II

(Незаконодателни актове)

РЕШЕНИЯ

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2022/254 НА КОМИСИЯТА

от 17 декември 2021 година

съгласно Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета относно адекватното ниво на защита на личните данни от страна на Република Корея по Закона за защита на личните данни

(нотифицирано под номер C(2021) 9316)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) ([1]), и по-специално член 45, параграф 3 от него,

като има предвид, че:

1. ВЪВЕДЕНИЕ

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

(2) Съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 Комисията може да реши посредством акт за изпълнение, че дадена трета държава, територия или един или повече конкретни сектори в дадена трета държава, или дадена международна организация осигуряват адекватно ниво на защита. При това условие предаването на лични данни на трета държава може да се извършва, без да е необходимо допълнително разрешение, както е предвидено в член 45, параграф 1 и в съображение 103 от Регламент (ЕС) 2016/679.

(3) Както е посочено в член 45, параграф 2 от Регламент (ЕС) 2016/679, приемането на решение относно адекватността на защита трябва да се основава на цялостен анализ на правния ред на третата държава, който обхваща както правилата, приложими към вносителите на данни, така и ограниченията и гаранциите по отношение на достъпа до лични данни от страна на публичните органи. В своята оценка Комисията трябва да определи дали въпросната трета държава гарантира ниво на защита, равностойно „по същество“ на осигуреното в рамките на Европейския съюз (съображение 104 от Регламент (ЕС) 2016/679). Стандартът, спрямо който се оценява равностойността по същество, е определеният от законодателството на ЕС, по-специално от Регламент (ЕС) 2016/679, както и от съдебната практика на Съда на Европейския съюз ([3]).

([1]) ОВ L 119, 4.5.2016 г., стр. 1.
([2]) Вж. съображение 101 от Регламент (ЕС) 2016/679.
([3]) Вж., като най-скорошна практика, решение по дело C-311/18, Facebook Ireland/Schrems („решение по делото *Schrems II*“), ECLI:EU:C:2020:559.

(4) Както бе пояснено от Съда на Европейския съюз, това не изисква установяване на идентично ниво на защита ([4]). По-специално средствата, до които въпросната трета държава прибягва за защита на личните данни, може да са различни от прилаганите в Съюза, стига те на практика да се окажат ефективни за осигуряването на адекватно ниво на защита ([5]). Поради това стандартът за адекватно ниво на защита не включва изискване за буквално възпроизвеждане на правилата на Съюза. Критерият се състои по-скоро в това дали чрез същността на правата на неприкосновеност на личния живот и тяхното ефективно прилагане, надзор и изпълнение чуждестранната система като цяло осигурява необходимото ниво на защита ([6]). В референтния документ за адекватното ниво на защита на Европейския комитет по защита на данните, който се стреми да изясни допълнително този стандарт, също са предоставени насоки в това отношение ([7]).

(5) Комисията анализира внимателно корейското право и практиката по него. Въз основа на констатациите, установени в съображения 8—208, Комисията заключава, че Република Корея осигурява адекватно ниво на защита на личните данни, предавани от администраторите или обработващите лични данни в Съюза ([8]) на образувания (например физически или юридически лица, организации, публични институции) в Корея, които попадат в приложното поле на Закона за защита на личните данни (Закон № 10465 от 29 март 2011 г., последно изменен със Закон № 16930 от 4 февруари 2020 г.). Това включва както администратори, така и обработващи лични данни (наречени „външни изпълнители“ ([9])) по смисъла на Регламент (ЕС) 2016/679. Констатацията за адекватно ниво на защита не обхваща обработването на лични данни за мисионерски дейности от религиозни организации или определянето на кандидати от политически партии, или обработването на лична кредитна информация съгласно Закона за кредитната информация от администратори на лични данни, които подлежат на надзор от Комисията по финансов надзор.

(6) В това заключение са взети предвид допълнителните гаранции, посочени в Уведомление № 2021-5 (приложение I), и официалните изявления, уверения и ангажименти от корейското правителство пред Комисията (приложение II).

(7) Действието на настоящото решение се изразява в това, че предаването на лични данни на администратори и обработващи лични данни в Република Корея може да се извършва, без да е необходимо получаването на допълнително разрешение. То не засяга прякото приложение на Регламент (ЕС) 2016/679 спрямо такива образувания, когато условията относно териториалното приложение на посочения регламент, изложени в член 3 от него, са изпълнени.

