

Становище на комитета (член 70, алинея 1, буква т)



**Становище 32/2021 относно проекта на Решение за
изпълнение на Европейската комисия съгласно
Регламент (ЕС) 2016/679 относно адекватното ниво на
защита на личните данни в Република Корея**

Версия 1.0

Прието на 24 септември 2021 г.

СЪДЪРЖАНИЕ

1.	ОБЩ ПРЕГЛЕД	4
1.1.	Области на сближаване	5
1.2.	Предизвикателства	5
1.2.1.	Общи положения	5
1.2.2.	Общи аспекти на защитата на данните	6
1.2.3.	Относно достъпа на публични органи до данни, предадени на Република Корея	7
1.3.	Заключение	8
2.	ВЪВЕДЕНИЕ	8
2.1.	Корейска рамка за защита на данните	8
2.2.	Обхват на оценката, извършена от КЗЛД	10
2.3.	Общи бележки и опасения	11
2.3.1.	Международни ангажименти, сключени от Република Корея	11
2.3.2.	Обхват на решението относно адекватното ниво на защита	11
3.	ОБЩИ АСПЕКТИ НА ЗАЩИТАТА НА ДАННИТЕ	12
3.1.	Принципи, отнасящи се до съдържанието	12
3.1.1.	Понятия	13
3.1.2.	Частични изключения, предвидени в Закона за защита на личната информация	15
3.1.3.	Основания за законосъобразна и добросъвестна обработка за легитимни цели	17
3.1.4.	Принцип на ограничаване в рамките на целта	18
3.1.5.	Принцип на качеството и пропорционалността на данните	19
3.1.6.	Принцип на запазване на данни	19
3.1.7.	Принцип на сигурност и поверителност	20
3.1.8.	Принцип на прозрачност	20
3.1.9.	Специални категории лични данни	21
3.1.10.	Право на достъп, коригиране, изтриване и възражение	22
3.1.11.	Ограничения на последващи предавания на данни	25
3.1.12.	Директен маркетинг	27
3.1.13.	Автоматизирано вземане на решения и профилиране	28
3.1.14.	Отчетност	29
3.2.	Процедурни механизми и механизми за правоприлагане	29
3.2.1.	Компетентен независим надзорен орган	29

3.2.2. Наличие на система за защита на данните, която гарантира добро равнище на съответствие	31
3.2.3. Системата за защита на данните трябва да осигурява подпомагане и помощ за субектите на данни при упражняването на техните права, както и подходящи механизми за съдебна защита.....	32
4. ДОСТЪП ДО И ИЗПОЛЗВАНЕ НА ПРЕДАВАНИТЕ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ ЛИЧНИ ДАННИ ОТ ПУБЛИЧНИТЕ ОРГАНИ В ЮЖНА КОРЕЯ.....	32
4.1. Обща рамка за защита на данните по отношение на достъпа на държавата	32
4.2. Защита и гаранции за данни, потвърждаващи за получени съобщения, по отношение на държавния достъп за целите на правоприлагането.....	33
4.3. Достъп до комуникационна информация от корейските публични органи за целите на националната сигурност	35
4.3.1. Липса на задължение за уведомяване на лицата относно държавния достъп до съобщения между чуждестранни граждани	35
4.3.2. Липса на предварително независимо разрешение за събиране на комуникационна информация между чуждестранни граждани.....	36
4.4. Доброволно разкриване на информация.....	38
4.5. По-нататъшно използване на информацията	39
4.5. Последващо предаване на данни и споделяне на разузнавателни данни	39
4.5.1. Приложима правна уредба за по-нататъшно предаване на данни от правоприлагащите органи.....	40
4.5.2. Приложима правна уредба за по-нататъшно предаване на данни за целите на правоприлагането.....	41
4.5.3. Международни споразумения	42
4.7. Надзор	43
4.8. Средства за правна и съдебна защита.....	43

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 и за отмяна на Директива 95/46/ЕО (по-нататък „ОРЗД“),

като взе предвид Споразумението за Европейското икономическо пространство („ЕИП“), и поспециално Приложение XI и протокол 37 към него, изменени 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. ОБЩ ПРЕГЛЕД

1. На 16 юни 2021 г. Европейската комисия стартира официалния процес по приемане на нейния проект на решение за изпълнение („**проект на решение**“) относно адекватното ниво на защита на личните данни в Република Корея съгласно Закона за защита на личната информация (ЗЗЛИ) в съответствие с ОРЗД².
2. На същата дата Европейската комисия поиска становището на Европейския комитет по защита на данните („**ЕКЗД**“) ³. Оценката на ЕКЗД относно адекватността на нивото на защита, което се осигурява в Република Корея, е извършена въз основа на анализ както на самия проект на решение, така и на информацията, предоставена⁴ от ЕК.
3. При извършването на оценката ЕКЗД насочи своето внимание както към общите аспекти, свързани с ОРЗД, заложи в проекта на решението, така и върху достъпа на публичните органи до лични данни, предадени от Европейското икономическо пространство (ЕИП), за целите на правоприлагането и националната сигурност, включително върху средствата за правна защита, достъпни за физическите лица от ЕИП. ЕКЗД оцени също така дали гаранциите, предвидени в корейската нормативна уредба, са налични и ефективни.
4. Като основен източник за справка за настоящия документ ЕКЗД използва своя Референтен документ по ОРЗД относно адекватното ниво на защита⁵ („**Референтен документ по ОРЗД относно адекватното ниво на защита**“), приет през февруари 2018 г., и Препоръки 2/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение⁶.

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

² Съобщение за пресата https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.

³ Пак там.

⁴ ЕКЗД е извършил своя анализ въз основа на официалните преводи, подготвени от корейското правителство.

⁵ РД 254, Референтен документ по ОРЗД относно адекватното ниво на защита, 6 февруари 2018 г., (одобрен от ЕКЗД, вж. <https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines>).

⁶ Вж. Препоръки 2/2020 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/preporki/recommendations-022020-european-essential-guarantees_en.

1.1. Области на сближаване

5. Ключова цел на ЕКЗД е да даде становище на Европейската комисия относно адекватността на нивото на защита, предоставяна на физическите лица, чиито лични данни се прехвърлят към Република Корея. Важно е да се вземе предвид, че ЕКЗД не очаква корейската рамка за защита на данните да възпроизвежда европейското законодателство за защита на данните.
6. ЕКЗД напомня обаче, че съгласно член 45 от ОРЗД и практиката на Съда на Европейския съюз (наричан по-нататък „Съд на ЕС“), за да бъде сметено за предоставящо адекватно ниво на защита, законодателството на третата държава трябва да е хармонизирано със същността на основните принципи, заложи в ОРЗД. В тази връзка корейската рамка за защита на данните има много сходства с европейската рамка за защита на данните, тъй като един основен законодателен акт обхваща и публичния, и частния сектор, и се допълва от специфични за сектора законодателни актове.
7. Що се отнася до съдържанието, ЕКЗД отбелязва ключови области на хармонизация между рамката на ОРЗД и корейската рамка за защита на данните във връзка с определени основни разпоредби, като понятията (напр. „лична информация“, „обработка“, „субект на данни“); основанията за законосъобразна и добросъвестна обработка за легитимни цели; ограничаването в рамките на целта; качеството и пропорционалността на данните; задържането, сигурността и поверителността на данните; прозрачността и специалните категории от данни.
8. В допълнение към горепосоченото ЕКЗД приветства положените от Европейската комисия и корейските органи усилия, за да гарантират, че Република Корея осигурява адекватно ниво на защита в съответствие с ОРЗД чрез приемане на уведомления от страна на корейския надзорен орган (приложими не само към личните данни, предавани от ЕИП на Корея) с цел запълване на пропуските между ОРЗД и корейската рамка за защита на данните. В този смисъл ЕКЗД желае да подчертае значимостта на тези уведомления за оценката на адекватното ниво на защита на Република Корея, като отбелязва например, че те осигуряват съответните изяснения относно някои важни гаранции, между другото и във връзка с обхвата на прилагане на изключенията от Закона за защита на личната информация за обработването на псевдонимизирана лична информация за научни, научноизследователски и статистически цели, последващо предаване на данни и приложимите правила за достъп до данни от публичните органи.

1.2. Предизвикателства

9. Макар че ЕКЗД определи много аспекти от корейската рамка за защита на данните като равностойни по същество на европейската рамка за защита на данните, той заключи също, че има някои аспекти, които може да е необходимо да се разгледат по-отблизо и да се изяснят. ЕКЗД по-специално счита, че следните елементи следва допълнително да се оценят, за да се гарантира, че е спазено изискването за равностойна защита, както и че те следва да се наблюдават отблизо от Европейската комисия.

1.2.1. Общи положения

10. ЕКЗД отбелязва, че Уведомление № 2021-1 *има статут на административно правило с правнообвързваща сила върху администратора на лични данни, в смисъл че всяко нарушение на Уведомлението може да се счита за нарушение на съответните разпоредби на Закона за защита на личната информация*⁷. Като се има предвид обаче, че Уведомлението не включва допълнителни правила сами по себе си, а по-скоро пояснения за начина, по който следва да се разбира прилагането на правната норма на Закона за защита на личната информация и предвид

⁷ Вж. раздел I от приложение I към проекта на решение.

цялостната му важност, по-специално, що се отнася до разпоредбите относно псевдонимизацията съгласно ЗЗЛИ, които ЕКЗД разбира, че са обект на текущи съдебни дела, ЕК се приканва да предостави допълнителна информация относно обвързващия характер, приложимостта и валидността на Уведомление № 2021-1 и би препоръчал внимателен мониторинг на спазването му на практика, особено по отношение на приложението му не само от корейския надзорен орган, но и от съдилищата, особено когато еквивалентното ниво на защита, осигурявано с корейската нормативна уредба, е въз основа на предоставените в него пояснения.

1.2.2. Общи аспекти на защитата на данните

11. Във връзка с обхвата на прилагане на решението относно адекватното ниво на защита, ЕКЗД отбелязва, че то ще обхваща пренос, регламентиран в правната рамка на ЕИП, до публични и частни „администратори на лични данни“, които попадат в обхвата на Закона за защита на личната информация. ЕКЗД разбира, че дружествата, които изпълняват ролята на обработващи лични данни по смисъла на ОРЗД, са включени в това понятие, но за да се избегнат недоразумения, той приканва Европейската комисия да поясни, че решението относно адекватното ниво на защита ще обхваща също и преноса до „обработващи лични данни“ в Корея.
12. Важен аспект, към който ЕКЗД би искал да насочи вниманието, е свързан с концепцията за псевдонимизирана информация, заложен в корейската рамка за защита на данните. Съгласно корейското право изключенията от редица от свързаните разпоредби, включително тези относно правата на отделните субекти на данни и задържането на данни се прилагат към обработването на псевдонимизирана лична информация. Според Европейската комисия това е единственият случай, когато псевдонимизирана лична информация се обработва за целите на статистиката, научните изследвания или архивирането в обществения интерес. Това твърдение обаче се подкрепя главно от Уведомление № 2021-1, съгласно което вече споменатата необходимост от допълнителна информация относно обвързващия характер, приложимостта и валидността и тяхното спазване са от особено голямо значение. В допълнение към това, ЕКЗД приканва Европейската комисия допълнително да оцени въздействието на псевдонимизацията съгласно корейското право и най-вече по какъв начин тя може да се отрази на основните права и свободите на субектите на данни, чиито лични данни се предават на Република Корея съгласно решението относно адекватното ниво на защита. По-специално, ЕКЗД приканва Европейската комисия допълнително да оцени дерогациите, съдържащи се в член 28, параграф 7 от Закона за защита на личната информация и член 40, параграф 3 от Закона за използването и защитата на кредитна информация, както и внимателно да наблюдава тяхното прилагане, и съответната съдебна практика, за да гарантира, че правата на субектите на данни не са неправомерно ограничени, при предаването и обработването на личните данни въз основа на решението относно адекватното ниво на защита.
13. Освен това ЕКЗД отбелязва, че съгласно корейското право, правото за оттегляне на съгласие съществува само при определени обстоятелства и затова приканва Европейската комисия допълнително да оцени въздействието на липсата на общо право за оттегляне на съгласие и да предостави допълнителни гаранции, за да осигури прилагането по всяко време на основно ниво на защита на данните, ако е необходимо, чрез изясняване на ролята на правото на спиране на обработването съгласно Закона за защита на личната информация.
14. Що се отнася до последващото предаване, ЕКЗД признава, че информираното съгласие на субекта на данни като цяло ще се използва като основа за пренос на данни от базиран в Корея администратор на лична информация до базиран в трета държава получател и че в Уведомление № 2021-1 е предвидено, че лицата трябва да се информират относно третата държава, на която ще се предоставят техните данни. ЕКЗД обаче приканва Европейската

комисия да гарантира, че информацията, която ще се предоставя на субекта на данни, включва също и възможните рискове при предаването, произтичащи от липсата на адекватна защита и подходящи гаранции в третата държава. Освен това ЕКЗД счита, че би било полезно, ако решението относно адекватното ниво на защита съдържа гаранции, че личните данни няма да бъдат предавани от корейски администратори на лични данни на трета държава в ситуация, в която съгласно ОРЗД не би могло да се предостави валидно съгласие, напр. поради неравнопоставеност между страните.

15. Що се отнася до назначаването на членове на южнокорейския надзорен орган, въпреки че официалната процедура би била в съответствие с ОРЗД и следователно би изпълнила критерия за равностойност с правната рамка на ЕИП, ЕКЗД би желал Европейската комисия да наблюдава всякакви развития, които може да се отразят на независимостта на членовете.
16. Що се отнася до бюджета, отново въз основа на информацията, предоставена от Европейската комисия, не е направено позоваване на спецификите на персонала, назначен в Комисията за защита на личната информация, нито на предоставените ѝ финансови ресурси. Следователно, ЕКЗД би искал в проекта на решение да бъде предоставена допълнителна информация относно тези две свързани теми.

1.2.3. Относно достъпа на публични органи до данни, предадени на Република Корея

17. ЕКЗД анализира корейската нормативна уредба също и по отношение на държавния достъп за целите на правоприлагането и националната сигурност до лични данни, предавани от ЕИП до Корея. Макар че признава обещанията и гаранциите, предвидени от корейското правителство, както са посочени в приложение II към проекта на решение, ЕКЗД определи редица аспекти, които е необходимо да се изяснят или които пораждаат безпокойства.
18. ЕКЗД отбелязва, че разпоредбите от Закона за защита на личната информация се прилагат без ограничение в сферата на правоприлагането. ЕКЗД отбелязва също, че обработването на данни в сферата на националната сигурност е предмет на по-ограничен набор от разпоредби, заложи в този закон.
19. Що се отнася до доброволното разкриване на лични данни от доставчиците на телекомуникационни услуги на националните органи за сигурност, ЕКЗД е загрижен, че връзката на раздел 3 от приложение I към проекта на решение, в което е посочено, че доставчиците по принцип трябва да уведомяват засегнатото лице, когато доброволно изпълняват изискване, с член 58, параграф 1, изр. 2 от Закона за защита на личната информация, т.е. частичното освобождаване за целите на национална сигурност, е неясна. Поради това изискванията за информация може да станат неефективни, което значително би затруднило субектите на данни в упражняването на своите права на защита на данните, особено що се отнася до средствата за съдебна защита.
20. Макар че в проекта на решение това не се споменава изрично, ЕКЗД разбира от обясненията, предоставени от Европейската комисия, че корейската нормативна уредба не позволява масовото прихващане на телекомуникационни данни. Следователно най-новата практика на Европейския съд по правата на човека („ЕСПЧ“) относно режимите на масово прихващане няма да бъде пряко приложим за оценката на равнището на защита на данни в Корея.
21. Проектът на решение не съдържа информация относно правната рамка за последващо предаване в сферата на националната сигурност. Макар ЕКЗД да разбира, че според Европейската комисия последващото предаване от съображения за национална сигурност е достатъчно регулирано с общите гаранции и принципи, произтичащи от конституционната рамка и Закона за защита на личната информация, Комитетът е загрижен дали поради тази причина може да се счита, че отговаря на изискванията за точност и яснота на правото, и

включва ефективни и приложими гаранции. Гаранциите, на които се позовава Европейската комисия, са от много общ характер и тяхното правно основание не покрива специфичните обстоятелства и условия, при които може да се извършва последващото предаване за целите на националната сигурност. В този смисъл ЕКЗД отбелязва също, че Европейската комисия не е взела предвид наличието на международни споразумения, сключени между Република Корея и трети държави или международни организации, които може да съдържат специфични разпоредби за международното предаване на лични данни от службите за правоприлагането и/или разузнаването на трети държави. ЕКЗД счита, че сключването на двустранни или многостранни споразумения с трети държави за целите на правоприлагането или сътрудничеството в областта на разузнаването вероятно ще се отрази на така оценената корейска нормативна уредба за защита на данните.

22. ЕКЗД отбелязва, че надзорът на наказателното правоприлагане, както и на националните органи за сигурност, се осигурява чрез комбинация от различни вътрешни и външни органи, по-специално Комисията за защита на личната информация, която разполага с достатъчно изпълнителни правомощия.
23. За осигуряването на ефективни средства за защита и обезщетение е необходимо субектите на данни да имат възможността да се обръщат към компетентен орган, който отговаря на изискванията на член 47 от Хартата на основните права на Европейския съюз („Хартата“), т.е. който има правомощието да определя дали се извършва обработване на данни, да проверява законността на обработването и който притежава приложими компетенции за предприемане на коригиращи мерки, в случай че обработването на данни е незаконно. Предвид това, ЕКЗД приканва Европейската комисия да изясни дали жалба, подадена до Комисията за защита на личната информация, или дадено съдебно дело е предмет на съществени и/или процедурни изисквания, като например тежест на доказване, и дали физическите лица в ЕИП биха могли да изпълнят такова предварително условие.

