия, Канада и Нова Зеландия.

193. Секретният характер на това споразумение и неговите конкретни разпоредби представляват сериозно предизвикателство по отношение на яснотата и предвидимостта на правото във връзка с последващото използване и разкриването в чужбина на информация, събрана от органите на Обединеното кралство за целите на националната сигурност. ЕКЗД напомня, че що се отнася до нивото на гарантираната в рамките на ЕС защита, Съдът на ЕС е подчертал, че законодателство, което включва намеса в основното право на защита на личните данни, трябва *„да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да установяват минимални изисквания, така че лицата, чиито данни са били предадени, да разполагат с достатъчни гаранции, позволяващи ефикасна защита на техните лични данни срещу рискове от злоупотреби и от неправомерен достъп и използване на такива данни. Необходимостта от такива гаранции е още по-голяма, когато личните данни са подложени на автоматизирано обработване и когато има значителен риск от неправомерен достъп до такива данни.*“[131]. Поради това ЕКЗД смята, че Европейската комисия следва да разгледа въздействието на Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на съобщенията като част от своята оценка на адекватността.

194. ЕСПЧ в своето решение по първи раздел от 13 септември 2018 г. в делото *Big Brother Watch* оцени режима на Обединеното кралство за споделяне на разузнавателни данни, и по-специално Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на съобщенията. В действителност ЕСПЧ заяви, че *„[з]аконовата уредба, която позволява на разузнавателните служби на Обединеното кралство да искат прихванат материал от чужди разузнавателни агенции, не се съдържа в ЗУПР. Със Споразумението за радиотехническа разузнавателна дейност между Великобритания и САЩ от 5 март 1946 г. изрично се разрешава обменът на материали между Съединените щати и Обединеното*

[130] Вж. съобщението за медиите на НАС, GCHQ and NSA Celebrate 75 Years of Partnership (ПЦК и НАС честват 75 години партньорство), 5 февруари 2021 г., https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.
[131] Вж. делото *Schrems I*, т. 91.

кралство“[132] и се смята, че има *„основание в правото за искането на разузнавателна информация от чужди разузнавателни агенции и че това право е достъпно в достатъчна степен*.“[133] ЕСПЧ е стигнал до заключението, че няма нарушение на член 8[134] от ЕКПЧ във връзка с режима на споделяне на разузнавателни данни, но отбелязва, че това решение е отнесено към големия състав и се очаква неговото решение. ЕКЗД отбелязва също така, че в частично съвпадащо, частично противоположно мнение по това решение съдия Koskelo, към когото се е присъединил съдия Turković[135], е стигнал до заключението, че има нарушение на член 8 от ЕКПЧ във връзка с режима на споделяне на разузнавателни данни, като е заявил, че *„[л]есно е да се съгласим с принципа, че всяка договореност, по която се получават разузнавателни данни от прихванатата комуникация, получена чрез чужди разузнавателни служби въз основа на искания за извършване на прихващане или за предаване на резултатите от него, не следва да се допуска да води до заобикаляне на гаранциите, които трябва да са осигурени при всяко наблюдение от националните органи (вж. точки 216, 423 и 447). В действителност всеки друг подход би бил неправдоподобен*“.

195. Както е подчертано в няколко репортажа на медиите и на неправителствени организации[136][137], последната версия на Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на комуникацията, която е оповестена публично, е от 1956 г., но оттогава комуникационните технологии и характерът на разузнавателните сигнали са се променили значително. Медийни репортажи например разкриха, че данните, предавани чрез подводни кабели, които се попадат в Обединеното кралство, се прихващат от ПЦК и на НАС се осигурява достъп до тях[138].

196. За ЕКЗД основен въпрос във връзка със споделянето на разузнавателна информация е дали член 109 от ЗЗД от 2018 г. и разпоредбите на ЗПР от 2016 г. остават приложими, когато разузнавателните служби на Обединеното кралство действат в съответствие със Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на съобщенията. Друг основен елемент, който трябва да бъде оценен, е дали разпоредбите или ефективното прилагане на това споразумение оказват въздействие върху нивото на защита на транзитно предаваните лични данни от ЕИП към Обединеното кралство или дали позволяват пряк достъп и придобиване на лични данни от разузнавателните служби на друга трета държава.