2. ПРАВИЛА, ПРИЛОЖИМИ КЪМ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

2.1. Уредбата на Република Корея за защита на данните

(8) Нормативната уредба на правото на неприкосновеност на личния живот и защита на личните данните в Корея се основава на Конституцията на Корея, обнародвана на 17 юли 1948 г. Макар че правото на защита на личните данни не е изрично уредено в Конституцията, все пак то е признато като основно право, произтичащо от конституционните права за човешко достойнство и стремеж към щастие (член 10), личен живот (член 17) и поверителност на комуникациите (член 18). Това е потвърдено както от Върховния съд ([10]), така и от Конституционния съд ([11]). Ограниченията на човешките права и свободи (включително правото на неприкосновеност на личния живот) могат да бъдат налагани само със закон и когато това е необходимо за националната сигурност или за поддържането на законността и реда за благото на обществото, и не могат да засягат същността на разглежданото право или свобода (член 37, параграф 2).

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

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

([6]) Вж. Съобщение на Комисията до Европейския парламент и Съвета „Обмен и защита на личните данни в един глобализиран свят“ (COM (2017) 7, 10.1.2017 г., раздел 3.1, стр. 6).

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

([8]) Настоящото решение има значение за ЕИП. В Споразумението за Европейското икономическо пространство (Споразумение за ЕИП) се предвижда разширяването на вътрешния пазар на Европейския съюз, за да включи трите държави от ЕИП — Исландия, Лихтенщайн и Норвегия. Решението на Съвместния комитет (РСК) за включване на Регламент (ЕС) 2016/679 в приложение XI към Споразумението за ЕИП бе прието от Съвместния комитет на ЕИП на 6 юли 2018 г. и влезе в сила на 20 юли 2018 г. Регламентът следователно попада в обхвата на това споразумение. Поради това за целите на решението позоваванията на ЕС и на държавите — членки на ЕС, следва да се разбират като обхващащи също така държавите от ЕИП.

([9]) Вж. раздел 2.2.3 от настоящото решение.

([10]) Вж. например Решение на Върховния съд 2014Da77970 от 15 октомври 2015 г. (резюме на английски език, достъпно чрез връзката „Lawmaker's disclosure of teachers' trade union members case“ на адрес https://www.privacy.go.kr/eng/enforcement_01.do), и цитираната в него съдебна практика, включваща Решение 2012Da49933, 24 юли 2014 г.

([11]) Вж. по-конкретно Решение на Конституционния съд 99Hun-ma513 от 26 май 2005 г. (резюме на английски език, достъпно на адрес http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2), и Решение 2014JHun-ma449 2013 Hun-Ba68 (консолидирано) от 23 декември 2015 г. (резюме на английски език, достъпно чрез връзката „Change of resident registration number case“ на адрес: https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Макар че на различни места в Конституцията се разглеждат правата на корейските граждани, Конституционният съд се е произнесъл, че чужденците също са обект на основни права ([12]). По-специално Съдът е постановил, че защитата на човешкото достойнство и стойност, както и правото на стремеж към щастие, са права на всяко човешко същество, а не само на гражданите на страната ([13]). Освен това съгласно официалните изявления на корейското правителство ([14]) по принцип се приема, че в членове 12—22 от Конституцията (които включват правата на неприкосновеност на личния живот) са залегнали основните човешки права ([15]). Макар че до момента не съществува съдебна практика, касаеща специално правото на неприкосновеност на личния живот на чужденците, обосноваването му със зачитането на човешкото достойнство и стремежа към щастие е в подкрепа на този извод ([16]).

(10) Освен това Корея е приела поредица от закони в областта на защитата на данните, които предоставят гаранции на всички физически лица, независимо от тяхната националност ([17]). За целите на настоящото решение са приложими следните закони:

— Закон за защита на личните данни (ЗЗЛД);

— Закон за използването и защитата на кредитна информация ([18]);

— Закон за защита на поверителността на комуникациите.

(11) Със ЗЗЛД се урежда общата правна уредба за защита на данните в Република Корея. Той е допълнен от 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 ЗЗЛД), който подобно на ЗЗЛД е правно обвързващ и приложим.