1.3. Заключение

24. ЕКЗД счита, че настоящото решение относно адекватното ниво на защита е от първостепенно значение също и като се има предвид, че — с изключенията, подчертани в становището — то ще обхваща предаване на данни както в публичния, така и в частния сектор.
25. ЕКЗД приветства усилията, положени от Европейската комисия и от корейските органи за постигането на хармонизация между южнокорейската и европейската нормативна уредба. Подобренията, които се планира да бъдат въведени с Уведомление № 2021-1, с цел преодоляването на някои от разликите между двете нормативни уредби, са много важни и се приемат с одобрение. ЕКЗД обаче отбелязва, че продължават да съществуват редица безпокойства, включително във връзка с Уведомление № 2021-1, в комбинация с необходимостта от допълнителни пояснения по други въпроси, и препоръчва на Европейската комисия да разреши тези проблеми, и изисква да бъдат дадени поясненията, , и да бъде осигурена допълнителна информация и обяснения по въпросите, повдигнати в настоящото становище.

2. ВЪВЕДЕНИЕ

2.1. Корейска рамка за защита на данните

26. Основният законодателен акт, който урежда защитата на данните в Република Корея, е Законът за защита на личната информация (Закон № 10465 от 29 март 2011 г., последно изменен със Закон № 16930 от 4 февруари 2020 г., „**Закон за защита на личната информация**“). Той е допълнен с Указ за прилагане (Президентски указ № 23169 от 29 септември 2011 г., последно

изменен с Президентски указ № 30892 от 4 август 2020 г., „Указ за прилагане на Закона за защита на личната информация“), който е правнообвързващ и приложим.

27. В допълнение към Закона за защита на личната информация (ЗЗЛИ) корейската рамка за защита на данните включва регулаторни „уведомления“, издадени от корейския надзорен орган — Комисията за защита на личната информация — които съдържат допълнителни правила относно тълкуването и прилагането на Закона. Неотдавна Комисията за защита на личната информация прие Уведомление № 2021-1 от 21 януари 2021 г. (с което беше изменено предходното Уведомление № 2020-10 от 1 септември 2020 г., наричано по-нататък „Уведомление № 2021-1“) относно тълкуването, прилагането и изпълнението на определени разпоредби от Закона за защита на личната информация. По-специално, това Уведомление е резултат от дискусии относно адекватността, провеждани между корейските органи и Европейската комисия. То съдържа пояснения относно прилагането на специфични разпоредби на Закона за защита на личната информация, включително относно обработването на лични данни, предадени на Корея на базата на предвиденото решение относно адекватното ниво на защита⁸, и *има статут на административно правило с правнообвързваща сила върху администратора на лични данни, в смисъл че всяко нарушение на Уведомлението може да се счита за нарушение на съответните разпоредби на Закона за защита на личната информация*⁹. В тази връзка ЕКЗД би желал да отбележи, че макар и в проекта на решение да се нарича „Допълнителни правила“, Уведомлението не включва допълнителни правила *per se*, а по-скоро обяснения, имащи за цел да се пояснят начините, по които следва да се прилага правната норма на Закона за защита на личната информация, по-специално по отношение на данните, предавани от ЕИП. На този фон ЕКЗД би препоръчал внимателно наблюдение на практическото спазване на Уведомление № 2021-1, особено по отношение на прилагането му не само от Комисията за защита на личната информация, но и от съдилищата, когато равностойното ниво на защита, осигурявано от корейската нормативна уредба, не е базирано на поясненията, предоставени в Уведомление № 2021-1.
28. В други свързани закони за защита на данните в корейската нормативна уредба са предвидени правилата за обработването на лични данни в конкретни промишлени сектори, като например:
- Законът относно използването и защитата на кредитната информация („ЗИЗКИ“), включително указа за неговото прилагане („Указ за прилагането на ЗИЗКИ“), в които са предвидени специфични правила, приложими към търговските оператори и специализираните образувания (като например агенции за кредитен рейтинг, финансови институции), когато обработват лична кредитна информация, необходима за определяне на кредитоспособността на страните по финансови или търговски сделки;
 - Законът относно насърчаване използването на информационни и комуникационни мрежи и защита на данните („Закон относно мрежите“); и
 - Законът за защита на неприкосновеността на комуникациите („ЗЗНК“)
29. В сферата на държавния достъп, освен съответните разпоредби, съдържащи се в Закона за защита на личната информация и ЗЗНК, ЕКЗД взе под внимание и някои други законодателни актове, тоест Наказателно-процесуалния закон („НПЗ“), Закона за далекосъобщенията („ЗД“), Закона относно докладването и използването на информация за конкретни финансови сделки („ЗДИИКФС“) и Закона за националната разузнавателна служба („ЗНРС“).

⁸ Вж. раздел I от приложение I към проекта на решение.

⁹ Пак там.

2.2. Обхват на оценката, извършена от КЗЛД

30. Проектът на решение на Европейската комисия е резултат от оценка на корейската рамка за защита на данните, след която бяха проведени дискусии с корейското правителство. В съответствие с член 70, параграф 1, буква т) от ОРЗД, ЕКЗД следва да представи независимо становище относно констатациите на Комисията, да установи евентуалните недостатъци на уредбата по отношение на адекватното ниво на защита и да се постарее да направи предложения, насочени към преодоляването на тези проблеми.
31. За да се избегнат повторения и с цел да се подпомогне оценката на корейската нормативна уредба, ЕКЗД избра да се фокусира върху някои специфични точки, представени в проекта на решение, и да предостави своя анализ и становище по тях, като се въздържа от това да повтаря повечето от фактическите констатации и оценки, когато ЕКЗД няма причина да допуска, че правото на Република Корея не би било равностойно по същество на правото на ЕИП. Освен това, в съответствие с практиката на Съда на ЕС, много важна част от анализа обхваща правния режим на достъп за целите на националната сигурност до личните данни, предавани на Република Корея, и практиката на нейния механизъм за национална сигурност.
32. В своята оценка ЕКЗД взе под внимание приложимата европейска рамка за защита на данните, включително членове 7, 8 и 47 от Хартата, съответно относно защита на правото на личен и семеен живот, правото на защита на личните данни и правото на ефективни средства за правна защита и на справедлив процес, както и член 8 от Европейската конвенция за правата на човека относно защитата на правото на личен и семеен живот. Освен горепосоченото, ЕКЗД взе предвид изискванията на ОРЗД и съответната съдебна практика.
33. Целта на това действие е да се предостави на Европейската комисия становище относно оценката на адекватността на нивото на защита в Република Корея. Понятието „адекватна степен на защита“, което съществуваше още в Директива 95/46, бе доразвито от Съда на ЕС. Важно е да се припомни стандартът, установен от Съда на ЕС в решението по делото Schrems I, а именно, че докато от една страна „степен на защита“ в третата държава трябва да бъде „по същество равностойна“ на гарантираната ЕС, от друга страна „средствата, до които третата страна прибегва в това отношение, за да гарантира такава степен на защита, могат да са различни от прилаганите вътре в Съюза“¹⁰. Следователно, целта не е да се повтори точка по точка европейското законодателство, а да се установят основните и съществените елементи на разглежданото законодателство. Адекватно ниво на защита може да бъде постигнато чрез съчетаване на правата на субектите на данни със задълженията на тези, които обработват личните данни или упражняват контрол върху обработването, и надзор чрез независими органи. Правилата за обработването на данни обаче са ефективни само ако могат да бъдат прилагани принудително и ако се спазват на практика. Ето защо е необходимо да се разгледа не само съдържанието на правилата, приложими към личните данни, предадени от трета държава или от международна организация, но и системата, която е въведена, за да гарантира ефективността на тези правила. Ефективните механизми за правоприлагане имат първостепенно значение за ефикасността на правилата за защита на данните¹¹.

¹⁰ C-362/14, *Maximilian Schrems срещу Data Protection Commissioner*, 6 октомври 2015 г., ECLI:EU:C:2015:650, т. 73—74.

¹¹ РД 254, стр. 2.

2.3. Общи бележки и опасения

2.3.1. Международни ангажименти, сключени от Република Корея

34. Съгласно член 45, параграф 2, буква в) от ОРЗД и Референтния документ по ОРЗД относно адекватното ниво на защита¹², при оценяването на адекватното на нивото на защита в трета държава Европейската комисия взема предвид също така международните ангажименти, поети от третата държава, или други задължения, произтичащи от участието на третата държава в многостранни или регионални системи, по-специално във връзка със защитата на личните данни, както и изпълнението на тези задължения.
35. Корея е страна по няколко международни споразумения, които гарантират правото на неприкосновеност на личния живот, като например Международния пакт за граждански и политически права (член 17), Конвенцията за правата на хората с увреждания (член 22) и Конвенцията за правата на детето (член 16). Освен това Корея, като член на ОИСР, спазва Рамката на ОИСР за неприкосновеност на личния живот, и по-специално насоките относно защитата на неприкосновеността на личния живот и трансграничните потоци от лични данни.
36. ЕКЗД отбелязва също участието на Корея като държава наблюдател в работата на Консултативния комитет на Конвенцията на Съвета на Европа 108(+), въпреки че все още не е решила дали да се присъедини.

2.3.2. Обхват на решението относно адекватното ниво на защита

37. Съгласно съображение 5 от проекта на решение Европейската комисия заключава, че Република Корея гарантира адекватно ниво на защита за личните данни, предавани от администратор или обработващ лични данни в Съюза, на администратори на лични данни (напр. физически или юридически лица, организации, публични институции), които попадат в обхвата на прилагане на Закона за защита на личните данни, с изключение на обработването на лични данни за мисионерски дейности, извършвани от религиозни организации, и за номиниране на кандидати от политически партии¹³ или обработването на лична кредитна информация съгласно ЗИЗКИ от администратори на лични данни, които са предмет на надзор от Комисията по финансовите услуги.
38. ЕКЗД отбелязва, че решението относно адекватното ниво на защита ще обхваща пренос от правната рамка на ЕИП до публични и частни „администратори на лични данни“, които попадат в обхвата на Закона за защита на личната информация. ЕКЗД разбира, че юридическите лица, които изпълняват ролята на обработващи лични данни по смисъла на ОРЗД, са обхванати и от термина „администратор на лична информация“, като се има предвид, че ЗЗЛИ ще се прилага към тях със същата сила и че са приложими специфични задължения, когато администратор на лична информация („възлагащият на външен изпълнител“) ангажира трета страна за обработването на лична информация („външният изпълнител“); за да се избегнат недоразумения обаче, ЕКЗД приканва Европейската комисия да изясни, че решението относно адекватното ниво на защита ще обхваща също преноса на данни на „обработващи лични данни“ в Корея, както и че нивото на защита на личните данни, предадени от ЕИП, няма да бъде подкопано и в тези случаи.
39. Освен това, като се има предвид, че решението относно адекватното ниво на защита обхваща също преноса на лични данни между публични органи, ЕКЗД разбира, че то ще обхваща също и

¹² РД254, стр. 2.

¹³ За повече информация вж. по-долу в раздел 3.1.2 от настоящото становище.

трансфера между надзорни органи по защита на данните и, за по-голяма яснота, приканва Европейската комисия да разгледа специално този въпрос.

40. Освен това, що се отнася до дружествата, които са изключени от обхвата на прилагане на решението относно адекватното ниво на защита, ЕКЗД би желал да подчертае, че би било от полза, ако в решението относно адекватното ниво на защита се съдържа по-ясно определение за „търговските организации“, които са предмет на надзора на Комисията за защита на личната информация (член 45, параграф 3 от ЗИЗКИ), така че базираните в ЕИП администратори и обработващи лични данни лесно да могат да оценят дали вносителят попада също в обхвата на прилагане на решението относно адекватното ниво на защита, преди да предават данните на юридически лица, за които се прилага ЗИЗКИ, или поне да бъдат осведомени за нуждата от оценка на този аспект.
41. Що се отнася до обхвата на решението относно адекватното ниво на защита, ЕКЗД разбира от допълнителните обяснения на Европейската комисия, че Звеното за финансово разузнаване на Корея („ЗФР“), създадено към Комисията по финансови услуги и осъществяващо надзор над предотвратяването на изпирането на пари и финансирането на тероризма съгласно ЗДИИКФС¹⁴, също е изключено от обхвата, тъй като то има компетентност само във връзка с финансовите институции, които сами по себе си не са обхванати от проекта на решението. От обхвата на член 1, параграф 2, буква в) от проекта на решение обаче са изключени само администраторите на лична информация, които са предмет на надзор от Комисията по финансови услуги и които обработват лична кредитна информация съгласно ЗИЗКИ. На този фон ЕКЗД приканва Европейската комисия да изясни дали ЗФР и дейности по обработване на лични данни, осъществявани от него, попадат в обхвата на проекта на решение.

3. ОБЩИ АСПЕКТИ НА ЗАЩИТАТА НА ДАННИТЕ

3.1. Принципи, отнасящи се до съдържанието

42. Глава 3 от Референтния документ по ОРЗД относно адекватното ниво на защита е посветена на принципите, отнасящи се до съдържанието. Системата на третата държава трябва да съдържа тези принципи, за да може осигуряването ниво на защита да се счита за по същество равностойно на нивото, гарантирано от законодателството на ЕС.
43. Въпреки че правото на защита на личните данни не е изрично заложено самостоятелно в корейската конституция, то се признава за основно право, произтичащо от конституционните права на човешко достойнство и стремежа към щастие (член 10), личен живот (член 17) и неприкосновеност на комуникациите (член 18). Това е потвърдено и от Върховния съд, и от Конституционния съд, както е посочено в проекта на решение на Европейската комисия¹⁵. ЕКЗД отбелязва това признание, понеже от него той стига до заключението, че защитата на данните като основно право според член 37 от корейската конституция „може да бъде ограничавана единствено от правото и когато е необходимо за националната сигурност или за спазването на закона и реда, или за общественото благо“, и че „дори когато бъдат наложени такива ограничения, те не може да засягат същността на свободата или правото“.

¹⁴ Вж. приложение II, раздел 2.2.3.1.

¹⁵ Вж. съображение 8 от проекта на решение и съответната съдебна практика, посочена в бележка под линия 10 от проекта на решение, резюмета на която са налични само на английски език.

44. Според Европейската комисия¹⁶ Конституционният съд е постановил, че чуждестранните граждани също са предмет на основни права. Съгласно официалните декларации на корейското правителство¹⁷, макар и досега в съдебната практика да не е специално разглеждано правото на неприкосновеност на личния живот на лица, които не са корейски граждани, сред учените е общоприето, че в членове 12—22 от Конституцията са предвидени „правата на хората“. Освен това, Република Корея прие редица закони в областта на защитата на данните, като например Закона за защита на личната информация, които предвиждат гаранции за всички лица, независимо от тяхната националност. В тази връзка ЕКЗД отбелязва, че член 6, параграф 2 от Конституцията предвижда, че статусът на чуждестранните граждани е гарантиран, както е предвидено в международното право и договорите, както и отбелязва съдебната практика, посочена в проекта на решение, според която „чуждестранен гражданин“ може да притежава „основни права“. Като се има предвид значението на това да се признава правото на защита на данните на „чуждестранните граждани“, ЕКЗД приканва Европейската комисия да насочи вниманието си към нуждата да се продължи наблюдението на съдебната практика, свързана със защитата на данните като основно право, признато не само на корейските граждани, но и на всички субекти на данни, за да се гарантира, че равнището на защита на физическите лица, гарантирано с ОРЗД, не е подкопано при предаване на лични данни на Корея по силата на решението относно адекватното ниво на защита.

3.1.1. Понятия

45. Съгласно Референтния документ по ОРЗД относно адекватното ниво на защита, нормативната уредба на третата държава следва да съдържа основните понятия и/или принципи, отнасящи се до защитата на данните. Въпреки че не е задължително да представляват огледален образ на терминологията в ОРЗД, те трябва да отразяват понятията, заложи в европейското законодателство за защита на данните, и да съответстват на тях. Например, ОРЗД включва следните важни понятия: „лични данни“, „обработване на лични данни“, „администратор на данни“, „обработващ лични данни“, „получател“ и „чувствителни данни“¹⁸.
46. В Закона за защита на личната информация се съдържат редица определения, като например, наред с другото, тези за „лична информация“, „обработване“ и „субект на данни“, които силно наподобяват съответните термини в ОРЗД.

3.1.1.1. Концепция относно псевдонимизирани данни

47. Наред с определенията, предоставени в Закона за защита на личната информация, в член 2, параграф 1, личната информация е определена като всяка от следната информация, свързана с живо лице: а) информация, която идентифицира дадено лице с неговото или нейното пълно име, регистрационен номер по местоживеене, изображение и др., и б) информация, която дори сама по себе си да не идентифицира дадено лице, лесно може да бъде комбинирана с друга информация, като по този начин дадено лице може да бъде идентифицирано. В последните случаи дали комбинирането би било лесно се определя чрез разумно вземане предвид на времето, разходите, технологиите и др., вложени в идентифициране на лицето, като например вероятността за получаване на другата информация.
48. Освен това, съгласно член 2, параграф 1, буква в) от Закона за защита на личната информация, „псевдонимизирана информация“ също се счита за лична информация. Псевдонимизираната информация се определя като информацията съгласно букви а) или б) по-горе, която е псевдонимизирана в съответствие с алинеи 1—2, поради което става невъзможно идентифицирането на дадено лице, без да се използва или комбинира информация с цел

¹⁶ Вж. съображение 9 от проекта на решение.

¹⁷ Вж. раздел 1.1 от приложение II към проекта на решение.

¹⁸ РД 254, стр. 4.

възстановяването ѝ в оригинален вид. Информацията, която е напълно анонимизирана, е изключена от обхвата на прилагане на Закона за защита на информацията. Според член 58, параграф 2 от ЗЗЛИ, законът не се прилага към информация, с която вече не може да бъде идентифицирано дадено лице при комбиниране с друга информация, като се вземат разумно предвид времето, разходите, технологиите и др.