197. Поради това в допълнение към изразените резерви относно „разкриванията в чужбина“ въз основа на част 4 от ЗЗД от 2018 г. и свързаното с нея изключение относно националната

---

[132] Вж. решение на ЕСПЧ, *Big Brother Watch*, т. 425.
[133] Вж. решение на ЕСПЧ, *Big Brother Watch*, т. 427.
[134] Вж. решение на ЕСПЧ, *Big Brother Watch*, т. 448.
[135] Вж. решение на ЕСПЧ, *Big Brother Watch*, частично съвпадащо, частично противоположно мнение на съдия Koskelo, към което се е присъединил съдия Turković.
[136] Вж. BBC, Diary reveals birth of secret UK-US spy pact that grew into Five Eyes (Дневник разкрива таен пакт между ОК и САЩ за шпиониране, който прераства в споразумение между пет държави) , 5 март 2021 г., https://www.bbc.com/news/uk-56284453.
[137] Вж. Privacy International, Policy Briefing — UK Intelligence Sharing Arrangements (Брифинг за политиката-споразуменията на ОК за обмен на разузнавателна информация), април 2018 г., https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.
[138] Вж. The Guardian, GCHQ taps fibre-optic cables for secret access to world's communications (ПЦК прониква в кабелите с оптични влакна за таен достъп до световното общуване), 21 юни 2013 г., https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

сигурност, както и въз основа на искания в рамките на ЗПР от 2016 г., **ЕКЗД изказва опасения относно наличието на други форми на споделяне и разкриване на информация въз основа на други инструменти, по-специално различните международни споразумения, сключени от Обединеното кралство с други трети държави, особено когато тези инструменти остават недостъпни за обществеността, какъвто е случаят със Споразумението между Обединеното кралство и САЩ относно разузнаването в областта на съобщенията. Последиците от това споразумение биха могли да доведат до заобикаляне на установените гаранции във връзка с достъпа и използването на лични данни за целите на националната сигурност.**

198. В действителност ЕКЗД споделя мнението, изразено от специалния докладчик към Обединените нации Joe Cannataci, че *„[с]поделянето на разузнавателна информация не трябва да създава вратички за получаване или улесняване на другите да получават разузнавателна информация, по отношение на която не се прилагат национални гаранции, нито да позволява на чуждестранни правителства с по-ниски стандарти на защита на неприкосновеността на личния живот (или на други човешки права) да получават разузнавателни данни от Обединеното кралство, които биха могли да доведат до нарушаване на човешките права“*[139].

199. Освен това **ЕКЗД смята, че сключването на двустранни или многостранни споразумения с трети държави за целите на сътрудничеството в областта на разузнаването, предвиждащи правно основание за пряко прихващане и придобиване на лични данни или за предаване на лични данни на тези държави, също може значително да повлияе на условията за последващо използване на събраната информация, тъй като тези споразумения може да окажат влияние на вече оценената правна уредба на Обединеното кралство в областта на защитата на личните данни.**

4.3.3. Надзор

200. ЕКЗД подчертава важността на цялостния надзор от независими надзорни органи за осигуряване на адекватно ниво на защита на личните данни. Гарантирането на независимост на надзорните органи по смисъла на член 8, параграф 3 от Хартата на ЕС има за цел да осигури ефективно и надеждно наблюдение на спазването на правилата за защита на гражданите във връзка обработването на техните лични данни.

201. По отношение на достъпа и използването на лични данни за целите на националната сигурност надзорната функция се изпълнява основно от КПР и съдебните комисари (наричани по-нататък „съдебни комисари“).

202. **ЕКЗД по принцип признава като значително подобрение въвеждането на съдебните комисари в ЗПР от 2016 г.** В съответствие с отправено по-горе искане Европейската комисия се приканва да оцени по-подробно независимостта на **съдебните комисари, и по-специално до каква степен независимостта на КПР и на службата на КПР (наричана по-нататък „СКПР“) е правно обоснована, тъй като в ЗПР от 2016 г. няма такава правна разпоредба.** Това е още по-

[139] Вж. End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland (Край на изявлението на специалния докладчик по правото на неприкосновеност на личния живот при приключването на неговата мисия в Обединеното Кралство и Северна Ирландия), Лондон, 29 юни 2018 г., https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

важно, тъй като КПР взема решения по обжалвания от правителството в случай на отхвърляне на заявление за **мярка** за наблюдение **от** съдебен комисар.

203. КПР има функции за *предварителен*, както и за *последващ* надзор. Що се отнася до *предварителния* надзор, ЕКЗД разбира, че функцията на съдебните комисари е да одобряват в отделни случаи различни мерки за наблюдение, включително целево прихващане и масово събиране на комуникационни данни. ЕКЗД освен това отбелязва, че предварително одобрение на мерки за наблюдение не може да бъде обосновано от практиката на Съда на ЕС като абсолютно изискване за пропорционалността на тези мерки [140].

204. За да оцени ефективността на това ниво на надзор, ЕКЗД все пак вижда необходимост от допълнително пояснияване на сценариите, в които е възможно законно прихващане без предварително одобрение от съдебния комисар.

205. В своето проекторешение Европейската комисия споменава в бележки под линия 201 и 266 „специални ограничени случаи“, предвидени в ЗПР от 2016 г. в членове 44—52 във връзка с целевите прихващания. ЕКЗД отбелязва, че членове 45—51 от ЗПР от 2016 г. са изключения, за които се твърди, че не се използват редовно от разузнавателните служби. Освен това **ЕКЗД разбира** че в **случаите, в които се прилагат изключенията** (например за доставчици на далекосъобщителни и пощенски мрежи), предварителното одобрение на съдебните комисари се извършва в случай че правоприлагащите органи или разузнавателните служби **поискат** достъп до тези данни**, и приканва Европейската комисия да потвърди в своето решение, че това е така**.