(12) Освен това в регулаторните „Уведомления“, приети от Комисията за защита на личните данни (КЗЛД), са предвидени допълнителни правила относно тълкуването и прилагането на ЗЗЛД. Въз основа на член 5 (Задължения на държавата) и член 14 (Международно сътрудничество) от ЗЗЛД КЗЛД прие Уведомление № 2021-5 от 1 септември 2020 г. (изменено с № 2021-1 от 21 януари 2021 г. и Уведомление № 2021-5 от 16 ноември 2021 г., по-долу „Уведомление №2021-5“) относно тълкуването, прилагането и изпълнението на определени разпоредби на ЗЗЛД. В това уведомление се дават пояснения относно обработването на лични данни съгласно ЗЗЛД, както и допълнителни гаранции за предаваните на Корея лични данни въз основа на настоящото решение. Уведомлението е правно обвързващо за администраторите на лични данни и спазването му може да бъде осигурено както от КЗЛД, така и от съдилищата ([19]). Нарушението на посочените в Уведомлението правила означава нарушение на съответните разпоредби на ЗЗЛД, които те допълват. Поради това съдържанието на допълнителните гаранции се анализира като част от оценката на съответните членове на ЗЗЛД. Накрая, допълнителни насоки относно ЗЗЛД и Указа за прилагането му, в които се предоставя информация за прилагането и изпълнението на правилата за защита на данните от КЗЛД, са предоставени в Наръчника относно ЗЗЛД и приетите от КЗЛД насоки ([20]).

([12]) Решение на Конституционния съд 93 Hun-MA120 от 29 декември 1994 г.

([13]) Решение на Конституционния съд 99HeonMa494 от 29 ноември 2001 г.

([14]) Вж. раздел 1.1 от приложение II.

([15]) Вж. също така член 1 от Закона за защита на личните данни, който се позовава изрично на „свободите и правата на физическите лица“. По-конкретно в него се заявява, че целта на закона е „уреждането на обработването и защитата на личните данни с цел да се защитят свободата и правата на физическите лица, както и за допълнително утвърждаване на тяхното достойнство и стойност.“ По подобен начин в член 5, параграф 1 от Закона за защита на личните данни се установява отговорността на държавата да „формулира политики с цел предотвратяване на вредните последици от безцелното събиране, злоупотребата и неправилното използване на лични данни, недискретното наблюдение и преследване и др., както и с цел подобряване на зачитането на човешкото достойнство и личната неприкосновеност“.

([16]) Освен това в член 6, параграф 2 от Конституцията се предвижда, че статутът на чужденците е гарантиран в съответствие с международното право и международните договори. 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).

([17]) Това включва правила, които са приложими по отношение на защитата на личните данни, но не се прилагат в ситуация, при която личните данни се събират в Съюза и се предават на Корея съгласно Регламент (ЕС) 2016/679, например в Закона за защитата, използването и пр. на информация за местоположението.

([18]) Целта на този закон е да се стимулира надеждното боравене с кредитна информация, като се насърчи ефикасното използване и системното управление на кредитната информация и като се защити неприкосновеността на личния живот от неправилно използване и злоупотреба с кредитна информация (член 1 от закона).

([19]) Например корейските съдилища са се произнесли относно спазването на регулаторните уведомления по редица дела, включително във връзка с това, че корейските администратори на лични данни носят отговорност за нарушаване на дадено уведомление (вж. например Решение на Върховния съд 2018Da219406 от 25 октомври 2018 г., в което съдът е разпоредил на съответния администратор на лични данни да заплати обезщетение на физическите лица за понесени вреди поради нарушение на „Известие за стандарта за мерките за гарантиране на безопасността на личните данни“; вж. също Решение 2018Da219352 на Върховния съд от 25 октомври 2018 г.; Решение 2011Da24555 на Върховния съд от 16 май 2016 г.; Решение 2014Gahap511956 на Централния градски съд на Сеул от 13 октомври 2016 г.; Решение 2009Gahap43176 на Централния градски съд на Сеул от 26 януари 2010 г.).

([20]) Член 12, параграф 1 от ЗЗЛД.