49. В съображение 17 от своя проект на решение Европейската комисия заявява, че това отговаря на материалния обхват на прилагане на ОРЗД и понятията в него за „лични данни“, „псевдонимизация“ и „анонимизирана информация“.
50. Съгласно член 28, параграф 7 от Закона за защита на личната информация обаче членове 20, 21, 27, 34, параграф 1, 35—37, 39, параграфи 3, 4, 6 до 8 не се прилагат към псевдонимизираната лична информация.
51. В своя проект на решение Европейската комисия заявява, че член 28, параграф 7 от Закона за защита на личната информация е приложим единствено към псевдонимизираната лична информация, когато се обработва за целите на статистиката, научните изследвания или архивирането в обществен интерес¹⁹. Това обаче не е пряко следствие от буквата на закона, а от обясненията, предоставени в Уведомление № 2021-1²⁰. Макар ЕКЗД да признава, че може да бъде изготвен аргумент въз основа на структурата и обосновката в ЗЗЛИ, че член 28, параграф 2 от посочения закон следва да се разбира и логично да се тълкува като приложим също и към член 28, параграф 7 от него, предвид значението, което има Уведомление № 2021-1 в оценката на Европейската комисия за адекватността на нивото на защита на личните данни в Република Корея, а и за да се избегнат съмнения, ЕКЗД приканва Европейската комисия да предостави допълнителна информация относно обвързващия характер, приложимостта и валидността на Уведомление № 2021-1, както и да наблюдава неговото прилагане.
52. В този смисъл, ЕКЗД би искал да припомни, че съгласно ОРЗД псевдонимизацията се счита за препоръчителна мярка за сигурност. С други думи, съгласно ОРЗД псевдонимизираните данни продължават да бъдат лични данни, за които Регламента се прилага в пълна сила. На базата на горепосоченото ЕКЗД е загрижен, че нивото на защита на ОРЗД на псевдонимизирани данни би могло да бъде подкопано, когато личните данни се предават на Корея. Следователно, ЕКЗД приканва Европейската комисия допълнително да оцени въздействието на псевдонимизацията съгласно Закона за защита на личната информация и най-вече по какъв начин тя може да се отрази на основните права и свободите на физическите лица, чиито данни ще се предават на Република Корея въз основа на решението относно адекватното ниво на защита. ЕКЗД приканва Европейската комисия да предостави гаранции за това, че нивото на защита на личните данни на субектите на данни в ЕИП няма да бъде понижено след предаването на Република Корея дори, когато предадените лични данни са псевдонимизирани.

3.1.1.2. Концепция за администратор на лични данни

53. Член 2, параграф 5 от Закона за защита на личната информация включва определение за „администратор на лични данни“, което означава публична институция, юридическо лице, организация или физическо лице и др., което обработва лична информация с цел пряко или косвено боравене с файлове с лична информация „като част от неговите дейности“. В допълнителните гаранции, определени в уведомление № 2021-1 обаче, терминът администратор на лични данни се определя като публична институция, юридическо лице, организация, физическо лице и др., което обработва лична информация с цел пряка или косвена

¹⁹ Вж. *inter alia* съображение 82 от проекта на решение.

²⁰ Раздел 4 от приложение I към проекта на решение.

работа с файлове с лична информация „за стопански цели“. Вместо това в бележка под линия 272 от проекта на решение е посочено следното относно понятието за администратор на лична информация: „Както е определено в член 2 от Закона за защита на личната информация, т.е. публична институция, юридическо лице, организация, физическо лице и др., което обработва лична информация с цел пряко или косвено боравене с файлове с лична информация „за стопански цели“.“

54. ЕКЗД признава, че тези несъответствия може да се дължат на преводите на оригиналния текст, предоставени от корейските органи, и приканва Европейската комисия редовно да проверява качеството и истинността на преводите. Комитетът обаче подчертава факта, че за да може да се оцени равностойността по същество на нивото на защита на личните данни в корейската правна уредба, е необходимо ясно разбиране за целите на обработването, което попада в материалния обхват на ЗЗЛИ. Освен това, ЕКЗД отбелязва, че в закона не се използва същата терминология, както в ОРЗД, във връзка с понятията „администратор на лични данни“ и „обработващ лични“ и приканва Европейската комисия да изясни правилното определение и обхват на концепцията за „администратор на лична информация“, както и по-специално да прецени дали този термин обхваща също и обработващите лични данни по смисъла на ОРЗД, тъй като това пряко засяга обхвата на решението относно адекватното ниво на защита²¹

3.1.2. Частични изключения, предвидени в Закона за защита на личната информация

55. Член 58, параграф 1 от Закона за защита на личната информация изключва прилагането на части от посочения закон (т.е. членове 15 — 57) във връзка с четири категории обработване на лични данни, както е описано по-долу. По-специално, изключенията са свързани с разпоредбите от ЗЗЛИ относно специфични основания за обработване, определени задължения за защита на данните, подробните правила за упражняването на индивидуални права, както и правилата, уреждащи разрешаването на спорове. ЕКЗД обаче отбелязва, че продължават да са приложими някои общи разпоредби от Закона за защита на личната информация, като например тези, които са свързани с принципите за защита на данните (член 3 от ЗЗЛИ) и индивидуалните права (член 4 от ЗЗЛИ). Освен това в член 58, параграф 4 са предвидени специфични задължения във връзка с тези четири категории обработване на лични данни.
56. Първо, частичното изключение обхваща личната информация, събрана съгласно Закона относно статистическите данни, за целите на обработването от публичните институции. В съображение 27 от своя проект на решение Европейската комисия заявява, че съгласно получените от корейското правителство пояснения обработваните лични данни обикновено се отнасят до корейски граждани и само по изключение може да включват информация за чуждестранни граждани, а именно в случая на статистическите данни относно влизането на територията или напускането ѝ, или относно чуждестранни инвестиции. Според проекта на решение обаче дори в тези ситуации такива данни обикновено не се предават от администратори/обработващи в ЕИП, а по-скоро се събират пряко от публичните органи в Корея.
57. ЕКЗД признава обосновката на Европейската комисия относно изключителния характер на прилагането на Закона относно статистическите данни към обработването на лични данни, предавани по линия на решението относно адекватното ниво на защита; той обаче би желал да получи допълнителна информация и уверения относно специфичните гаранции, които биха се прилагали в случай на по-нататъшно събиране на лични данни, предавани от ЕИП, съгласно Закона относно статистическите данни, за да бъдат обработвани от публични институции, по-специално във връзка с упражняването на индивидуални права от субектите на данни в съответствие с член 89, параграф 2 от ОРЗД, доколкото упражняването на тези права не е

²¹ Вж. също точка 38 по-горе.

възможно да възпрепятства или спре постигането на специфичните цели, а такива дерогации не са необходими за изпълнението на тези услуги.

58. От тази гледна точка прилагането на член 4 от Закона за защита на личната информация също и към такъв вид обработване изглежда предоставя уверения, но ЕКЗД би желал да получи допълнителна информация и пояснения в решението относно адекватното ниво на защита във връзка със специфичните наложени задължения в съответствие с член 58, параграф 4 от Закона за тези дейности по обработване, а именно във връзка със свеждане на данните до минимум, ограничено задържане на данни, мерки за сигурност и разглеждането на жалби.
59. Второ, частичното изключение обхваща личната информация, събрана или изискана за анализ на информацията, свързана с националната сигурност. ЕКЗД осъзнава факта, че по въпросите, свързани с националната сигурност, държавите имат широка свобода на преценка, призната от Европейския съд по правата на човека. ЕКЗД отбелязва също, че съгласно член 37, параграф 2 от корейската конституция всяко ограничаване на свободите и правата, например когато е необходимо за защита на националната сигурност, не може да нарушава основния аспект на тази свобода или право. Освен това ЕКЗД отбелязва гаранциите в раздел 6 от Уведомление № 2021-1 във връзка с обработването на лична информация за целите на националната сигурност, включително разследването на нарушения и правоприлагането. В тази връзка обаче ЕКЗД приканва Европейската комисия допълнително да изясни обхвата на изключенията, тъй като би искал да разбере дали всички изключения, предоставени съгласно член 58, параграф 1, изр. 2 от Закона за защита на личната информация (глави III — VII), са от значение за работата на службите на разузнаването и дали те гарантират равностойност с принципите на необходимост и пропорционалност. По-специално, ЕКЗД приканва Европейската комисия да предостави повече яснота във връзка с обстоятелствата, при които службата за разузнаване би могла да се позовава на изключения. Комитетът счита за необходимо да се наблюдава отблизо практическото въздействието на тези ограничения, особено върху ефективното упражняване и прилагане на правата на субектите на данни.
60. Трето, частичното изключение се прилага за *„лична информация, обработвана временно, когато това е спешно необходимо за обществената безопасност и сигурност, общественото здраве и др.“* Според съображение 29 от проекта на решение на Европейската комисия тази категория се тълкува строго от Комисията за защита на личната информация и се прилага само в спешни ситуации, за които са необходими неотложни действия, например с цел проследяване на заразни агенти или спасяване и помощ на жертвите на природни бедствия.
61. ЕКЗД подчертава също, че всички дерогации от нивото на защита за лични данни следва да се тълкуват строго. Същевременно ЕКЗД отбелязва, че тази разпоредба не е строго определена и не предвижда изчерпателен списък с примери за ситуации, в които обработването на лични данни може да се счита за *„спешно необходимо“*. ЕКЗД например е загрижен за това дали международното предаване на здравни данни по време на текущата пандемия от COVID-19 също би попадало в обхвата на това изключение. Предвид горепосоченото ЕКЗД призовава Европейската комисия да предостави допълнителни пояснения относно обхвата на това изключение, както и да наблюдава отблизо неговото прилагане и обхват, за да гарантира, че то няма да доведе до понижаване на нивото на защита на личните данни от ЕИП след предаването на Корея въз основа на решението относно адекватното ниво на защита.
62. И накрая, частичното освобождаване се прилага към личната информация, събирана или използвана за целите на докладването от пресата, мисионерските дейности на религиозни

организации и номинирането на кандидати от политически партии²². Що се отнася до обработването на лична информация от пресата за журналистически дейности, в съображение 31 от своя проект на решение Европейската комисия заявява, че балансирането между свободата на изразяване и други права, включително правото на неприкосновеност на личната информация, е осигурено със Закона относно арбитража и средствата за правна защита, и др. за щети, нанесени чрез прессъобщения (наричан по-нататък „**Закон относно пресата**“) и предоставя специфични гаранции, които произтичат от Закона относно пресата. ЕКЗД обаче би искал да прикани Европейската комисия да наблюдава отблизо това изключение и съответната съдебна практика, за да гарантира, че в корейската нормативна уредба се гарантира и на практика равностойното ниво на защита на данните.

3.1.3. Основания за законосъобразна и добросъвестна обработка за легитимни цели

63. В Референтния документ по ОРЗД относно адекватното ниво на защита е посочено, че данните трябва да се обработват законосъобразно, добросъвестно и легитимно, както изисква ОРЗД. Правните основания, според които личните данни може да бъдат обработвани законосъобразно, добросъвестно и легитимно, следва да бъдат установени достатъчно ясно. Европейската рамка признава няколко такива легитимни основания, включително, например разпоредби в националното право, съгласието на субекта на данни, изпълнението на договор или законни интереси на администратора на данни или на трета страна, които нямат преимущество пред интересите на физическото лице.
64. Подобно на структурата на ОРЗД, в началото на Закона за защита на личната информация първо са въведени принципите на законност, справедливост и прозрачност (член 3, параграфи 1 и 2 от ЗЗЛД), като по-нататък (членове 15 — 19 от Закона) са изложени специфичните правила за неговото прилагане. По-специално, член 15 от Закона включва каталог с правни основания, въз основа на които администраторите на лична информация може да извършват събирането и използването на лична информация. Тези правни основания включват 1) информираното съгласие на субекта на данни; 2) законовото разрешение или необходимостта от спазването на правно задължение; 3) необходимост от изпълнение на задълженията на публична институция; 4) необходимост от изпълнение на договор със субект на данни; 5) необходимост от защита на живота, телесни или имуществени интереси на субекта на данни или трета страна от непосредствена опасност (и не може да бъде получено предварително съгласие); 6) необходимост от удовлетворяване на основателен интерес на администратор на лична информация, който превъзхожда този на субект на данни.
65. Освен това в член 17 от Закона за защита на личните данни са изброени правните основания, приложими за споделянето на лична информация с трета страна, които включват 1) информираното съгласие на субекта на данните; 2) законово разрешение или необходимост от спазване на правно задължение; 3) необходимост от изпълнение на задълженията на публична институция; и 4) необходимост от защита на живота, телесните или имуществените интереси на субекта на данните или на трета страна от непосредствена опасност (и не може да бъде получено предварително съгласие). Дори при липсата на съгласието на субекта на данните споделянето на лична информация се разрешава, когато това се извършва в обхвата, който в рамките на разумното е свързан с целите, за които първоначално е събрана личната информация (член 17, параграф 4 от ЗЗЛИ).

²² Съответно обработването на лична информация от страна на религиозните организации за техните мисионерски дейности и обработването на лична информация от политическите партии във връзка с номинирането на кандидати също са изключени от обхвата на решението относно адекватното ниво на защита. Вж. също точка 37 по-горе в раздел 2.3.2.

66. В член 18 от Закона за защита на личната информация са предвидени специфични правила за използването и споделянето на лична информация, когато то се извършва извън обхвата на първоначалната цел на събирането или предоставянето. Наред с другото, и тук съгласието представлява такова правило за разрешаване.
67. Макар да признава значителното сходство на корейския закон с ОРЗД по отношение на принципа на законност и наличието на общо право на прекратяване (член 37 от ЗЗЛИ), на който може да се прави позоваване също и когато данните се обработват въз основа на съгласие, ЕКЗД би желал да отбележи липсата на общо право за оттегляне на съгласие съгласно Закона за защита на личната информация²³. ЕКЗД приканва Европейската комисия допълнително да оцени въздействието на липсата на общо право за оттегляне на съгласие според корейското право, като се има предвид ролята на съгласието като правно основание във всички горепосочени сценарии и на индивидуалните права в правната система за защита на данните за целите на защитата на основните права и свободи на субектите на данни, и да предостави допълнителни уверения, че по всяко време ще е гарантирано основно ниво на защита на данните като това, което е предвидено с ОРЗД, също и като изясни ролята на правото на прекратяване на обработването на данни.

3.1.4. Принцип на ограничаване в рамките на целта

68. В Референтния документ по ОРЗД относно адекватното ниво на защита, в съответствие с ОРЗД, е предвидено, че личните данни следва да се обработват за специфична цел, а впоследствие да се използват само доколкото това не е несъвместимо с целта на обработването.
69. Съгласно член 3, параграфи 1 и 2 от Закона за защита на личната информация администраторите на лични данни определят и конкретизират целите на обработването и гарантират, че то е съвместимо с тези цели. Макар че този принцип е потвърден в други разпоредби (т.е. член 15, параграф 1, член 18, параграф 1 и член 19, параграф 1 от ЗЗЛИ), обработването за цели „в рамките на разумното“ се допуска при определени обстоятелства (вж. член 17, параграф 4 от Закона),²⁴ както и използването не по предназначение и предоставянето на лична информация (вж. членове 18 и 19 от Закона)²⁵.
70. ЕКЗД разбира, че в случай на пренос на лични данни от ЕИП до Република Корея въз основа на решение относно адекватното ниво на защита целта на събирането от страна на базираните в ЕИП администратори на лични данни представлява целта, за която данните се предават на получаващия администратор на лична информация, базиран в Корея. Промяната в предназначението от страна на базираните в Корея администратор би била допустима само ако е предвидено в член 18, параграф 2, изр. 1—3 от Закона за защита на личната информация,

²³ Въпреки че субектите на данни може да отказват съгласие при определени обстоятелства, вж. например член 18, параграф 3 от Закона за защита на личната информация. За разлика от това, правото на оттегляне на съгласието изглежда съществува само в специфични случаи; съгласно член 27, параграф 1, точка 2 от ЗЗЛИ субектите на данни имат правото да оттеглят съгласието си, когато не желаят личната им информация да бъде предавана на трета страна поради прехвърлянето на цялата стопанска дейност на администратора на лична информация или на част от него, сливане и др.; съгласно член 39, параграф 7 на Закона ползвателите може да оттеглят съгласието си за събирането, използването и предоставянето на лична информация по всяко време от доставчика на информационни и комуникационни услуги и др.; а съгласно член 37 от ЗИЗКИ индивидуален субект на кредитна информация може да оттегли съгласието, което е предоставил на доставчик/ползвател на кредитна информация.

²⁴ При което съвместимостта с предназначението трябва да се установи предварително въз основа на критериите, изложени в член 14, параграф 2 от Указа за прилагането на Закона за защита на личната информация.

²⁵ Вж. също параграф 66 по-горе.

„освен ако това няма неправомерно да накърни интереса на субекта на данни или на трета страна“²⁶ В този смисъл, ЕКЗД признава твърдението на Европейската комисия в съображение 55 от проекта на решение, че когато промените в предназначението са разрешени по закон, тези закони трябва да са съобразени с основното право на неприкосновеност на личните данни и защитата на данните. ЕКЗД обаче отбелязва, че не е предоставена специфична информация в подкрепа на това конкретно твърдение, например не е направено позоваване на член 37 от Конституцията (на Корея). Следователно, ЕКЗД приканва Европейската комисия да предостави допълнителни уверения и гаранции в проекта на решение, че всички закони, с които се разрешава промяна в целта на обработването, трябва да зачитат основните права и свободи на субектите на данни, свързани с неприкосновеност на личния живот и защита на данните.

3.1.5. Принцип на качеството и пропорционалността на данните

71. В Референтния документ по ОРЗД относно адекватното ниво на защита е посочено, че данните следва да бъдат точни и, ако е необходимо, актуални. Данните следва да бъдат подходящи, относими и да не надхвърлят необходимото във връзка с целите, за които се обработват.
72. Съгласно ЗЗЛИ администраторите трябва да гарантират, че личната информация е точна, изчерпателна и актуална, доколкото е необходимо във връзка с целите, за които се обработва личната информация (член 3, параграф 3 от ЗЗЛИ). Администраторите на лична информация трябва да събират само толкова информация, колкото е необходима за постигането на дадена цел. Те носят тежестта на доказване (член 16, параграф 1 от ЗЗЛИ).
73. В тази връзка, ЕКЗД споделя оценката на Европейската комисия по отношение на равностойността по същество на нивото на защита съгласно Закона за защита на личната информация спрямо ОРЗД.