206. ЕКЗД признава, че с член 44, параграф 2 от ЗПР от 2016 г. се разрешава прихващане на комуникация, ако една от страните (изпращач или получател) се е съгласила и има разрешение съгласно ЗУПР от 2000 г. или съгласно Закона за уреждане на правомощията за разследване от 2000 г. (Шотландия) (акт 11 на Шотландския парламент от 2000 г.), т.е. съгласно предишното правно положение преди създаването на съдебните комисари. ЕКЗД **приканва** Европейската комисия да поясни дали това означава, че в случаите когато има едностранно съгласие, процедурата за предварително одобрение няма да се прилага изобщо.

207. Що се отнася до *последващия* надзор, също е важно да се провери дали е гарантиран ефикасен независим надзор без пропуски, по-конкретно когато не е предвидена *предварителна* проверка.

208. ЕКЗД отбелязва, че за членове 48—52 от ЗПР от 2016 г. се извършва *последваща* проверка от съдебните комисари, и **приканва Европейската комисия да поясни съгласно кои изисквания и по чия инициатива следва да се извърши такава проверка**.

209. Съгласно член 229, параграф 4 от ЗПР от 2016 г. КПР не трябва да проверява упражняването на определени функции. В това отношение ЕКЗД приканва Европейската комисия да поясни разпоредбите на член 229, параграф 4, букви г) и д) от ЗПР от 2016 г. относно практическото му въздействие върху проверката на компетенциите на КПР. **Разбирането на ЕКЗД е, че СКИ е компетентният надзорен орган, когато се прилагат изключенията по член 229, параграф 4 от**

[140] Той отбелязва също така, че Съдът на ЕС при обявяването за невалиден на Щита за личните данни по делото *Schrems II* е взел предвид факта, че съгласно правото на САЩ т.нар. Съд за надзор на външното разузнаване (FISA Court) *„не дава разрешение за отделни мерки за наблюдение; а по-скоро за програми за наблюдение (като PRISM, UPSTREAM) въз основа на годишни сертифицирания*“.“ (т. 179).

ЗПР от 2016 г., и ЕКЗД приканва Европейската комисия да потвърди в своето решение, че това е така.

210. **Изглежда, че при провеждането на** *последващ* надзор **ролята** на КПР е **ограничена** до отправяне на препоръки в случаите на неспазване и до уведомяване на субекта на данните, ако грешката е сериозна и е от обществен интерес лицето да бъде информирано. **ЕКЗД приканва Европейската комисия да поясни как СКПР може ефективно да гарантира съответствието със закона.**

211. **Накрая, ЕКЗД разбира, че засегнатите граждани не могат да се обърнат пряко към СКПР, а трябва да подадат жалба до СКИ, който обаче има ограничени компетенции в областта на националната сигурност. Поради това ЕКЗД приканва Европейската комисия да поясни допълнително как е гарантирано законово, че СКПР разглежда жалби в тези случаи.**

4.3.4. Правни средства за защита

212. В светлината на решенията на Съда на ЕС по делата *Schrems I* и *Schrems II* е ясно, че ефективната съдебна защита по смисъла на член 47 от Хартата на ЕС е от основно значение за допускането на адекватност на закона на трета държава. Решенията показаха също така, че следва да се обърне специално внимание на ефективната съдебна защита по отношение на достъпа до личните данни за целите на националната сигурност.

213. **ЕКЗД признава, че Обединеното кралство е създало ТПР. ТПР е компетентен да разглежда дела за упражняването на правомощия за разследване не само от страна на правоприлагащи органи, но и от разузнавателни служби. Според разбирането на ЕКЗД, ТПР функционира като надлежно създаден съд по смисъла на член 47 от Хартата на ЕС. Що се отнася до неговите правомощия, Европейската комисия се приканва да потвърди, че ТПР също има всички правомощия, посочени в съображение 262 от проекторешението, независимо от правното основание, на което се завежда жалбата.**

214. Дискретното наблюдение от разузнавателните агенции често означава, че обектът на наблюдение — субектът на данни, не е информиран и няма да бъде информиран за наблюдението. В този смисъл, когато трябваше да анализира правото на САЩ, ЕКЗД многократно изрази опасенията си относно изискването за „постоянно“, съгласно тълкуването на правото на САЩ, в случаи на наблюдение. На този фон ЕКЗД отбелязва, че жалбата пред ТПР изисква тест за „убеждение“, според който жалбоподателят трябва да докаже, че по отношение на нея или на него съществува потенциален риск от използване на мярката.

215. В анализа по отношение на ТПР, ЕКЗД обръща особено внимание също така на факта, че многократно е било установявано, че функционирането на ТПР съответства на ЕКПЧ, съгласно тълкуването на ЕСПЧ.