(13) Въз основа на член 5 (Задължения на държавата) и член 14 (Международно сътрудничество) от ЗЗЛД КЗЛД прие Уведомление № 2021-1 от 1 септември 2020 г. (изменено с № 2021-1 от 21 януари 2021 г., по-долу „Уведомление №2021-1“) относно тълкуването, прилагането и изпълнението на определени разпоредби на ЗЗЛД. По-конкретно това включва името, данните за контакт, финансовите сделки, кредитния рейтинг, застрахователния статут или салдото по заем, когато тази информация се използва за определяне на кредитоспособността на лицето ([21]). От друга страна когато тази информация се използва за други цели (като например във връзка с човешки ресурси), ЗЗЛД се прилага в своята цялост. Що се отнася до специалните разпоредби на ЗКИ за защита на данните, спазването им се контролира частично от КЗЛД (за търговски организации вж. член 45-3 от ЗКИ) и частично от Комисията по финансовите услуги ([22]) (относно финансовия сектор, включително агенции за кредитен рейтинг, банки, застрахователни дружества, взаимоспомагателни банки, специализирани кредитни финансови дружества, дружества за финансови инвестиционни услуги, финансови дружества за ценни книжа, кредитни съюзи и т.н., вж. член 45, параграф 1 от ЗКИ във връзка с член 36-2 от Указа за прилагане на ЗКИ и член 38 от Закона за Комисията по финансовите услуги). Във връзка с това обхватът на настоящото решение е ограничен до търговски оператори, които подлежат на надзор от страна на КЗЛД ([23]). Специалните правила на ЗКИ, които са приложими в този контекст (когато няма специални правила, се прилагат общите правила на ЗЗЛД), са описани в раздел 2.3.11.

2.2. **Материално и персонално приложно поле на ЗЗЛД**

(14) Защитата на личните данни се урежда от ЗЗЛД (член 6), освен ако в други законови актове е предвидено друго. Неговото материално и персонално приложно поле се определя от установените понятия за „лични данни“, „обработване“ и „администратор на лични данни“.

2.2.1. *Определение за лични данни*

(15) В член 2, параграф 1 от ЗЗЛД личните данни се определят като информация, свързана с живо физическо лице, която го идентифицира пряко, например чрез неговото име, регистрационен номер или изображение, или непряко, а именно когато информация, която сама по себе си не може да послужи за идентифициране на определено лице, лесно може да се комбинира с друга информация. Дали информацията може да се комбинира „лесно“, зависи от това дали има достатъчна вероятност за такава комбинация, като се отчита възможността за получаване на друга информация, както и времето, разходите и технологиите, необходими за идентифицирането на дадено лице.

(16) Освен това псевдонимизирана информация, т.е. информация, чрез която не може да се идентифицира конкретно лице, без да се използва допълнителна информация или без тя да се комбинира с допълнителна информация, за да бъде възстановена в предишния си вид, се смята за лични данни съгласно ЗЗЛД (член 2, параграф 1, буква в) от ЗЗЛД). За разлика от това информацията, която е напълно „анонимизирана“, е изключена от приложното поле на ЗЗЛД (член 58-2 от ЗЗЛД). Такъв е случаят с информация, чрез която не може да бъде идентифицирано конкретно физическо лице, дори ако се комбинира с друга информация, като се отчитат в разумна степен необходимите за идентифицирането време, разходи и технологии.

(17) Това съответства на материалното приложно поле на Регламент (ЕС) 2016/679 и неговите понятия за „лични данни“, „псевдонимизация“ ([24]) и „анонимна информация“ ([25]).

([21]) Член 2, параграф 1 от ЗКИ.

([22]) Комисията по финансовите услуги е надзорният орган на Корея по отношение на финансовия сектор и в това си качество тя отговаря също така за спазването на ЗКИ.

([23]) Ако това се промени в бъдеще, например чрез разширяване на юрисдикцията на КЗЛД към цялото обработване на лична кредитна информация съгласно ЗКИ, може да се помисли за изменение на решението относно адекватността с цел обхващане също така на образуванията, които понастоящем са под надзора на Комисията по финансовите услуги.