3.1.6. Принцип на запазване на данни

74. Съгласно Референтния документ по ОРЗД относно адекватното ниво на защита като общо правило данните следва да се запазват за не по-дълъг период от необходимия за постигане на целите, за които се обработват личните данни. Съгласно член 21, параграф 1 от Закона за защита на личната информация този принцип съществува и в корейското право. Според ЗЗЛИ администраторите са задължени незабавно да унищожават личната информация, когато тя стане ненужна след изтичане на периода на запазване или след постигане на предвидената цел на обработването, освен ако не са приложими законови периоди на запазване.
75. ЕКЗД обаче изразява загриженост относно факта, че член 21, параграф 1 от ЗЗЛИ не е приложим към псевдонимизираната лична информация. ЕКЗД отбелязва факта, че според раздел 4, точка iii) от Уведомление № 2021-1, „[а]ко администратор на лична информация обработва псевдонимизирана информация с цел съставяне на статистика, научни изследвания, съхраняване на публични регистри и др. и ако псевдонимизираната информация не е била унищожена, след като бъде изпълнена специфичната цел на обработването в съответствие с член 37 от Конституцията и член 3 (Принципи на защита на личната информация) от Закона, той анонимизира информацията, за да гарантира, че тя вече не идентифицира дадено лице самостоятелно или в комбинация с друга информация, като вземе предвид в рамките на разумното времето, разходите, технологиите и др. в съответствие с член 58, параграф 2 от Закона за защита на личната информация.“ Като се има предвид и тук значението на Уведомление № 2021-1 и с оглед осигуряване на правна сигурност по отношение на равностойното ниво на защита на личната информация, предавана на Република Корея по линия на решението относно адекватното ниво на защита, ЕКЗД отново

²⁶ Член 18, параграф 2 от Закона за защита на личната информация.

призовава Европейската комисия да предостави допълнителна информация конкретно относно начина, по който Уведомление № 2021-1 става обвързващо, а неговата приложимост и валидност — гарантирана²⁷.

3.1.7. Принцип на сигурност и поверителност

76. Както е описано в Референтния документ по ОРЗД относно адекватното ниво на защита, принципът на сигурност и поверителност налага организациите, които обработват данни, да гарантират, че данните се обработват по начин, който гарантира тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки. При определянето на степента на сигурност следва да се вземат предвид достиженията на техническия прогрес и свързаните разходи.
77. Европейската комисия определи сходен принцип за сигурност на данните в член 3, параграф 4 от ЗЗЛИ, който е обяснен по-подробно в член 29 от Закона. Освен това разпоредбите за защита на данните се прилагат, когато администраторът на лична информация ангажира „външен изпълнител“. Сигурността на обработването трябва да се гарантира чрез технически и организационни мерки, които трябва да бъдат включени също и в обвързващото споразумение за обработване на данните (член 26 от ЗЗЛИ и член 28 от Указа за прилагането на ЗЗЛИ). Освен това се прилагат специфични задължения в случай на нарушение на данните, включително задължението за уведомяване на засегнатите субекти на данните и надзорния орган, когато броят засегнати физически лица надвиши приложимия праг (член 34 от ЗЗЛИ във връзка с член 39 от Президентския указ относно същия Закон), освен когато засегнатите данни са псевдонимизирана лична информация, обработвана за целите на статистиката, научните изследвания или архивирането в обществен интерес (член 28, параграф 7 от Закона). И тук ²⁸ ЕКЗД е обезпокоен от обширните изключения за псевдонимизирана информация и отново призовава Европейската комисия допълнително да оцени този аспект, за да гарантира, че в корейското право е предвидено равностойно по същество ниво на защита²⁹.
78. Независимо от това, като цяло ЕКЗД е удовлетворен от оценката и заключението на Европейската комисия относно равностойното по същество ниво на защита по отношение на принципа на сигурност и поверителност.

3.1.8. Принцип на прозрачност

79. На базата на член 5, параграф 1, буква а) от ОРЗД прогласява прозрачността за основен принцип на системата на ЕС за защита на данните. В съображение 39 от ОРЗД е описана ключовата функция на този принцип, като е посочено, че *„[з]а физическите лица следва да е прозрачно по какъв начин отнасящи се до тях лични данни се събират, използват, консултират или обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данните. (...) Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни, и за начините, по които да упражняват правата си по отношение на обработването.“*
80. Референтният документ по ОРЗД относно адекватното ниво на защита изрично определя „прозрачността“ като един от принципите по отношение на съдържанието, който следва да бъде вземан предвид при оценка на равностойността по същество на нивото на защита, осигурявано

²⁷ Вж. също по-горе параграф 51 от раздел 3.1.1.1 от настоящото становище, както и параграф 52 във връзка с общите опасения на ЕКЗД относно въздействието на псевдонимизацията съгласно корейското право.

²⁸ Както вече е предвидено в параграфи 51—52 по-горе и раздел 3.1.1.1 от настоящото Становище.

²⁹ Вж. също раздели 3.1.6 и 3.1.10 от настоящото Становище.

от трета държава. По-специално в него е посочено, че „[в]сяко физическо лице следва да бъде информирано за всички основни елементи по обработването на неговите/нейните лични данни в ясна, лесно достъпна, кратка, прозрачна и разбираема форма. Тази информация следва да включва целта на обработването, идентичността на администратора на данни, правата, които са му предоставени, и друга информация, доколкото това е необходимо, за да се гарантира добросъвестността. При определени условия може да съществуват някои изключения от това право на информиране, например за защита на разследването на престъпления, националната сигурност, независимостта на съдебната власт, съдебните производства или други важни цели от широк обществен интерес, както е предвидено в член 23 от ОРЗД.“

81. Подобно на ОРЗД, в Закона за защита на личната информация се съдържа общ принцип на прозрачност, според който администраторите на лична информация трябва да оповестяват своята политика на поверителност и други въпроси, свързани с обработването на лична информация (член 3, параграф 5 от Закона). Приложими са специфични задължения за информираност, когато администраторите желаят да получат съгласие от субектите на данни за събирането и обработването на лична информация (член 15, параграф 2 от ЗЗЛИ), за споделянето на лична информация с трета страна (член 17, параграф 2 от Закона) и за обработването не по предназначение (член 18, параграф 3 от Закона). Важно е да се отбележи, че тези задължения за предоставяне на информация се прилагат също *mutatis mutandis* и за външния изпълнител (член 26, параграф 7 от Закона).
82. ЕКЗД признава и приветства допълнителните гаранции в раздел 3, точки i) и ii) от Уведомление № 2021-1³⁰, свързани с информацията, която трябва да бъде предоставена на субектите на данни, когато данните им се предават от дружество от ЕИП, като се има предвид фактът, че съгласно член 20, параграф 1 от Закона за защита на личната информация, когато данните не са получени от физическото лице, то се информира само при поискване, докато общо право за информиране се признава единствено съгласно член 20, параграф 2 от Закона, когато определени операции по обработване надхвърлят праговете, предвидени в Указа за прилагането на ЗЗЛИ (член 15, параграф 2).
83. Като цяло ЕКЗД е удовлетворен от това, че нивото на защита съгласно корейското право във връзка с принципа на прозрачност е по същество равностойно с това, което е предвидено в ОРЗД.

3.1.9. Специални категории лични данни

84. За да се признае, че системата за защита на данните на трета държава осигурява ниво на защита на личните данни, което по същество е равностойно на това на ОРЗД, следва да съществуват специфични гаранции, когато са засегнати категориите лични данни, заложен в членове 9 и 10 от ОРЗД.
85. Съгласно ЗЗЛИ към обработването на така наречената чувствителна информация, което включва лична информация, разкриваща идеология, убеждения, членуване или оттегляне на членството в синдикат или политическа партия, политически виждания, здраве, сексуален живот и друга лична информация, която е много вероятно да застраши неприкосновеността на личния живот на субект на данни, както и във връзка с Указа за прилагането на Закона за защита на личната информация, ДНК информация, получена от генетично изследване, данни от регистри за съдимост; лична информация, получена от специфично техническо обработване на данни, свързани с физическите, физиологичните или поведенческите характеристики на дадено лице

³⁰ Приложение I към проекта на решение.

за целите на уникалното идентифициране на това лице; както и личната информация, разкриваща расов или етнически произход, се прилагат специфични разпоредби.

86. Подобно на ОРЗД корейският закон за защита на данните забранява обработването на чувствителна информация, освен ако не се прилагат специфични изключения, които включват 1) информиране на субекта на данните и получаване на специфично съгласие и 2) правни разпоредби, които разрешават обработването (член 23, параграф 2 от ЗЗЛИ).
87. Въз основа на това, ЕКЗД по принцип е съгласен със заключението на Европейската комисия относно равностойността по същество на корейския закон по отношение на обработването на специални категории лични данни. Комитетът обаче би желал да отбележи, че не му е предоставено Ръководството относно Закона за защита на личната информация, нито поясненията на Комисията за защита на личната информация във връзка с тълкуването на термина „сексуален живот“ като включващ също сексуалната ориентация или предпочитания на лицето, които не са включени в Уведомление № 2021-1. Следователно, Европейската комисия се призовава да предостави тази информация, за да може тя да бъде оценена независимо. Освен това, Европейската комисия специално се приканва да цитира документите, където може да бъде намерена информацията, на която тя се позовава по този въпрос.

3.1.10. Право на достъп, коригиране, изтриване и възражение

88. В корейската нормативна уредба правата на субектите на данни са признати в член 3, параграф 5 от Закона за защита на личната информация — според който администраторът на лична информация гарантира правата на физическите лица, изброени в член 4 и допълнително посочени в членове 35—37, 39 и 39, параграф 2 от ЗЗЛИ, а що се отнася до „личната кредитна информация“ (тоест „кредитна информация“, която представлява информация, необходима за определяне на кредитоспособността на страните по финансови или търговски трансакции — вж. съображение 3 от проекта на решение) — в членове 37, 38, 38, параграф 3 от ЗИЗКИ.
89. ЕКЗД отбелязва, че правото на достъп (и на коригиране, и на изтриване, което може да се упражнява от „субект на данни, който е осъществил достъп до своята лична информация съгласно член 35 от Закона за защита на личната информация“, може да бъде ограничено или отказано, „когато достъпът е забранен или ограничен от закони“, „когато достъпът може да нанесе вреда на живота или тялото на трета страна или неоснователно нарушение на собствеността и други интереси на друго лице“, а освен това за публичните институции, когато предоставянето на достъп „би породило сериозни затруднения“ в извършването на определени функции, допълнително описани в член 35, параграф 4 от Закона за защита на личната информация³¹. Сходни разпоредби има и в член 37 от Закона, свързан с правото на прекратяване на обработването на лична информация.
90. Съгласно член 23 от ОРЗД правото на Съюза или на държава членка може да ограничава индивидуалните права, когато такова ограничение е съобразено със същността на основните права и свободи и е необходима и пропорционална мярка в демократично общество, и предвижда такива ограничения, чрез които да осигури, наред с другото, защитата на субектите на данни или правата и свободите на другите, както и „наблюдението, проверката или регулаторната функция, свързани дори и понякога с упражняването на официални правомощия в случаите, посочени в букви а) — д) и ж) от същия член“.
91. Предвид това, ЕКЗД би искал в проекта на решение да бъдат включени общи гаранции относно необходимостта от право или правилник за ограничаване на правата на субектите на данни с

³¹ Същите условия и изключения на правата на достъп и коригиране, предвидени от Закона за защита на личната информация, се прилагат и по отношение на правото на достъп и коригиране, предвидено в ЗИЗКИ за кредитната лична информация (бележка под линия 135 от проекта на решение).

цел изпълнение на изискванията в корейската конституция във връзка с ограничаването на основно право само, когато е необходимо за целите на националната сигурност или запазването на закона и реда за гарантиране на общественото благосъстояние, както и това ограничение да не засяга същността на въпросната свобода или право (член 37, параграф 2 от корейската конституция).

92. Освен това, що се отнася до изключението, свързано с *„неоснователно нарушение на собствеността или други интереси на други лица“*, ЕКЗД признава, че това *„предполага, че следва да се постигне баланс между защитените с конституцията права и свободи на лицето от една страна и на други лица от друга“*³²; той обаче би искал да прикани Европейската комисия да наблюдава изцяло прилагането на това изключение и съответната съдебна практика, за да гарантира, че в корейската правна уредба и на практика е осигурено равностойно ниво на защита на правата на субекта на данните.
93. По същата причина ЕКЗД би искал да се извършва внимателно наблюдение на прилагането на изключението за публичните органи, по-специално що се отнася до случаите, в които би се считало, че предоставянето на достъп би създадо *„сериозни затруднения“* при изпълнението на техните задължения, предвид по-широката формулировка на израза в сравнение с този, който е използван в други разпоредби на Закона за защита на личната информация, напр. член 18, параграф 2, изр. 5³³, и следва да се тълкува строго, за да се избегнат ненужни ограничения на правата на субектите на данни.
94. Освен това ЕКЗД е загрижен от това дали изключенията, според които разпоредбите относно прозрачността при поискване (член 20 от Закона за защита на личната информация) и индивидуалните права (членове 35—37 от посочения Закон), както и сходните изключения, свързани с изискванията за доставчиците на информационни и комуникационни услуги (член 39, параграфи 2, 6—8 от ЗЗЛИ), както и тези, които се съдържат в ЗИЗКИ (вж. изключенията, предвидени в член 40, параграф 3 от ЗИЗКИ) — не се прилагат по отношение на псевдонимизираната информация, когато тя се обработва за целите на статистиката, научните изследвания или архивирането в обществен интерес (член 28, параграф 7 от ЗЗЛИ), и са в съответствие с гаранциите, предвидени в европейската правна рамка.
95. С тези разпоредби изглежда се въвежда обща дерогация за такъв вид обработване, докато в ОРЗД е предвидено, че когато личните данни (включително псевдонимизираните лични данни) се обработват за научни, исторически или статистически цели, в правото на Съюза или на държавата членка може да са предвидени дерогации от правата на субектите на данни, но само *„доколкото такива права е вероятно да направят невъзможно или сериозно да накърнят постигането на конкретните цели и тези дерогации са необходими за изпълнението на тези цели“*, като псевдонимизацията е единствената от техническите и организационните мерки, които ще се приемат, за да се гарантира зачитането на принципа на свеждане на данните до минимум (член 89, параграф 1 от ОРЗД).
96. Европейската комисия счита, че изключението, предвидено в член 28, параграф 7 от ЗЗЛИ, е основателно също и по отношение на член 28, параграф 5 от Закона, с който на администратора на лична информация изрично се забранява да обработва псевдонимизираната информация за целите на идентифицирането на определено лице и в който се прави позоваване на подхода по

³² Съображение 76 от проекта на решение.

³³ Във връзка с изключенията на ограничаването до използването не по предназначение и предоставянето на лична информация в член 18, параграф 2, изр. 5 от Закона за защита на личната информация са посочени ситуации, в които за публичните институции *„е невъзможно“* да изпълняват своите задължения.

член 11, параграф 2 от ОРЗД (във връзка със съображение 57 от ОРЗД) за обработване, за който не е необходимо идентифициране³⁴.

97. Действително съгласно член 11 от ОРЗД администраторът на данни не е задължен да *„поддържа, да се сдобие или да обработи допълнителна информация, за да идентифицира субекта на данни“* с единствената цел да спазва ОРЗД ако за предвидените цели той може да обработва лични данни, за които вече не е необходимо идентифициране на субекта на данни; в такива случаи, когато администраторът може да демонстрира, че не е в позиция да идентифицира субекта на данните, правата на субекта на данните не се прилагат. Както признава Европейската комисия³⁵, поради това съгласно ОРЗД в такива случаи се изисква *„практическа“* невъзможност за администратора на данни и в съответствие с принципа на свеждане до минимум на данните се признава, че не е необходимо обработването на допълнителните данни *„поради“* ОРЗД.
98. ЕКЗД обаче счита, че тази ситуация е различна от тази, в която администраторът на практика е в позиция да идентифицира субекта на данни, но няма право да го направи поради законова разпоредба, като например тази, която се съдържа в член 28, параграф 5 от ЗЗЛИ. В това отношение ЕКЗД приветства поясненията, предоставени от Комисията за защита на личната информация в Уведомление № 2021-1³⁶, с които се потвърждава, че член 3 от ЗЗЛИ (включително член 28, параграф 7) и изключението по член 40, параграф 3 от ЗИЗКИ се прилагат само когато псевдонимизираната информация се обработва за научни изследвания, статистика или архивиране в обществен интерес. ЕКЗД обаче — и в допълнение към вече посочените безпокойства относно действащия обвързващ характер на Уведомление № 2021-1³⁷ — все още би желал да разбере дали дерогациите, предвидени в член 28, параграф 7 от Закона за защита на личната информация и член 40, параграф 3 от ЗИЗКИ, биха могли да бъдат сметени за необходими и пропорционални в демократично общество, доколкото те ограничават правата на субекта на данни във всички случаи, в които псевдонимизираната информация се обработва за такива цели — т.е. когато администраторът на лични данни на практика е в позиция да идентифицира субекта на данните и правата на лицето няма вероятност да застрашат сериозно или да възпрепятстват постигането на конкретните цели.
99. По-специално ЕКЗД се опасява, че тези дерогации не биха били обосновани и ще е необходимо допълнително да се проучат, особено ако се прилагат от администратора на лична информация, който псевдонимизира данните *„за статистически цели, за целите на научни изследвания и за целите на архивирането в обществен интерес и др.“* в съответствие с член 28, параграф 2 от Закона за защита на личната информация *„без съгласието на субектите на данни“* (и без да се предоставя информацията, предвидена в член 20 от ЗЗЛИ)³⁸, доколкото този администратор запазва информацията, която позволява повторно идентифициране. Съгласно ОРЗД лицата следва да могат да упражняват своите права във връзка с данните, които могат да

³⁴ Трябва да се отбележи, че същата обосновка не би била приложима като такава към изключението, предвидено в член 40, параграф 3 от ЗИЗКИ за обработването на псевдонимизирана кредитна информация, тъй като в член 40, параграф 2, точка 6 е предвидено, че: *„Дружество за кредитна информация и др. не обработва псевдонимизирана информация по такъв начин, че определено лице да бъде идентифицирано за каквито и да е стопански или нелоялни цели“* и следователно да позволи повторното идентифициране за разумна цел, като например за изпълнение на искане на субект на данни.