([24]) Съгласно ЗЗЛД „процесът на псевдонимизация“ означава обработване с методи, чрез които личните данни се заличават частично или се заместват частично или изцяло по такъв начин, че конкретното лице не може да бъде разпознато без допълнителна информация (член 2, параграфи 1—2 от ЗЗЛД). Това съответства на определението за псевдонимизация в член 4, параграф 5 от Регламент (ЕС) 2016/679, според който тя означава „обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано.“

([25]) По-специално в съображение 26 от Регламент (ЕС) 2016/679 се пояснява, че регламентът не се прилага по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано. Това на свой ред зависи от всички средства, за които има достатъчна вероятност да бъдат използвани от администратора или от друго лице, за да се идентифицира пряко или непряко съответното физическо лице. За да се установи дали има достатъчна вероятност тези средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития.

2.2.2. *Определение за обработване*

(18) Понятието „обработване“ се определя в широк смисъл в ЗЗЛД като „събирането, създаването, свързването, блокирането, записването, съхраняването, запазването, обработването с добавена стойност, редактирането, извличането, произвеждането, коригирането, възстановяването, използването, предоставянето и разкриването на лични данни и други сходни дейности“ ([26]). Макар че някои разпоредби на ЗЗЛД се отнасят само до конкретни видове обработване, като „използване“, „предоставяне“ или „събиране“ ([27]), понятието за „използване“ се тълкува като включващо всеки вид обработване, различно от „събиране“ или „предоставяне“ (на трета страна). Това широко тълкуване на „използване“ гарантира липсата на пропуски в защитата по отношение на конкретни дейности по обработване. Следователно понятието за обработване съответства на същото понятие съгласно Регламент (ЕС) 2016/679.

2.2.3. *Администратор на лични данни и „външен изпълнител“*

(19) ЗЗЛД се прилага за администраторите на лични данни („администратор“). Подобно на Регламент (ЕС) 2016/679 това включва всяка публична институция, юридическо лице, организация или физическо лице, които обработват лични данни пряко или непряко с цел управление на досиета с лични данни като част от своите дейности ([28]). В този контекст „досие с лични данни“ означава „набор или набори лични данни, подредени или организирани по систематичен начин въз основа на определено правило за лесен достъп до личните данни“ (член 2, параграф 4 от ЗЗЛД) ([29]). Във вътрешен план администраторът е длъжен да обучава лицата, които участват в обработването под негово ръководство, като например фирмени длъжностни лица или служители, и да упражнява подходящ контрол и надзор върху тях (член 28, параграф 1 от ЗЗЛД).

(20) Предвиждат се специални задължения, когато администратор („възложителят“) възлага обработването на лични данни на трето лице („външния изпълнител“). По-специално възлагането на дейности на външни изпълнители трябва да се урежда от правно обвързваща договореност (обикновено договор) ([30]), в която се определят обхватът на работата, възложена на външен изпълнител, целта на обработването, надзорът от администратора, отговорността (обезщетение за щети, причинени от нарушаването на договорни задължения), както и ограниченията при възложеното на подизпълнител обработване ([31]) (член 26, параграфи 1 и 2 от ЗЗЛД във връзка с член 28, параграф 1 от Указа за прилагане на ЗЗЛД) ([32]).

(21) Освен това администраторът трябва да публикува и постоянно да актуализира подробности за възложената на външен изпълнител работа и за идентичността на външния изпълнител или, доколкото възложеното на външен изпълнител обработване се отнася за дейности по директен маркетинг, да уведомява пряко лицата за съответната информация (член 26, параграфи 2 и 3 от ЗЗЛД във връзка с член 28, параграфи 2—5 от Указа за прилагане на ЗЗЛД) ([33]).

(22) Освен това съгласно член 26, параграф 4 от ЗЗЛД във връзка с член 28, параграф 6 от Указа за прилагане на ЗЗЛД администраторът е длъжен да „обучи“ външния изпълнител относно необходимите мерки за сигурност и да упражнява надзор, включително чрез инспекции, над спазването на всички задължения на администратора съгласно ЗЗЛД ([34]), както и съгласно договора с външния изпълнител. Когато външният изпълнител причини вреда поради нарушение на ЗЗЛД, неговите действия или бездействия ще бъдат приписани на администратора за целите на отговорността, както когато вредата е причинена от служител на администратора (член 26, параграф 6 от ЗЗЛД).

([26]) Член 2, параграф 2 от ЗЗЛД.

([27]) Например членове 15—19 от ЗЗЛД се отнасят само до събирането, използването и предоставянето на лични данни.