³⁵ Вж. съображение 82 от проекта на решение.

³⁶ Вж. раздел 4 от приложение I към проекта на решение.

³⁷ Вж. раздел 3.1.1.1 по-горе.

³⁸ Вж. член 28, параграф 7 от Закона за защита на личната информация, обяснен с Уведомление № 2021-1, според което определени гаранции, съдържащи се в Закона за защита на личната информация, т.е. *„членове 20, 21, 27, 34, параграф 1, 35 — 37, член 39, параграфи 3, 4, 6 — 8“* не се прилагат към псевдонимизираната информация, обработвана за целите на съставянето на статистика, научните изследвания, съхраняването на публични регистри и др.

ги идентифицират или посочат, дори ако информацията се счита за „псевдонимизирана“, освен ако се прилага вече посоченият член 11 от ОРЗД. В това отношение ЕКЗД отбелязва, че едва след като тези данни бъдат предоставени на трета страна за същите статистически цели, за научни изследвания или за архивирание, информацията, която може да се използва за идентифициране на дадено лице, не следва да бъде включвана и следователно единствено администраторът на лична информация, на когото се представят псевдонимизираните данни съгласно член 28-2, параграф 2 от Закона за защитата на личната информация вероятно „на практика“ няма да бъде в позиция да идентифицира субекта на данните без допълнителни данни.

100. Накратко, като се има предвид, че, както признава Европейската комисия, *„вместо да разчита на псевдонимизацията като евентуална гаранция, в Закона за защита на личната информация тя е заложена като предварително условие за извършване на определени дейности по обработване за целите на статистиката научни изследвания и архивирание в обществен интерес (като например възможността за обработване на данните без съгласие или комбиниране на различни набори от данни)“*³⁹, но за такива случаи са предвидени важни ограничения за правата на субектите на данни, ЕКЗД приканва Европейската комисия да оцени допълнително съдържащите се в член 28, параграф 7 от Закона и член 40, параграф 3 от ЗИЗКИ дерогации и внимателно да наблюдава прилагането им и съответната съдебна практика⁴⁰, за да гарантира, че правата на субектите на данни няма да бъдат неправомерно ограничавани, когато прехвърлените, въз основа на решението относно адекватното ниво на защита, лични данни се обработват за тези цели, като се има предвид, че в много случаи тези права помагат и на администратора да гарантира качеството на обработваните данни.

3.1.11. Ограничения на последващи предавания на данни

101. В Референтния документ по ОРЗД относно адекватното ниво на защита е пояснено, че нивото на защита на физическите лица, чиито лични данни се предават по линия на решение относно адекватното ниво на защита, не трябва да бъде накърнено от последващото предаване и следователно всички последващи предавания *„следва да бъдат разрешени само когато следващият получател (т.е. получателят на последващото предаване на данни) също е обвързан с правила (включително договорни правила), осигуряващи подходящо ниво на защита, и при спазване на съответните указания, когато данните се обработват от името на администратора на данни“*.
102. Що се отнася до последващото предаване на външни изпълнители (т.е. „администратори на данни“), установени в други трети държави, ЕКЗД отбелязва, че в корейската нормативна уредба не съществуват специални правила, които да обхващат тези случаи, и че, както заявява Европейската комисия⁴¹, корейският администратор на лична информация трябва да гарантира спазване на разпоредбите на Закона за защита на личната информация относно възлагането на външни изпълнители (член 36 от Закона) посредством правнообвързващ инструмент, както и че той ще носи отговорността за личната информация, която е възложена на външен изпълнител (член 26 от Закона).
103. Що се отнася до последващо предаване до трети страни (т.е. други администратори на лична информация), съгласно член 17, параграф 3 от Закона за защита на личната информация, корейският администратор на лична информация трябва да уведомява субектите на данни относно възможността за даване на съгласие и да получи тяхното съгласие за задгранично

³⁹ Съображение 42 от проекта на решение.

⁴⁰ Вж. например оспорванията на конституцията от страна на Open Net (информацията на <https://opennet.or.kr/19909> е достъпна само на корейски език).

⁴¹ Съображение 87 от проекта на решение.

предаване и „не сключва договор за трансграничното предаване на лична информация в нарушение на Закона за защита на личната информация“. ЕКЗД отбелязва, че с тази последна разпоредба ще се гарантира — както счита Европейската комисия⁴² — че договорите за трансгранично предаване не биха съдържали задължения, които са в противоречие с изискванията, наложени от ЗЗЛИ върху администратора на лична информация, и следователно биха могли да бъдат сметнати за гаранция. С нея обаче не се налага задължение за въвеждане на мерки, за да се гарантира, че получателят ще осигури същото ниво на защита, което се предоставя от ЗЗЛИ. Следователно, ЕКЗД признава, че по принцип информираното съгласие на субекта на данните ще се използва като основа за предаване на данни от базиран в Корея администратор на лична информация до получател в трета държава.

104. В тази връзка допълнителните пояснения, предоставени от Комисията за защита на личната информация в Уведомление № 2021-1 относно задължението за информиране на лицата относно третата държава, на която ще бъдат предоставяни данните им⁴³, са добре дошли, тъй като това — както подчерта Европейската комисия⁴⁴ — би помогнало на субектите на данни в ЕИП да вземат напълно информирано решение за това дали да дадат съгласието си за предоставяне на данните им зад граница.
105. Както обаче е сметено в Становище № 28/2018 по проекта на решение за изпълнение на Европейската комисия относно адекватното ниво на защита на личните данни в Япония, трябва да се подчертае, че съгласно ОРЗД субектите на данни трябва да бъдат изрично информирани относно възможните рискове за такова предаване, произтичащи от липсата на адекватна защита в третата държава и липсата на подходящи гаранции преди да дадат съгласие. Това уведомяване следва например да включва информация, че е възможно в третата държава да няма надзорен орган и/или в нея да не са предвидени принципи на обработването на данни и/или права на субектите на данни⁴⁵. Според ЕКЗД предоставянето на тази информация е от изключителна важност, за да може при даването на съгласие физическото лице да даде информирано съгласие, като е изцяло запознато с тези специфични обстоятелства на предаването⁴⁶. ЕКЗД е обезпокоен от констатациите на Европейската комисия в проекта на решение относно адекватното ниво на защита във връзка с този специфичен вид предаване. Обикновено субектите на данни не познават рамката за защита на данните в трети държави. Следователно не може да бъде заключено, че физическото лице би могло да оцени риска на предаването само като знае конкретната държава по местоназначение. По-скоро, трябва да има ясна информация относно специфичните рискове от такова предаване на лични данни на държава извън територията на Република Корея, преди субектът на данните да даде съгласието си.
106. Затова ЕКЗД приканва Европейската комисия да гарантира, че информацията, която ще се предоставя на субекта на данни „относно обстоятелствата, свързани с предаването“, включва такава относно възможните рискове при предаването, произтичащи от липсата на адекватна защита и подходящи гаранции в третата държава. Това е важно за ЕКЗД, за да оцени дали изискванията относно съгласието са по същество равностойни на тези от ОРЗД.
107. Освен това, като се има предвид, че съгласието трябва да е дадено свободно, информирано, специално и недвусмислено, ЕКЗД счита, че би било полезно, ако решението относно адекватното ниво на защита съдържа гаранции, че личните данни няма да бъдат предавани от

⁴² Съображение 88 от проекта на решение.

⁴³ Пак там.

⁴⁴ Пак там.

⁴⁵ Насоки на ЕКЗД № 2/2018 г. относно дерогациите по член 49 на Регламент 2016/679, 25 май 2018 г., стр. 8.

⁴⁶ Насоки на ЕКЗД № 2/2018 г. относно дерогациите по член 49 на Регламент 2016/679, 25 май 2018 г., стр. 7.

корейски администратори на лични данни на трета държава в ситуация, в която, съгласно ОРЗД, не би могло да се предостави валидно съгласие, напр. поради неравнопоставеност между силите.

108. Във връзка със случаите, в които администратор на лична информация може да предоставя лична информация на трета страна зад граница без съгласието на субекта на данните — т.е. (1) ако личната информация се предоставя в обхвата, който в рамките на разумното е свързан с първоначалната цел на събирането съгласно член 17, параграф 4 от Закона за защита на личната информация; и (2) ако личната информация може да бъде предоставена на трета страна в изключителни случаи, посочени в член 18, параграф 2 от Закона — ЕКЗД отбелязва поясненията, предоставени от Комитета за защита на личната информация в раздел 2 от Уведомление № 2021-1 (и приветства предвиденото задължение, наложено на базирания в Корея администратор на лични данни и получателя зад граница да гарантират чрез правнообвързващ инструмент (като например договор) ниво на защита, което е равностойно на Закона за защита на личната информация, включително във връзка с правата на субекта на данните).

3.1.12. Директен маркетинг

109. Съгласно член 21, параграфи 2 и 3 от ОРЗД и Референтния документ по ОРЗД относно адекватното ниво на защита субектът на данни винаги трябва да е в позиция да възрази, без това да му коства никакви разходи, на обработването на данни за целите на профилирането и директния маркетинг.
110. Що се отнася до правото на прекратяване, предвидено в член 37 от Закона за защита на личната информация, ЕКЗД признава, че Европейската комисия счита, че това право се прилага също и когато данните се използват за целите на директния маркетинг⁴⁷. Комитетът обаче би искал в проекта на решение да се включат допълнителна информация и пояснения относно тази оценка, и по-специално относно практическото приложение на правото на прекратяване в случай на директен маркетинг (напр. препратки до съответната съдебна практика и др.). В тази връзка ЕКЗД би искал също да подчертае, че правото на искане от доставчика/ползвателя на кредитна информация да спре да се свързва с физическото лице с цел да се представя или да го убеждава да закупува стоки или услуги, е изрично предвидено в ЗИЗКИ (член 37, параграф 2).
111. Освен това, както признава Европейската комисия⁴⁸, в корейската нормативна уредба за такова обработване като цяло е необходимо специфичното (допълнително) съгласие на субекта на данните (вж. член 15, параграф 1, изр. 1, член 17, параграф 2, изр. 1 от Закона за защита на личната информация).
112. Тъй като не може да бъде изключено, че личните данни, предадени от ЕИП, може да бъдат обработени в Корея за такива цели, ЕКЗД би желал също в решението относно адекватното ниво на защита да бъдат включени пояснения относно наличието на правото за субекта на данните да оттегля съгласието си⁴⁹, както и относно правото неговите лични данни да бъдат изтрети и вече да не бъдат обработвани, когато обработването е на базата на съгласие (като например в случая на обработването, извършвано за целите на маркетинга), а физическото лице го е оттеглило.

⁴⁷ Съображение 79 от проекта на решение.

⁴⁸ Пак там.

⁴⁹ Вж. също параграф 67 по-горе: Докато възможността за оттегляне на съгласие е ясно предвидена в член 37, параграф 1 от ЗИЗКИ, това право се споменава само два пъти в Закона за защита на личната информация за специфични обстоятелства в член 27, параграф 1, точка 2 и член 39, параграф 7.

3.1.13. Автоматизирано вземане на решения и профилиране

113. Както Европейската комисия признава в своя проект на решение⁵⁰, Законът за защита на личната информация и неговият Указ за прилагане не съдържат общи разпоредби, насочени към въпроса с решенията, които засягат субекта на данните, и базирани единствено на автоматичното обработване на лични данни. И все пак в корейската правна система е предвидено такова право в ЗИЗКИ, което съдържа правила относно автоматизирани решения (член 36, параграф 2) дори ако прилагането им изглежда извън обхвата на надзора по линия на Закона за защита на личната информация (и като такова, извън обхвата на прилагане на този проект на решение — вж. раздел 2.3.2 по-горе относно обхвата на прилагане на проекта на решение).
114. Както вече е разгледано от Работната група по член 29⁵¹ в нейното становище 1/2016 относно Щита за личните данни и от ЕКЗД в предишното ѝ становище относно решението относно адекватното ниво на защита, свързано с Япония⁵², увеличаващото се значение на автоматизираното вземане на решение, профилирането и изкуствения интелект би предполагало възприемането на по-защитен подход. Противно на аргументите на Европейската комисия⁵³, според които е малко вероятно липсата на специфични правила относно автоматизираното вземане на решения в Закона за защита на личната информация да засегне нивото на защита по отношение на личните данни, събрани в Съюза (тъй като всяко решение, базирано на автоматизирано обработване, обикновено се взема от администратора на лични данни в Съюза, който има пряка връзка със засегнатия субект на данните), ЕКЗД счита, че не може да се изключи възможността базиран в Корея администратор да извършва автоматизирано вземане на решения при обработване на данни, предавани по линия на решението относно адекватното ниво на защита (например в сферата на заетостта с цел оценка на резултатите на работното място, надеждността, поведението и др.).
115. Разработването на нови технологии позволява на компаниите по-лесно да прилагат или да обмислят прилагането на автоматизирани системи за вземане на решения, които може да доведат до отслабване на позицията на лицата. Когато решенията, взети единствено от тези автоматизирани системи, окажат въздействие върху правното положение на лицата или значително ги засегнат (например чрез поставяне в черни списъци и по този начин лишаване на лицата от техните права), е от ключово значение да се предвидят достатъчно гаранции, включително правото на информираност относно специфичните причини в основата на решението и приложената логика, да се коригира неточната или непълната информация, както и да се оспори решението, когато то е взето въз основа на неточни данни⁵⁴.
116. В този смисъл ЕКЗД има опасения относно липсата на правни разпоредби, регламентиращи автоматизираното вземане на решения в ЗЗЛИ и поради това приканва Европейската комисия да вземе предвид тази загриженост и да продължи да наблюдава развитието на корейската нормативна уредба в това отношение.

⁵⁰ Вж. съображение 81 от проекта на решение.

⁵¹ Тази работна група бе създадена въз основа на член 29 от Директива 95/46/ЕО. Тя бе независим европейски консултативен орган по защитата на данните и неприкосновеността на личния живот. Задачите ѝ са описани в член 30 от Директива 95/46/ЕО и член 15 от Директива 2002/58/ЕО. Работната група по член 29 сега е преименувана на ЕКЗД.

⁵² Становище 28/2018 относно проекта на Решение за изпълнение на Европейската комисия относно адекватното ниво на защита на личните данни в Япония, приет на 5 декември 2018 г.

⁵³ Съображение 81 от проекта на решение.

⁵⁴ РД 254, стр. 7.

3.1.14. Отчетност

117. Корейската нормативна уредба съдържа няколко правила, насочени към гарантиране, че администраторите на лична информация въвеждат подходящи технически и организационни мерки за ефективно спазване на своите задължения за защита на данните и за да могат да докажат такова спазване, наред с другото, пред компетентния надзорен орган. По-специално ЕКЗД приветства наличието на правила, които предвиждат приемането на вътрешен план за управление (член 29 от Закона за защита на личната информация), задължението за извършване на така наречената оценка на въздействието върху неприкосновеността на личния живот („ОВНЛЖ“) за случаите, в които обработването представлява по-висок риск от възможни нарушения на неприкосновеността на личния живот (член 33, параграф 1 от Закона за защита на личната информация и член 35 от Указа за прилагане на Закона), както и задължението за определяне на служител по защитата на личните данни (член 3 от Закона във връзка с член 32 от Указа за прилагане на Закона).
118. ЕКЗД споделя мнението на Европейската комисия, отнасящо се до равностойната по същество защита, която те осигуряват — дори и в случаите, когато правилата изглеждат в известна степен се различават от предвидените в ОРЗД, напр. няма разпоредба, която да предвижда нуждата служителът по защитата на личните данни да бъде независим. Ясно предвидено е обаче, че той/тя трябва да докладва на ръководството на администратора на лична информация (член 31, параграф 4 от Закона за защита на личната информация) и че той/тя не трябва да е обект на неоправдани пречки като следствие от изпълнението на тези функции (член 31, параграф 5 от ЗЗЛИ) — което би предполагало наблюдение от Европейската комисия на реалното прилагане на тези разпоредби, когато извършва преглед на решението относно адекватното ниво на защита, за да оцени ефективното им прилагане.

3.2. Процедурни механизми и механизми за правоприлагане

119. Въз основа на критериите, предвидени в Референтния документ по ОРЗД относно адекватното ниво на защита, ЕКЗД анализира следните аспекти на рамката за защитата на данните в Корея, обхванати от проекта на решението: съществуването и ефективното функциониране на независим надзорен орган; съществуването на система, гарантираща добро ниво на съответствие, и на система за достъп до подходящи механизми за защита, която позволява на физическите лица от ЕС да упражняват правата си и да търсят обезщетение, без да срещат трудно преодолими бариери пред административната и правната защита.
120. В съответствие с глава VI от ОРЗД и глава 3 от Референтния документ по ОРЗД относно адекватното ниво на защита, за да гарантира равностойно на ЕИП ниво на защита трябва да съществува един или повече независими надзорни органи, които да имат задачата да наблюдават, гарантират и налагат спазването на разпоредбите относно защита на данните и неприкосновеност на личния живот в трета държава.
121. В този смисъл надзорният орган трябва да действа с пълна независимост и безпристрастност, когато изпълнява своите задължения и упражнява своите правомощия, без да иска, нито да приема указания. Освен това надзорният орган следва да има всички необходими и налични правомощия и цели, за да гарантира спазване на правата за защита на личната информация и да насърчава осведомеността. Персоналът и бюджетът на надзорния орган също трябва да се вземат предвид. Надзорният орган също следва да има възможността да образува производства по собствена инициатива.