([28]) Член 2, параграф 5 от ЗЗЛД. Публичните институции по смисъла на ЗЗЛД включват всички ведомства или агенции на централната администрация и свързаните с тях органи, органите на местното самоуправление, училищата и публичните корпорации с инвестиции от органите на местното самоуправление, административните органи на Националното събрание и съдебната власт (включително Конституционния съд) (член 2, параграф 6 от ЗЗЛД във връзка с член 2 от Указа за прилагане на ЗЗЛД).

([29]) Това съответства на материалното приложно поле на Регламент (ЕС) 2016/679. Съгласно член 2, параграф 1 от Регламент (ЕС) 2016/679 регламентът се прилага за „обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.“ В член 4, точка 6 от Регламент (ЕС) 2016/679 „регистър с лични данни“ се определя като „всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии“. Във връзка с това в съображение 15 се пояснява, че защитата на лицата следва да се прилага за „обработването на лични данни с автоматични средства, както и за ръчното им обработване, ако личните данни се съхраняват или са предназначени да се съхраняват в регистър с лични данни. Досиетата или групите от досиета, както и заглавните им страници, които не са структурирани съгласно специфични критерии, не следва да попадат в обхвата на настоящия регламент.“

([30]) Вж. Наръчник относно ЗЗЛД, глава III, раздел 2 относно член 26 (стр. 203—212), в който се обяснява, че член 26, параграф 1 от ЗЗЛД се отнася за обвързващи договорености, например договори или подобни договорености.

([31]) Съгласно член 26, параграф 5 от ЗЗЛД на обработващия лични данни е забранено да използва лични данни извън обхвата на възложената на външен изпълнител работа или да предоставя лични данни на трета страна. Неспазването на това изискване може да доведе до наказателна санкция съгласно член 71, точка 2 от ЗЗЛД.

([32]) Неспазването на това изискване може да доведе до налагането на глоба, вж. член 75, параграф 4, точка 4 от ЗЗЛД.

([33]) Неспазването на това изискване може да доведе до налагането на глоба, вж. член 75, параграф 2, точка 1, параграф 4, точка 5 от ЗЗЛД.

([34]) Вж. също така член 26, параграф 7 от ЗЗЛД, съгласно който членове 15—25, 27—31, 33—38 и 50 се прилагат *mutatis mutandis* за обработващия лични данни.

(23) Макар че в ЗЗЛД не се използват различни понятия за „администратори“ и „обработващи лични данни“, правилата за възлагане на дейности на външни изпълнители предвиждат по същество равностойни задължения и гаранции, като тези, с които се урежда взаимоотношението между администратори и обработващи лични данни съгласно Регламент (ЕС) 2016/679.

2.2.4. *Специални разпоредби за доставчиците на информационни и комуникационни услуги*

(24) Макар че ЗЗЛД се отнася за обработването на лични данни от администратор, определени разпоредби съдържат специални правила (като *lex specialis*) за обработването на лични данни на „ползватели“ от „доставчици на информационни и комуникационни услуги“ ([35]). Понятието „ползватели“ обхваща лица, които използват информационни и комуникационни услуги (член 2, параграф 1, точка 4 от Закона за насърчаване на използването на информационната и комуникационната мрежа и за защита на данните, „Закон за мрежата“). Това изисква от лицето да използва пряко телекомуникационните услуги, които се предоставят от корейски телекомуникационен оператор, или да използва информационни услуги ([36]), които се предоставят за търговски цели (т.е. за печалба) от образуване, което на свой ред разчита на услугите на телекомуникационен оператор, лизензиран/регистриран в Корея ([37]). И в двата случая образуването, което е обвързано от специалните разпоредби на ЗЗЛД, е това, което предлага онлайн услуга пряко на дадено лице (т.е. ползвател).

(25) За разлика от това констатацията за адекватно ниво на защита засяга единствено нивото на защита, което се осигурява за личните данни, предавани от администратор/обработващ лични данни в Съюза на образувание в трета държава (в случая: Република Корея). В този сценарий лицата в Съюза обикновено ще имат пряко взаимоотношение само с „износителя на данни“ в Съюза, а не с корейския доставчик на информационни и комуникационни услуги ([38]). Следователно специалните разпоредби на ЗЗЛД по отношение на личните данни на ползвателите на информационни и комуникационни услуги ще се прилагат най-много само в ограничени ситуации за лични данни, предавани съгласно настоящото решение.