3.2.1. Компетентен независим надзорен орган

122. В Република Корея независимият орган, отговарящ за наблюдението и прилагането на Закона за защита на личната информация, е Комисията за защита на личната информация. Тя се състои

от един председател, един заместник-председател и седем комисари. Председателят и заместник-председателят се назначават от президента по препоръка на министър-председателя. Двама от комисарите се назначават по препоръка на председателя, двама — по препоръка на представителите на политическата партия, към която принадлежи президентът, а тримата други членове — по препоръка на представители на други политически партии (член 7, параграф 2, точка 2 от Закона за защита на личната информация). Комисията за защита на личната информация се подпомага от Секретариат (член 7, параграф 13 от Закона) и може да създава подкомисии (които се състоят от трима комисари), които да разглеждат дребни нарушения и често възникващи въпроси (член 7, параграф 12 от Закона).

123. В този смисъл ЕКЗД признава, че въпреки скорошната ѝ реорганизация, при която беше съществено изменен нейният статут и правомощия, Комисията за защита на личната информация е вложила значителни усилия, за да изгради необходимата инфраструктура, така че да се подпомогне прилагането на Закона за защита на личната информация и най-новите му изменения. Сред тези усилия може да се спомене създаването на правилата на Комисията за защита на личната информация, изготвянето на ръководство за даване на насоки относно тълкуването на ЗЗЛИ и създаването на телефонна услуга за консултиране на бизнес оператори и лица относно разпоредбите, свързани със защитата на данните, както и услуга по медиация за разглеждане на жалби. По-специално задачите на Комисията за защита на личната информация включват консултиране относно законите и регламентите, свързани със защитата на данните, разработването на политики и насоки за защита на данните, разследване на нарушения на индивидуалните права, разглеждане на жалби и провеждане на медиация при спорове, осигуряване на спазване на ЗЗЛИ, гарантиране на образование и насърчаване в сферата на защитата на данните, и обмен и сътрудничество с органи за защита на данните от трети държави⁵⁵.
124. Назначаването и съставът на Комисията за защита на личната информация са предвидени в член 7, параграф 2 от Закона за защита на личната информация. Въпреки че Комисията спада към юрисдикцията на министър-председателя (а председателят и заместник-председателят се назначават от президента по препоръка на министър-председателя), според правната уредба комисарите трябва да изпълняват задълженията си независимо, съобразно правото и тяхната съвест. ЕКЗД признава институционалните и процедурните гаранции, които се съдържат в ЗЗЛИ, и по-специално в член 7, параграфи 4—7. И все пак Комитетът би желал да прикани Европейската комисия да наблюдава развитието, които може да засегнат независимостта на членовете на южнокорейския надзорен орган.
125. Освен това проектът на решение все още не включва анализ на бюджета на Комитета за защита на личната информация, включително източниците на финансиране и прозрачност на бюджета. ЕКЗД счита, че този елемент, който се споменава и в член 56, параграф 1 от ОРЗД, и в процедурните и правоприлагащите принципи и механизми за защита на данните, които се вземат предвид в Референтния документ по ОРЗД относно адекватното ниво на защита при оценяване на системата на дадена държава или международна организация, трябва внимателно да се анализира, понеже той е показател за икономическите и човешките ресурси, с които разполага надзорният орган, за да изпълнява независимо своите законови задължения и задачи за защита на данните, и поради това ЕКЗД би посъветвал Европейската комисия да обърне повече внимание на този елемент в проекта на решение.

⁵⁵ Задачите и правомощията на Комисията за защита на личната информация са предвидени главно в член 7, параграфи 8 и 9, както и в членове 61—66 от Закона за защита на личната информация.

3.2.2. Наличие на система за защита на данните, която гарантира добро равнище на съответствие

126. В сферата на правоприлагането ЕКЗД признава широката гама от изпълнителни правомощия и санкции, които притежава Комисията за защита на личната информация, както е предвидено в Закона за защита на личната информация и в ЗИЗКИ, и отбелязва поясненията, съдържащи се в Уведомление № 2021-1, според които условията, посочени в член 64, параграф 1 от ЗЗЛИ и член 45, параграф 4 от ЗИЗКИ⁵⁶, ще бъдат приложими винаги когато бъде нарушен някой от принципите, правата и задълженията, включени в правото относно защитата на личната информация. Той би искал да препоръча на Европейската комисия обаче да наблюдава отблизо прилагането на практика на правомощията на Комисията за защита на личната информация да разпорежи на нарушителя да предприеме мярка, която счита за подходяща, от тези, които са изброени в член 64, параграф 1 от ЗЗЛИ и член 45, параграф 4 от ЗИЗКИ.
127. Освен това, що се отнася до корективните мерки, предвидени в член 64, параграф 1 от Закона за защита на личната информация, в случай на неспазване на корективната мярка, Комисията за защита на личната информация има правомощията да наложи глоба в максимален размер 50 милиона южнокорейски вона (член 75, параграф 2, изр. 13 от ЗЗЛИ). Тази сума се равнява на 36 564 EUR. ЕКЗД счита и е обезпокоен, че такъв ограничен набор от имуществени санкции може да не окаже особено силен възпиращ ефект върху нарушителите, какъвто е предвиден в закона, за да се гарантира прилагането на правилата за защита на данните, понеже той не изглежда достатъчен, за да ги разубеди, особено в случая на големи организации или предприятия със значителни финансови ресурси.
128. Що се отнася до възможността Комисията за защита на личната информация да изиска ръководител на централна административна агенция да разследва администратора на лична информация или да се включи в съвместно разследване на нарушения на Закона за защита на личната информация и дори да наложи корективни мерки по отношение на администраторите в своята юрисдикция (член 63, параграфи 4—5 от ЗЗЛИ), ЕКЗД отбелязва, че въпреки че в съображение 122 от проекта на решение е предвидена информация, цялостният характер на тези други агенции и техните правни отношения с КЗЛИ остават доста неясни. Освен това в член 68, параграф 1 от ЗЗЛИ се споменават много организации, на които би било невъзможно да се делегират правомощията на Комисията за защита на личната информация. Макар и да изглежда, че тази разпоредба е прилагана само във връзка с Корейската агенция за интернет и сигурност⁵⁷, ЕКЗД би желал да бъдат включени пояснения относно естеството на възможните взаимодействия между тези организации, както и внимателно наблюдение на прилагането на тази разпоредба в бъдеще, за да се гарантира независимостта на органите, имащи задачата да прилагат правилата относно защитата на данните.
129. Що се отнася до санкциите, в корейската система изглежда са комбинирани различни видове санкции — от корективни мерки и административни глоби до наказателни санкции, които вероятно имат силен възпиращ ефект, а корейските органи представиха няколко примера за глоби, наскоро наложени от Комисията за защита на личната информация, *inter alia* една от 6,7 милиарда корейски вона, наложена през декември 2020 г. на дружество за нарушение на различни разпоредби на ЗЗЛИ, и друга глоба в размер на 103,3 милиона корейски вона на 28 април 2021 г., издадена на дружество за технологии в сферата на изкуствения интелект, за нарушаване на правилата за законност на обработването, по-специално съгласието, и обработването на псевдонимизирана информация.

⁵⁶ Т.е. „счита се, че нарушение на правото е вероятно да накърни правата и свободите на лицата във връзка с личната информация, а непредприемането на действие е вероятно да нанесе вреда, която ще бъде трудно да се отстрани“.

⁵⁷ Вж. съображение 117 от проекта на решение и член 62 от Указа за прилагане.

130. Въпреки че горепосочените суми може да имат възпиращ ефект, ЕКЗД би желал да бъде включена допълнителна информация относно метода, използван от Комисията за защита на личната информация, за изчисляване на размера на административните глоби, например във връзка с глобите, наложени поради неспазване на корективна мярка, издадена съгласно член 64, параграф 1 от ЗЗЛИ (вж. член 75, параграф 2., изр. 13 от Закона). Това е от особено голямо значение във връзка с наказателните санкции и прилагането на Закона за престъпленията (на Корея).

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

131. Що се отнася до механизмите за съдебна защита, корейската система изглежда предлага различни начини за гарантиране на адекватна защита, и по-специално прилагането на индивидуалните права с ефективни административни и съдебни средства за защита, включително за обезщетение за претърпени вреди.
132. Корейската система предлага и алтернативни механизми, които лицата могат да използват, за да получат съдебна защита, в допълнение към административните и съдебните възможности, обяснени в съображения 132 и 133 от проекта на решение, свързани съответно с Центъра за обаждания във връзка с поверителността и Комитета за медиация при спорове. Тъй като това са допълнителни начини за съдебна защита, ЕКЗД би желал да бъдат включени по-подробни обяснения за начина, по който те допълват възможностите за съдебна защита пред Комисията за защита на личната информация и съдилищата за субектите на данни, чиито лични данни се предават на Корея по линия на решението относно адекватното ниво на защита.
133. **ДОСТЪП ДО И ИЗПОЛЗВАНЕ НА ПРЕДАВАНИТЕ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ ЛИЧНИ ДАННИ ОТ ПУБЛИЧНИТЕ ОРГАНИ В ЮЖНА КОРЕЯ**
Европейската комисия е представила подробна информация в предоставения си проект на решение и приложенията по отношение на оценката на равнището на защита на данните в сферите на правоприлагането и националната сигурност. Следователно, ЕКЗД се въздържа от това да повтаря повечето от фактическите констатации и оценки в настоящото становище.
134. Европейската комисия стига до заключението, че в горепосочените области съществува ниво на защита на данните, което съответства на изискванията, определени в практиката на Съда на ЕС, и затова може да се счита за равностойно по същество на това на Европейския съюз.
135. Като обща забележка ЕКЗД би желал да подчертае, че дори и в случаите, в които изглежда или Европейската комисия твърди, че данните, предавани от ЕС на Южна Корея, е малко вероятно да бъдат засегнати от съответното корейско право, все пак е нужно да се оцени адекватното ниво на защита на данните. Тяхното значение се демонстрира и от факта, че самата Европейска комисия ги е разгледала в проекта на решение.

4.1. Обща рамка за защита на данните по отношение на достъпа на държавата

136. Що се отнася до достъпа до лични данни от публичните органи, трябва да се разгледат различни корейски закони, за да се оцени нивото на защита на данните и на правото на неприкосновеност на личния живот. Преди всичко, ЕКЗД отбелязва, че Законът за защита на личната информация, като ключов закон, е с широка приложимост. Докато обаче, ЗЗЛИ е приложим в сферата на правоприлагането, неговото прилагане към обработването на лични данни за целите на националната сигурност е ограничено. Съгласно член 58, параграф 1, изр. 2 от ЗЗЛИ, глави III—

VII не се прилагат към обработването на лични данни за целите на националната сигурност. Все пак глави I, II, IX и X продължават да са приложими в тази сфера. По този начин основните принципи на Закона за защита на личната информация, както и основните гаранции за правата на субектите на данни и разпоредбите относно надзора, правоприлагането и средствата за защита, действително се прилагат към достъпа до лични данни и използването им от националните органи за сигурност.

137. В конституцията на Южна Корея също са заложили основни принципи за защита на данните, а именно принципите за законност, необходимост и пропорционалност. Тези принципи за защита на данните също са приложими по отношение на достъпа до лични данни от страна на публичните органи на Южна Корея в областта на правоприлагането и националната сигурност⁵⁸.
138. В областта на правоприлагането полицията, прокурорите, съдилищата и други публични органи може да събират лични данни на базата на специфично законодателство, т.е. Наказателно-процесуалния закон („НПЗ“), Закона за защита на неприкосновеността на комуникациите („ЗЗНК“) Закона за далекосъобщенията („ЗД“) и Закона относно докладването и използването на информация за конкретни финансови сделки („ЗДИИФС“), който се прилага към преследване и предотвратяване на изпирането на пари, и финансирането на тероризма. Тези конкретни закони предвиждат допълнителни ограничения, гаранции и изключения.
139. В сферата на националната сигурност, на базата на Закона за националната разузнавателна служба („ЗНРС“) и последващи „законали относно националната сигурност“⁵⁹, националната разузнавателна служба („НРС“) може да събира лични данни и да прихваща комуникации. ЕКЗД разбира, че НРС трябва да спазва горепосочените правни разпоредби, както и Закона за защита на личната информация при упражняване на своите правомощия.
140. ЕКЗД приканва Комисията да изясни дали и други органи в Корея освен НРС имат отговорност за сферата на националната сигурност, понеже в приложение I, раздел 6 Европейската комисия създава впечатлението за НРС като пример за национална агенция за сигурност.

4.2. Защита и гаранции за данни, потвърждаващи за получени съобщения, по отношение на държавния достъп за целите на правоприлагането

141. Въз основа на съответния закон (ЗЗНК) правоприлагащите органи може да вземат само два вида мерки за достъп до комуникационна информация. В ЗЗНК е направено разграничение между ограничаващите комуникацията мерки, които обхващат както събирането на съдържанието в обикновената поща, така и директното прихващане на съдържанието на телекомуникациите⁶⁰, и събирането на така наречените данни, потвърждаващи за получени съобщения. Последните включват датата на съобщенията, часът на тяхното начало и край, броят на изходящите и входящите обаждания, както и номера на абоната на другата страна, честотата на използване, файлове с данни относно използването на телекомуникационни услуги и информацията относно местоположението⁶¹.
142. ЕКЗД отбелязва, че данните, потвърждаващи за получени съобщения, не се ползват със същите гаранции, както данните, събрани посредством ограничаващи комуникацията мерки, т.е. данни за съдържанието. Действително ЕКЗД забелязва, че за целите на правоприлагането събирането на съдържание се ползва с повече гаранции, отколкото събирането на данни, потвърждаващи

⁵⁸Вж. съображение 145 от проекта на решение.

⁵⁹ Националните закони за сигурност включват например Закона за защита на неприкосновеността на комуникациите, Закона за борба с тероризма за защита на гражданите и обществената сигурност или Закона за далекосъобщенията.

⁶⁰ Член 3, параграф 2, член 2, параграф 6, член 2, параграф 7 от ЗЗНК.

⁶¹ Член 2, параграф 11 от ЗЗНК.

за получени съобщения: Първо, за разлика от събирането на данни за съдържанието, събирането на данни, потвърждаващи за получени съобщения, не е ограничено до разследването на определени сериозни престъпления, а може да се извършва, когато се счита за необходимо за провеждане на „всякакво разследване или за изпълнение на всякакво наказание“ (член 13, параграф 1 от ЗЗНК). Второ, събирането на данни, потвърждаващи съдържанието, по принцип не е структурирано като последна мярка, а трябва да се използва само когато е трудно да се предотврати извършването на престъпление по друг начин, арестуване на престъпник или събиране на доказателства⁶². Данни, потвърждаващи съдържанието, могат да се събират винаги когато прокурор или служител на съдебната полиция го „сметне за необходимо“ за разследването на престъпление или изпълнението на наказание. Има обаче изключение в това отношение за проследяването на данни в реално време и данните, потвърждаващи за получено съобщение, във връзка с дадена базова станция съгласно член 13, параграф 2 от ЗЗНК. Трето, правоприлагащите агенции, които събират съдържанието на съобщението, трябва незабавно да прекратят това, когато вече не се счита за необходимо да се осъществява постоянен достъп⁶³. Що се отнася до данните, потвърждаващи за получено съобщение, това най-малкото не е изрично предвидено в ЗЗНК или в неговия Указ за прилагане.

143. ЕКЗД отбелязва, че събирането на данни, потвърждаващи за получено съобщение, може да се извършва единствено въз основа на издадена заповед от съда. Освен това съгласно ЗЗНК се изисква да се предостави подробна информация както в молбата за заповедта, така и в самата заповед⁶⁴. Това предварително разрешение от съда служи, за да се ограничи свободата на действие на правоприлагащите органи при прилагането на правото и да се провери дали във всеки случай има достатъчно основания за събиране на данни, потвърждаващи за получено съобщение. ЕКЗД признава също, че в правото на Република Корея изглежда не е предвидено общо и неизбирателно запазване на данни, потвърждаващи за получени съобщения. Поради това държавният достъп до такива данни винаги е свързан с данни, които все още са запазени за целите на фактурирането и предоставянето на самите комуникационни услуги.
144. ЕКЗД обаче подчертава, че Съдът на ЕС е поставил под въпрос факта, че данните за трафика са по-малко чувствителни от други, и по-специално от данните за съдържанието⁶⁵. Като се има предвид, че данните, потвърждаващи получаването на съобщение, в няколко отношения са с по-ниско ниво на защита, отколкото данните за съдържанието, ЕКЗД приканва Европейската комисия да проследи отблизо дали гаранциите, предоставени по линия на корейското право за такава категория лични данни, гарантират равностойно по същество ниво на защита на това, което е гарантирано в ЕС, по-специално по отношение на пропорционалността и предвидимостта на правото.

⁶² Такъв е случаят за данни относно съдържанието съгласно член 3, параграф 2 и член 5, параграф 1 от ЗЗНК.

⁶³ Член 2 от Указа за прилагане на ЗЗНК.

⁶⁴ Вж. съображение 156 от проекта на решение.

⁶⁵ Вж. Съд на ЕС, Решение по дело C-623/17, *Privacy International*, 6 октомври 2020 г., ECLI:EU:C:2020:790, т. 71: „*Произтичащата от предаването на услугите 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 счита 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 е и самото съдържание на съобщенията. Освен това тя може да породи усещане в съзнанието на съответните лица, че личният им живот е обект на постоянно наблюдение (вж. по аналогия решение 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).*“

4.3. Достъп до комуникационна информация от корейските публични органи за целите на националната сигурност

145. Що се отнася до нормативната уредба за достъпа на националните органи за сигурност до комуникационната информация, която е предадена от ЕИП до Корея, ЕКЗД определи два повода за безпокойство, като и двата са свързани с режима на достъп до комуникациите между лица, които не са корейски граждани, които попадат в определени случаи (вж. параграф 29). В тези случаи не са приложими предоставените по друга линия гаранции, както по отношение както на данните, предоставящи потвърждение за получено съобщение, така и на данните за съдържанието. С други думи в тези конкретни случаи тези данни не се ползват със същите гаранции, както съобщените данни, когато поне един корейски гражданин участва в комуникацията.