2.2.5. *Освобождаване от прилагането на някои разпоредби на ЗЗЛД*

(26) Съгласно член 58, параграф 1 от ЗЗЛД част от ЗЗЛД (т.е. членове 15—57) не се прилага по отношение на четири категории обработване на данни ([39]). По-конкретно не се прилагат частите от ЗЗЛД, в които се разглеждат конкретните основания за обработването, определени задължения за защита на данните, подробните правила за упражняването на индивидуални права, както и правилата, уреждащи разрешаването на спорове от Комитета за уреждане на спорове, свързани с лични данни. Други основни разпоредби от ЗЗЛД остават приложими, по-конкретно общите разпоредби относно принципите за защита на данните (член 3 от ЗЗЛД) — включително например принципите за законосъобразност, за определяне на целта и за ограничаване на целта, за свеждане на данните до минимум, за точност и сигурност на данните — и индивидуалните права (на достъп, коригиране, заличаване и преустановяване, вж. член 4 от ЗЗЛД). В допълнение към това в член 58, параграф 4 от ЗЗЛД се налагат конкретни задължения по отношение на такива дейности по обработване, а именно по отношение на свеждането на данните до минимум, ограниченото съхраняване на данни, мерките за сигурност и разглеждането на жалби ([40]). В резултат на това физическите лица все пак могат да подават жалба до КЗЛД, ако тези принципи и задължения не се спазват, и КЗЛД е оправомощена да предприеме мерки по прилагане на законодателството в случай на неспазване.

([35]) Вж. по-конкретно член 18, параграф 2 и глава VI от ЗЗЛД.

([36]) Информационните услуги включват както предоставянето на информация, така и посреднически услуги за предоставянето на информация.

([37]) Вж. член 2, параграф 1, точка 3 (във връзка с член 2, параграф 1, точки 2 и 4) от Закона за мрежата и член 2, параграфи 6 и 8 от Закона за телекомуникационните дейности.

([38]) Доколкото корейските доставчици на информационни и комуникационни услуги имат пряко взаимоотношение с лица в ЕС (чрез предлагане на онлайн услуги), това би могло да доведе до прякото прилагане на Регламент (ЕС) 2016/679 съгласно член 3, параграф 2, буква а) от него.

([39]) В член 58, параграф 2 от ЗЗЛД се предвижда също така, че членове 15, 22, член 27, параграфи 1—2, членове 34 и 37 не се прилагат за лични данни, обработени чрез използване на устройства за обработване на визуални данни, инсталирани и функциониращи на открити места. Тъй като тази разпоредба засяга използването на видеонаблюдение на територията на Корея, т.е. прякото събиране на лични данни от физически лица в Корея, тя не е от значение за целта на настоящото решение, което се отнася до предаване на лични данни от администратори/обработващи лични данни в ЕС на образувания в Корея. В допълнение към това съгласно член 58, параграф 3 от ЗЗЛД член 15 (събиране и използване на лични данни), член 30 (задължение за въвеждане на публична политика за неприкосновеност на личния живот) и член 31 (задължение за определяне на служител по въпросите на поверителността) не се прилагат по отношение на лични данни, които се обработват с цел управление на групи или асоциации за приятелство (т.е. клубове по интереси). Тъй като тези групи се смятат за лични по характер, без никаква връзка с професионална или търговска дейност, не се изисква специална правна уредба (например съгласие на засегнатите физически лица), за да се събират и използват техните данни в този контекст. Всички други разпоредби на ЗЗЛД обаче (например свеждане на данните до минимум, ограничаване на целите, законосъобразност на обработването, сигурност и индивидуални права) продължават да се прилагат. Освен това обработването на лични данни извън целта за създаване на социална група не би могло да се ползва от освобождаването.

([40]) По-специално в член 58, параграф 4 от ЗЗЛД се предвижда задължение за обработване на лични данни до минималната необходима степен за постигане на предвидената цел, за обработване на лични данни за минимален период и за предприемане на необходимите мерки за безопасното управление и подходящото обработване на лични данни. Последното включва технически, управленски и физически гаранции, както и мерки за гарантиране на надлежното разглеждане на индивидуалните жалби.