4.3.1. Липса на задължение за уведомяване на лицата относно държавния достъп до съобщения между чуждестранни граждани

146. В сценария, описан по-горе, т.е. когато никоя от страните в комуникацията не е корейски гражданин, националните органи за сигурност не са задължени да уведомяват лицата относно събирането и обработването на техните данни. ЕКЗД признава, че този въпрос засяга само някои определени случаи. Първо, както вече е отбелязано, когато в комуникацията участва поне един корейски гражданин, изискванията за уведомяване според ЗЗНК се прилагат към всички страни в комуникацията, независимо от тяхната националност⁶⁶. Второ, събирането на лични данни, произтичащи от съобщения изключително между чуждестранни граждани, е предмет на специфичен набор от случаи на използване на информация. По-специално, правото на достъп в такива случаи обхваща комуникациите на а) държави, които са враждебно настроени към Република Корея, б) чуждестранни агенции, групи или граждани, за които има подозрения, че участват в антикорейски дейности⁶⁷ или в) членове на групи, опериращи на Корейския полуостров, но на практика са извън суверенитета на Република Корея и техните групи-чадъри са базирани в чужди държави. Следователно, комуникациите между лица от ЕС, предадени от ЕИП на Корея, могат да се контролират единствено за целите на националната сигурност, ако спадат към една от горепосочените категории⁶⁸. Като допълнително ограничаващ фактор, от допълнителните обяснения на Европейската комисия ЕКЗД разбра, че приложимата нормативна рамка не предвижда прихващането на данни, прехвърляни извън Корея.
147. Следователно, негативният ефект от липсата на изискване за уведомяване може да се счита за ограничен предвид въздействието, което тази липса може да окаже на практика. ЕКЗД обаче подчертава значението на (последващото) уведомяването за извършен държавен достъп до информация, по-специално във връзка с гарантирането на ефективни средства за защита. Според Съда на ЕС уведомяването е необходимо, „за да се даде възможност на засегнатите лица да упражнят правата си съгласно членове 7 и 8 от Хартата да поискат достъп до личните си данни, които са били предмет на тези мерки, и когато е уместно, последните да бъдат поправени или заличени, както и да се възползват, в съответствие с член 47, първи параграф от Хартата, от ефективни правни средства за защита пред съд“.⁶⁹ Държавният достъп за целите на националната сигурност често включва тайни мерки за надзор, което

⁶⁶Вж. съображение 192 от проекта на решение.

⁶⁷ Вж. приложение II, бележка под линия 244, според която понятието за антикорейски действия се отнася до действия, които застрашават съществуването и безопасността на държавата, демократичния ред или оцеляването и свободата на хората.

⁶⁸Вж. съображение 187 от проекта на решение.

⁶⁹ Съд на ЕС, Решение по 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. 190.

означава, че обектите на надзора — субектите на данни — не знаят за обработването на техните данни. Следователно „по принцип няма достатъчно възможности за сезиране на съдилищата от страна на засегнатото лице, освен ако то не е уведомено за взетите мерки и по този начин може да оспори тяхната законосъобразност ретроспективно или при условията на евентуалност, освен ако лице, което подозира, че неговите съобщения се прихващат или са били прихванати, може да се обърне към съда, така че компетентността на съдилищата да не зависи от уведомяването за прихващането, при условие че е извършено прихващане на неговите съобщения“.⁷⁰ В този смисъл и във връзка с настоящия документ ЕКЗД неколкостранно е изразявал безпокойство относно ефективните средства за съдебна защита в случаите на надзор. ЕКЗД подчертава, че тайната на държавните мерки не трябва да води до това те на практика да бъдат неоспорими. На този фон дали липсата на изискване за уведомяване за проследяването на комуникациите между чуждестранните граждани оказва въздействие върху нивото на защитата на данните, оценено в проекта на решение, трябва да се прецени като част от цялостна оценка, като специално да се вземе предвид надзорът и механизмите за съдебна защита, предвидени в корейското право (вж. раздели 4.7 и 4.8).

148. Освен това ЕКЗД отбелязва, че в закона се използват доста обширни термини, като например антикорейски или антинационални дейности⁷¹, и че е достатъчно да се предвиди по какъв начин тези концепции се тълкуват в корейското право. ЕКЗД приканва Европейската комисия да наблюдава по какъв начин тези термини са разработени в Корейското право и дали прилагането им на практика е съобразено с изискванията за пропорционалност, произтичащи от правото на ЕС.

4.3.2. Липса на предварително независимо разрешение за събиране на комуникационна информация между чуждестранни граждани

149. В случаите, в които лични данни от ЕИП, произтичащи от комуникации между лица, които не са граждани на Корея (и спадащи към един от горепосочените случаи на използване), трябва да се обработват в Корея за целите на националната сигурност, събирането на такива данни не е предмет на предварително одобрение от независим орган (каквото е случаят за комуникациите, в които поне едно от засегнатите лица е корейски гражданин).⁷²
150. Особено в светлината на последните решения на Европейския съд по правата на човека („ЕСПЧ“) „Big Brother Watch и други срещу Обединеното кралство“ и „Centrum för Rättvisa срещу Швеция“ ЕКЗД счита за необходимо да се проучи дали това представлява сериозен недостатък на корейската рамка за защита на данните. В това отношение ЕКЗД припомня, че, както е подчертано в актуализираните му препоръки относно основни европейски гаранции за мерки за надзор⁷³, в член 6, параграф 3 от Договора за Европейския съюз е предвидено, че основните права, заложи в ЕКПЧ, представляват общи принципи на правото на ЕС, докато, както припомня Съдът на ЕС в своята практика, Конвенцията не представлява правен инструмент,

⁷⁰ Европейски съд по правата на човека, *Big Brother Watch и други срещу Обединеното кралство*, 25 май 2021 г., ECLI:CE:ECHR:2021:0525JUD005817013, т. 337 и Европейски съд по правата на човека, *Дело Roman Zakharov срещу Русия*, 4 декември 2015 г., ECLI:CE:ECHR:2015:1204JUD004714306, т. 234.

⁷¹ Европейската комисия обясни, че според обясненията на корейското правителство това се отнася до „дейностите, които застрашават съществуването и безопасността на държавата, демократичния ред или оцеляването и свободата на хората“, вж. също бележка под линия 319 от проекта на решение относно адекватното ниво на защита.

⁷² Вж. съображение 190 от проекта на решение.

⁷³ Вж. Препоръки 2/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение, т. 10, 11.

официално въведен в правото на ЕС, докато Европейският съюз не се е присъединил към нея⁷⁴. Така, ниво на защита на основните права, заложено в член 45 от ОРЗД трябва да се определи въз основа на разпоредбите на същия регламент, като се вземат предвид основните права, гарантирани от Хартата. Въпреки това, според член 52, параграф 3 от Хартата, съдържащите се в него права, които съответстват на правата, гарантирани от ЕКПЧ, трябва да имат същото значение и обхват, както тези, които са изложени в тази Конвенция. Следователно, практиката на Европейския съд по правата на човека относно правата, които са предвидени и в Хартата трябва да се вземе предвид като минимален праг на защита при тълкуването на съответните права в Хартата, доколкото Хартата, както е тълкувана от Съда на ЕС, не предвижда по-високо ниво на защита⁷⁵.

151. ЕКЗД отбелязва, че макар предварителното (независимо) одобрение на мерките за надзор да се счита за важна гаранция срещу произволни действия, такова одобрение не може да бъде извлечено от практиката на Съда на ЕС като абсолютно изискване за пропорционалността на тези мерки. ЕСПЧ обаче вече изрично е въвел изискването за предварително независимо издадено разрешение за масово прихващане⁷⁶. Макар че в проекта на решение не е изрично предвидено, ЕКЗД разбира, че нормативната рамка на Република Корея не предвижда масово, а само целево прихващане на телекомуникации⁷⁷. Европейската комисия потвърди това разбиране.
152. При все това горепосочените решения на ЕСПЧ в съответствие с практиката на Съда на ЕС⁷⁸ и предишната практика на ЕСПЧ⁷⁹ отново показват значението на всеобхватния надзор от независимите надзорни органи. ЕКЗД подчертава, че независимият надзор на всички етапи от процеса на осъществяване на държавен достъп за целите на правоприлагането и националната сигурност е важна гаранция срещу произволните мерки за надзор и поради това за оценката на адекватното ниво на защита на данните. Гаранцията за независимост на надзорните органи по смисъла на член 8, параграф 3 от Хартата има за цел да се гарантира ефективно и надеждно наблюдение на спазването на правилата относно защитата на лицата при обработването на лични данни. Това се прилага по-специално при обстоятелствата, при които поради естеството на тайния надзор лицето не може да поиска преразглеждане или да участва пряко в производство по преразглеждане преди изпълнението на мярката за надзор или по време на нея.
153. Липсата на предварително независимо одобрение сама по себе си не може да се счита за сериозен недостатък в корейското право при оценката на равностойното по същество ниво на

⁷⁴ Виж. Съд на ЕС, Решение по дело C-311/18, *Data Protection Commissioner срещу Facebook Ireland Ltd. и Maximilian Schrems*, 16 юли 2020 г., ECLI:EU:C:2020:559 (наричано по-нататък „Schrems II“), т. 98.

⁷⁵ Вж. Съд на ЕС, Решение по съединени дела C-511/18, C-512/18 и C-520/18, *La Quadrature du Net и други*, 6 октомври 2020 г., т. 124.

⁷⁶ Вж. ЕСПЧ, *Big Brother Watch и други срещу Обединеното кралство*, 25 май 2021 г., ECLI:CE:ECHR:2021:0525JUD005817013, т. 351: „Масовото прихващане следва да бъде предмет на независимо разрешение още от самото начало“, „масовото прихващане следва да се разрешава от независим орган; тоест орган, който е независим от изпълнителната власт“.

⁷⁷ Единствено в приложение II, раздел 3.2 се съдържа изрична декларация за целите на националната сигурност, когато е посочено, че ограниченията и мерките за защита „гарантират, че събирането и обработването на информация е ограничено до строго необходимото за постигането на легитимна цел. Това изключва масово и безразборно събиране на лична информация за целите на националната сигурност“.

⁷⁸ Вж. например Решение на Съда на ЕС по съединени дела C-203/15 и C-698/15, *Tele2 Sverige AB и други*, ECLI:EU:C:2016:970.

⁷⁹ Вж. например решение на ЕСПЧ, *Дело Roman Zakharov срещу Русия*, 4 декември 2015 г., ECLI:CE:ECHR:2015:1204JUD004714306.

защита на данните. Оценката на адекватното ниво на защита отново зависи от всички обстоятелства по делото, по-специално ефективността на последващия надзор и средства за правна защита, предвидени в нормативната рамка на Корея (вж. още раздели 4.7 и 4.8).

4.1. Доброволно разкриване на информация

154. Съгласно член 83, параграф 3 от ЗД доставчиците на телекомуникационни услуги при поискване може доброволно да предават така наречените „данни на абоната“⁸⁰ на националните органи по сигурността и правоприлагането. Макар че ЕК отбелязва, че случаите с лични данни, които са предадени от ЕИП на Корея, вероятно са редки, те все пак трябва да се анализират, за да се оцени нивото на защита на данните, както е посочено по-горе.
155. ЕКЗД разбира, че в тези случаи се прилагат гаранциите за защита на данните в ЗЗЛИ, а публичните органи, както и доставчиците на телекомуникационни услуги, трябва да спазват тези изисквания⁸¹, както и че и двете организации могат да бъдат държани под отговорност за нарушаване на правата и свободите на засегнатите субекти на данни⁸². Освен това ЕКЗД разбира, че доставчиците на телекомуникационни услуги не са задължени да спазват тези изисквания.
156. Що се отнася обаче до концепцията за достъп до данните на абоната от страна на националните органи за целите на правоприлагането, както и по-специално за целите на националната сигурност чрез „доброволно разкриване на информация“ от страна на операторите на далекосъобщения, има опасност да се увеличи рискът за правата и свободите на субектите на данни, особено що се отнася до тяхното право на информиране.
157. Съгласно член 58, параграф 1, изр. 2 от Закона за защита на личната информация, разпоредбите на глави III—VII не се прилагат за лична информация, която е изисквана във връзка с националната сигурност. В това отношение например разпоредбите на член 18 (Ограничаване до използването не по предназначение и предоставянето на лична информация) и член 20 (Уведомяване относно източниците и др. на личната информация, събрана от трети страни) от Закона за защита на личната информация не са приложими към такива искания. В случаите, когато е отправено искане от национален орган за сигурност, това поражда въпроса от една страна дали член 58, параграф 1, изр. 2 също забранява прилагането на ЗЗЛИ също и при искания, адресирани до доставчиците на телекомуникационни услуги. От друга страна възниква въпросът дали изключването на прилагането на член 20 от Закона за защита на личната информация в такива случаи се прилага и към съответната разпоредба от раздел 2 от приложение I (Уведомяване относно данните, когато личните данни не са получени от субекта на данни (член 20 от Закона)). Ако това е така и ако в член 58, параграф 1, изр. 2 също се разглеждат доставчиците на телекомуникационни услуги, би имало риск според наличната информация от липса на правно задължение за уведомяване на субектите на данни относно доброволното оповестяване.
158. Поради това ЕКЗД е загрижен относно ефективността — че изискванията за информация би могло да станат неефективни, което значително би затруднило субектите на данни в упражняването на техните права на защита на данните, особено що се отнася до средствата за съдебна защита. В тази връзка ЕКЗД приканва Европейската комисия да поясни обхвата на съответните разпоредби.

⁸⁰ Въпросните масиви от данни биха били: името, местният регистрационен номер, адресът и телефонният номер на потребителите, датите, на които потребителите се абонират или прекратяват своя абонамент, както и идентификационните кодове на потребителите (използвани за идентифициране на законния ползвател на компютърните системи или мрежите за комуникация).

⁸¹ Вж. съображения 164 и 194 от проекта на решение.

⁸² Вж. съображение 166 от проекта на решение.

4.5. По-нататъшно използване на информацията

159. Принципът на ограничаване в рамките на целта е основно правно изискване за защита на данните. Според него е необходимо личните данни да бъдат събирани само за конкретни, изрични и легитимни цели, и да не се обработват допълнително по начин, който е несъвместим с тези цели. Освен това на публичните органи е разрешено съгласно правото на ЕС да обработват лични данни с цел предотвратяване, разследване или наказателно преследване на престъпления дори и ако тези данни първоначално са получени за различна цел, ако тези органи имат правно основание да обработват такива данни съгласно съответното право и ако допълнителното обработване не е непропорционално⁸³.
160. Предвид това, ЕКЗД отбелязва, че в корейската правна уредба за защита на данните са предвидени сходни гаранции и ограничения с тези, които са предвидени в правото на ЕС във връзка с по-нататъшното използване на събраната информация за целите на правоприлагането и националната сигурност, напр. принципа на ограничаване в рамките на целта съгласно член 3, параграфи 1—2 от Закона за защита на личната информация.

4.6. Последващо предаване на данни и споделяне на разузнавателни данни

161. В член 44 от ОРЗД е предвидено, че предаването и последващото предоставяне на лични данни се извършва само ако нивото на защита, гарантирано с ОРЗД, не е подкопано. Следователно нивото на защита, осигурявано на личните данни, предавани от ЕИП на Корея, не трябва да се подкопава от по-нататъшно предаване на получатели в трета държава, т.е. по-нататъшния трансфер следва да е разрешен само когато е гарантирано постоянно ниво на защита, което е в същността си равностойно на това, което е предоставено съгласно правото на ЕС. Следователно, когато се оценява дали трета държава гарантира адекватно ниво на защита на личните данни, трябва да се вземе под внимание правната рамка на държавата за по-нататъшно предаване на данни. Това е безспорно и в съответствие с мнението както на Европейската комисия⁸⁴, така и на ЕКЗД.
162. В този смисъл ЕКЗД отбелязва, че в последните си решения „Big Brother Watch и други срещу Обединеното кралство“ и „Centrum för Rättvisa срещу Швеция“ ЕСПЧ е предоставил насоки⁸⁵ относно предпазните мерки за защита на данните, които трябва да се спазват в договарящите се държави, когато съобщават личните данни на други страни за целите на правоприлагането и националната сигурност в случаи на масово събиране: *„Преди всичко обстоятелствата, в които може да се извършва такова предаване, трябва ясно да бъдат определени в националното право. Второ, предаващата държава трябва да гарантира, че приемащата държава, докато обработва данните, разполага с гаранции, с които може да се предотвратява злоупотреба и непропорционална намеса. По-специално получаващата държава трябва да гарантира сигурното съхраняване на материала и да ограничи по-нататъшното му разкриване. [...] Трето, ще бъдат необходими засилени гаранции, когато е*

⁸³ Вж. член 4, параграф 2 от Директивата относно правоприлагането в областта на защитата на данните.

⁸⁴ Вж. съображение 84 и сл. от проекта на решение.

⁸⁵ По случай делата *Big Brother Watch u Centrum för Rättvisa*, които се отнасят до режимите на масово прихващане, бяха установени следните елементи. Изискването за предприемане на предпазни мерки при предоставяне на материалите до други страни вече е било част от критериите, разработени от ЕСПЧ в контекста на целевото прихващане, и не са допълнително конкретизирани от ЕСПЧ (вж. *Big Brother Watch u други срещу Обединеното кралство*, т. 335, 362).

ясно, че се предават материали, за които е необходима специална поверителност — като например поверителните журналистически материали.”⁸⁶

163. В прилагането на тези стандарти ЕСПЧ е установил в дело „Centrum för Rättvisa срещу Швеция“, че липсата на изрично правно изискване, заложено в режима на прихващане, за оценяване на необходимостта и пропорционалността на споделянето на разузнавателни данни във връзка с възможното му въздействие върху правото на неприкосновеност на личния живот е в нарушение на член 8 от ЕКПЧ. ЕСПЧ е отправил критика, че поради общия характер на правото прихванатите материали като цяло биха могли да бъдат изпращани в чужбина, когато се счита, че това е в национален интерес, независимо дали чуждестранният получател осигурява допустимо минимално ниво на гаранции⁸⁷.
164. Като признава, че правната уредба на Южна Корея не позволява масово прихващане, все пак предвид последиците от практиката на ЕСПЧ, описана по-горе, ЕКЗД счита, че в допълнение към изискванията, произтичащи от правото на ЕС, както е изтълкувано от Съда на ЕС, следва да се вземе предвид линията на аргументиране на ЕСПЧ, за да се оцени дали правната рамка за по-нататъшно предаване на трета държава предвижда адекватни стандарти за защита на данните.

4.6.1. Приложима правна уредба за по-нататъшно предаване на данни от правоприлагащите органи

165. Що се отнася до по-нататъшното предаване от компетентните органи за целите на правоприлагането, ЕКЗД разбира от обясненията на Европейската комисия, че е приложим раздел 2 от приложение I към проекта на решение по отношение на ограничаването на по-нататъшното предаване, включително когато предаването се извършва въз основа на правен акт, различен от Закона за защита на личната информация. Според това правило, „ако лична информация се предоставя на трета страна зад граница, тя може да не получава нивото на защита, предоставено от Закона за защита на личната информация на Корея поради разлики в системите за защита на личната информация на различните държави. Съответно такива случаи ще се считат за „случаи, в които е възможно субектът на данните да изпадне в неблагоприятно положение“, както е посочено в член 17, параграф 4 от Закона, или „случаите, в които е несправедливо накърнен интересът на субекта на данни или трета страна“, както е посочено в член 18, параграф 2 от Закона и член 14, параграф 2 от Указа за прилагане на същия Закон. За да изпълни изискванията на тези разпоредби, администраторът на лична информация и третата страна трябва изрично да гарантират ниво на защита, което е равностойно на Закона, включително гаранцията, че субектът на данните ще упражнява своите права в правнообвързващи документи, като например договори, дори след като личната информация е предадена зад граница“⁸⁸.
166. ЕКЗД приветства тази разпоредба, въз основа на която се преценява адекватното ниво на защита в Корея и се гарантира непрекъснатост на нивото на защита, което по същество се предоставя съгласно правото на ЕС за по-нататъшното предаване. Комисията потвърди, че е правилно разбирането на ЕКЗД, а именно, че този раздел от приложение I се прилага към всички по-нататъшни предавания от компетентните органи за целите на правоприлагането. ЕКЗД обаче отбелязва, че трябва да се гарантира, че в тази разпоредба е практически предвидено постоянно ниво на защита, тъй като е възможно да има неяснота по отношение на това кои договорни

⁸⁶ ЕСПЧ, *Big Brother Watch и други срещу Обединеното кралство*, 25 май 2021 г., ECLI:CE:ECHR:2021:0525JUD005817013, т. 362.

⁸⁷ Вж. ЕСПЧ, *Centrum för Rättvisa срещу Швеция*, 25 май 2021 г., ECLI:CE:ECHR:2021:0525JUD003525208, т. 326.

⁸⁸ Проект на решение, приложение I, стр. 7.

гаранции и задължения или други сходни механизми могат да се използват за постигане на такова ниво на защита в случай на обработване за целите на правоприлагането. В това отношение следва допълнително да се посочи например, че личните данни може да бъдат споделяни само със съответните компетентни органи в третата държава.

167. Предмет на изисканото по-горе пояснение относно това дали ЗФР е обхванато от проекта на решение, ЕКЗД отбелязва, че официалното представителство относно държавния достъп⁸⁹ обяснява, че според член 8, параграф 1 от ЗДИИКФ комисарят на ЗФР може да предоставя на чуждестранно финансово разузнаване специфична информация за финансови трансакции, ако бъде сметнено за необходимо за постигането на целта на ЗДИИКФ⁹⁰ В самия член 8 от ЗДИИКФ не е предвидено задължение за определяне дали и гарантиране, че чуждата държава предоставя адекватни гаранции за защита на данните. В тази връзка в приложение II не е направена препратка към новия раздел на приложение I. Следователно, ЕКЗД призовава Европейската комисия да изясни взаимовръзката на съответния раздел на приложение I относно ограничаването на по-нататъшното предаване и правната основание за по-нататъшно предаване съгласно ЗДИИКФ.

4.6.2. Приложима правна уредба за по-нататъшно предаване на данни за целите на правоприлагането

168. Проектът на решение не съдържа информация относно правната рамка за последващо предаване в сферата на националната сигурност. За тази цел ЕКЗД разбира, че за разлика от целите на правоприлагането, раздел 2 от приложение I не е приложим към по-нататъшното предаване за целите на националната сигурност. Членове 17 и 18 от Закона за защита на личната информация, които са предмет на въпросния раздел от приложение I, са част от глава III от ЗЗЛИ, която на свой ред не е приложима към обработването на лични данни за целите на националната сигурност (член 58, параграф 1 от ЗЗЛИ).
169. ЕКЗД обаче допуска, че на Корея може да се налага да предава лични данни на чуждестранни разузнавателни служби за целите на националната сигурност и че действително го прави, напр. с цел сътрудничество в борбата срещу трансграничните заплахи за националната сигурност, за предупреждаване на чуждестранните правителства относно такива заплахи или за получаване на тяхната помощ в откриването на тези заплахи.
170. ЕКЗД разбира, че по мнение на Европейската комисия по-нататъшното предаване е достатъчно регулирано в корейското право посредством гаранции, които произтичат от всеобхватната конституционна рамка, по-специално принципите на необходимост и пропорционалност, както посредством основните принципи за защита на данните, регулирани в Закона за защита на личната информация, като например законност и справедливост на обработването, ограничаване в рамките на целта, свеждане до минимум на данните, сигурност и общи задължения за предотвратяване на злоупотреба и неправилно използване на личната информация.
171. ЕКЗД признава общата приложимост на тези ключови принципи (за защита на данните), но изразява безпокойства, че тези гаранции са от много общ характер и не се отнасят специално

⁸⁹ Вж. проект на решение, приложение II.

⁹⁰ Вж. проект на решение, приложение II, раздел 2.2.3.2. Докато такъв обмен може да се извършва единствено при условието, че чуждестранната служба не може да използва информация за друга цел, освен за оригиналната цел на оповестяването, и по-специално не и за наказателно разследване или съдебен процес (член 8, параграф 2 от ЗДИИКФ), комисарят на ЗФР може, когато получи искане от чужда държава, да даде съгласие за използването на такива данни за наказателни разследвания или съдебни процеси, свързани с престъпления, с предварителното съгласие на Министъра на правосъдието (член 8, параграф 3 от ЗДИИКФ).

до, нито включват в правното основание специфичните обстоятелства и условия за по-нататъшно предаване на данни, получени от ЕИП за целите на националната сигурност. Макар че тези общи и първостепенни принципи са широкоприложими, ЕКЗД повдига въпроса дали би могло да се счита, че те отговарят на критериите за ясни и точни правила, както и че в достатъчна степен включват ефективни и приложими гаранции. Особено когато държавният достъп и обработването на лични данни се упражнява тайно, а предположенията, които могат да бъдат направени въз основа на данните, са особено сериозни, е от съществено значение да има налице ясни и подробни правила. В закона следва да бъде посочен обхватът на всяка свобода на преценка, предоставена на компетентните органи, и начинът, по който тя се упражнява, с достатъчно яснота, за да се осигури на лицето адекватна защита. В решение по дело *Schrems II* Съдът на ЕС припомня, че правното основание, което позволява намеса в основните права, за да отговаря на изискванията за принципите на необходимост и пропорционалност, трябва само по себе си да определя обхвата на ограничението на упражняването на въпросното право и да съдържа ясни и точни правила, които уреждат обхвата и прилагането на въпросната мярка, и налагат минимални гаранции⁹¹. Затова ЕКЗД е обезпокоен, че не е достатъчно такива гаранции като цяло да са заложили в норми от по-висок ранг, без съответното правно основание специално да включва понятието напр. за пропорционалност.

172. Тези опасения са подкрепени с горепосоченото решение на ЕСПЧ, в което съдът е установил, че общо правило, което не съдържа изрично изискване за оценка на необходимостта и пропорционалността или в което не са взети предвид съображенията за неприкосновеност на личния живот, не е съвместимо с правото на неприкосновеност на личния живот съгласно член 8 от ЕКПЧ. В тази връзка ЕКЗД отбелязва, че в правото, свързано с разглежданото обработване (както и в правото на Корея) действително съществуват първостепенни (конституционно гарантирани) принципи на необходимост и пропорционалност, напр. съгласно Хартата и чрез присъединяването към ЕКПЧ.
173. ЕКЗД приканва Европейската комисия да поясни правното основание, по какъв начин и в каква степен, и при какви специфични условия агенциите на разузнавателните служби са задължени да вземат предвид съображенията за неприкосновеност на личния живот и гаранциите за защита на данните, преди да разкриват на чуждестранни партньори лични данни за целите на националната сигурност. В случай че такова задължение произлиза пряко от конституционните принципи, Европейската комисия следва допълнително да оцени изискванията за точност и яснота на съответното право и да потвърди, че общите конституционни принципи и принципи за защита на данните са правилно прилагани и упражнявани.

4.6.3. Международни споразумения

174. ЕКЗД отбелязва, че Европейската комисия не е взела предвид като част от своята оценка на адекватността наличието на международни споразумения, сключени между Корея и трети държави или международни организации, които може да съдържат специфични разпоредби за международното предаване на лични данни от службите по правоприлагането и/или за разузнаване на трети държави. ЕКЗД счита, че сключването на двустранни или многостранни споразумения с трети държави за целите на правоприлагането или сътрудничеството в областта на разузнаването вероятно ще се отрази на така оценената правна рамка на Корея за защита на данните.
175. Следователно, ЕКЗД приканва Европейската комисия да поясни дали съществуват такива споразумения, при какви условия могат да бъдат сключвани и да оцени дали разпоредбите на международните споразумения може да засегнат нивото на защита, осигурено за личните данни, предавани от ЕИП на Корея със законодателната рамка и практиките във връзка с

⁹¹ Вж. решение по дело *Schrems II*, т. 175 и 180.

оповестяването зад граница на информация за целите на правоприлагането и националната сигурност.

4.7. Надзор

176. ЕКЗД отбелязва, че надзорът на наказателното правоприлагане, както и националните органи за сигурност се осигурява чрез комбинация от различни вътрешни и външни органи.
177. В този смисъл трябва да се отбележи, че Съдът на ЕС неколккратно е подчертавал нуждата от независим надзор като основен компонент за защитата на физическите лица във връзка с обработването на личните им данни. Концепцията за независимост обхваща областите на институционална автономност, необвързаност от указания и материална независимост. За да се гарантира последователно наблюдение и прилагане на правото в областта на защитата на данните, надзорните органи трябва да притежават ефективни правомощия, включително корективни правомощия и компетенции за предприемане на коригиращи мерки.
178. ЕКЗД е съгласен със заключението на Европейската комисия, че като цялостна оценка може да се счита, че Корея има независима и ефективна система за надзор, въпреки че няколко органа от системата за надзор сами по себе си не отговарят на горепосочените изисквания. Повечето от тях например нямат изпълнителни правомощия, а са ограничени само до препоръки, напр. Националната комисия по правата на човека или Комисията за одити и проверки. Освен това повечето от съответните публични органи не са изключително институции за защита на данните, а обикновено изпълняват други задачи в сферата на защитата на основните права.
179. Според обясненията на Европейската комисия обаче ЕКЗД отбелязва, че надзорът над правоприлагащите органи е всеобхватно и без изключение гарантиран от Комисията за защита на личната информация. Следователно, КЗЛИ притежава правомощия за разследване, за предприемане на коригиращи мерки и изпълнителни правомощия съгласно ЗЗЛИ и други закони за защита на данните (напр. ЗЗНК), които се прилагат към цялата област на достъпа до лични данни от органите за правоприлагане и национална сигурност.
180. В този смисъл, ЕКЗД би искал още веднъж да подчертае, че за да упражняват своите задачи и правомощия, надзорните органи трябва да разполагат с достатъчно човешки, технически и финансови ресурси. В тази връзка за жалост няма достатъчно информация относно определените надзорни органи, по-специално Комисията за защита на личната информация. Следователно, ЕКЗД повтаря своето искане към Европейската комисия да предостави допълнителна информация по въпроса.
181. Като цяло ЕКЗД би желал да отбележи, че проектът на решение не съдържа почти никакви твърдения, примери или цифри относно надзорните дейности, както и законното прилагане на Закона за защита на данните от надзорните органи в сферата на правоприлагането и националната сигурност. Те биха били от полза при оценяването на ефективността на надзорните органи.

4.8. Средства за правна и съдебна защита

182. ЕКЗД припомня, че е от съществено значение за адекватното ниво на защита на данните физическите лица да разполагат с всеобхватни средства за правна и съдебна защита срещу неразрешен достъп до или обработване на данни. Тези средства за правна защита трябва да са достатъчни, за да позволят на субекта на данни да получи достъп до неговите или нейните съхранявани данни и да изисква тяхното коригиране или изтриване.
183. Предвид решенията по дела *Schrems I* и *Schrems II* от Съда на ЕС е ясно, че в допълнение към правото на лицата да се обръщат към компетентните органи, ефективната съдебна защита по

смисъла на член 47, параграф 1 от Хартата е от основно значение, за да се приеме за адекватно правото на трета държава.

184. ЕКЗД признава, че Корея е въвела различни начини за упражняване на правата на лицата на достъп, запазване, изтриване и преустановяване на обработването съгласно Закона за защита на личната информация. Тези права могат да се упражняват спрямо самия администратор на лични данни или посредством жалба, внесена до Комисията за защита на личната информация или други надзорни органи, напр. Националната комисия по правата на човека. Освен това, ЕКЗД признава възможността за оспорване на решението на администраторите или публичните органи, взето въз основа на тяхно искане съгласно Закона за административното производство.
185. Освен това ЕКЗД разбира от обясненията, дадени от Европейската комисия, че лицата може да оспорват действията на органите на правоприлагането и националните органи за сигурност пред компетентните органи съгласно Закона за административното производство или Закона за конституционния съд и имат възможността да получават компенсация за щети по линия на Закона за държавната компенсация⁹².
186. В този смисъл обаче ЕКЗД е загрижен относно ефективните средства за защита за лицата от ЕС в дела, свързани с националната сигурност, в които не участва корейски гражданин. Както е посочено в параграф 33 и сл., националните органи за сигурност нямат задължението да уведомяват субектите на данни относно събирането и обработването на личните им данни. Тъй като в такива случаи получаването на ефективна правна защита е значително по-трудно, ЕКЗД би искал да отбележи, че тук са необходими определени правни гаранции, ако става дума за данни, предадени от ЕИП. Тези гаранции трябва да позволяват на субектите на данни да предприемат ефективни действия срещу незаконното обработване на данни по законоустановен начин, без да бъдат възпрепятствани от изключително тесни процедурни изисквания, напр. чрез налагане на тежест на доказване, която те не могат да поемат, без да имат информация за обработването. Освен това физическите лица трябва да имат възможността да се обръщат към компетентен орган, който отговаря на изискванията на член 47 от Хартата на основните права, т.е. който има компетентността да определя дали се извършва обработване на данни, да проверява законността на обработването и да притежава правомощия за предприемане на коригиращи мерки, в случай че обработването на данни е незаконно. На този фон само правото за подаване на жалба до Националната комисия по правата на човека например не би било достатъчно. Следователно, ЕКЗД призовава Комисията да обясни по-подробно по какъв начин тези изисквания се прилагат в процесуален план и по същество, напр. дали е възможно субектите на данни да се обръщат към Комисията за защита на личната информация, както и към съд, без да е необходимо да доказват въпросното обработване на данни.
187. Освен това ЕКЗД отбелязва, че в проекта на решение е предвиден механизъм за препращане на жалби, т.е. че лица от ЕС може да подават жалба до Комисията за защита на личната информация чрез своя национален орган за защита на данните или чрез ЕКЗД. След това Комисията за защита на личната информация уведомява лицето по същия канал, след като разследването приключи⁹³. ЕКЗД приветства усилията за улесняване на достъпа до средства за защита срещу корейските национални органи за сигурност. Същевременно ЕКЗД насърчава такъв механизъм за препращане да бъде създаден чрез европейските национални органи за защита на данните, вместо чрез ЕКЗД, понеже те са компетентни и по-опитни в разглеждането на индивидуалните жалби.

⁹² Вж. приложение II, точка 3.2.4 във връзка с 2.4.3.

⁹³ Вж. съображение 205 и приложение I, т. 19 към проекта на решение.

188. Освен това ЕКЗД отбелязва възможно противоречие във връзка с доброволно разкриване на информация. От една страна проектът на решение гласи, че лицата могат да получат средства за защита, в случай че данните им бъдат разкрити незаконно след искане за доброволно разкриване, включително срещу правоприлагащия орган, издал искането⁹⁴. От друга страна в проекта на решение се споменава изискването относно преценката на прякото въздействие върху правото на лицето да оспорва действията на публичните органи, като се посочват (единствено) обвързващи искания за разкриване като пример за случай, в който се счита, че административните действия оказват пряко въздействие върху правото на неприкосновеност на личната информация⁹⁵. От обясненията на Европейската комисия ЕКЗД разбира, че в действителност няма ограничение на възможностите за защита срещу искания за доброволно разкриване на информация и затова приканва Европейската комисия допълнително да изясни това в решението както в сферата на правоприлагането, така и по отношение на националната сигурност (за разлика от раздела относно правоприлагането, разделът относно доброволното разкриване на информация за целите на националната сигурност не съдържа изрично изявление относно средствата за защита в този контекст).

⁹⁴ Вж. съображение 166 от проекта на решение.

⁹⁵ Вж. съображение 181 (правоприлагане) и съображения 208 и 181 (национална сигурност) на проекта на решение.