(27) Първо, частичното освобождаване обхваща лични данни, събрани съгласно Закона за статистиката, с оглед на обработването им от публични институции. Съгласно поясненията, получени от корейското правителство, обработваните в този контекст лични данни обикновено засягат корейски граждани и само по изключение биха включвали информация за чужденци, а именно във връзка с данни за влизане в държавата и за напускането ѝ или относно чуждестранни инвестиции. В такива ситуации обаче тези данни обикновено не се предават от администратори/обработващи лични данни в Съюза, а по-скоро се събират пряко от публичните органи в Корея ([41]). Освен това подобно на предвиденото в съображение 162 от Регламент (ЕС) 2016/679 обработването на данни по Закона за статистиката подлежи на няколко изисквания и гаранции. По-конкретно със Закона за статистиката се налагат специални задължения, за да се гарантират точност, съгласуваност и безпристрастност; за да се гарантира поверителността на физическите лица; за да се защити информацията на респондентите в статистически изследвания, включително да се предотврати използването на тази информация за друга цел, различна от целта за събиране на статистически данни, и да се подложат членовете на персонала на изисквания за спазване на поверителност ([42]). Освен това публичните органи, които обработват статистически данни, трябва също така да спазват, наред с другото, принципите за свеждане на данните до минимум, за ограничаване на целта и за сигурност на данните (член 3 и член 58, параграф 4 от ЗЗЛД) и да позволяват на физическите лица да упражняват правата си (на достъп, коригиране, заличаване и преустановяване на използването, вж. член 4 от ЗЗЛД). Накрая, данните трябва да бъдат обработвани в анонимизирана или псевдонимизирана форма, ако това позволява да се изпълни целта на обработването (член 3, параграф 7 от ЗЗЛД).

(28) Второ, в член 58, параграф 1 от ЗЗЛД се разглеждат лични данни, които се събират или изискват за анализ на информация, свързана с националната сигурност. Обхватът и последиците от това частично освобождаване са описани по-подробно в съображение 149.

(29) Трето, частичното освобождаване се прилага за временното обработване на лични данни, когато това е спешно необходимо за обществената безопасност или сигурност, включително за общественото здраве. Тази категория се тълкува стриктно от КЗЛД и съгласно получената информация не е била използвана никога. Тя се прилага само в спешни случаи, изискващи спешни действия, например за проследяване на инфекциозни агенти или за спасяване и подпомагане на жертви на природни бедствия ([43]). Дори в тези ситуации частичното освобождаване обхваща само временното обработване на лични данни за ограничен период от време, който е необходим за извършването на такова действие. Ситуациите, в които това може да се прилага за видовете предаване на данни, обхванати от настоящото решение, са дори още по-ограничени с оглед на малката вероятност за това лични данни, предавани от Съюза към корейските оператори, да са от типа, който може да направи тяхното последващо обработване „спешно необходимо“ за такива спешни ситуации.

(30) Накрая, частичното освобождаване се прилага по отношение на лични данни, събирани или използвани от пресата, за мисионерски дейности на религиозни организации или за номинирането на кандидати от политически партии. Освобождаването се прилага само когато лични данни се обработват от пресата, от религиозни организации или от политически партии за тези конкретни цели (т.е. журналистически дейности, мисионерска работа и номинирането на политически кандидати). Когато тези образувания обработват лични данни за други цели, като управление на човешки ресурси или вътрешно администриране, ЗЗЛД се прилага изцяло.

(31) Що се отнася до обработването на лични данни от пресата за журналистически дейности, балансът между свободата на изразяване на мнение и други права (включително правото на неприкосновеност на личния живот) се осигурява чрез Закона за арбитража и средствата за правна защита и др. за вреди, причинени от публикации в пресата („Закон за пресата“) ([44]). По-специално в член 5 от Закона за пресата се

([41]) В това отношение в член 33 от Закона за статистиката се изисква от публичните институции да защитават информацията на респондентите в статистическите изследвания, включително с цел да се предотврати използването на тази информация за друга цел, различна от целта за събиране на статистически данни.

([42]) Член 2, параграфи 2—3, член 30, параграф 2, членове 33 и 34 от Закона за статистиката.

([43]) Наръчник относно ЗЗЛД, раздел във връзка с член 58.

([44]) Например в член 4 от Закона за пресата се предвижда, че репортажите в пресата трябва да бъдат безпристрастни и обективни, в обществен интерес, да зачитат достойнството и човешките качества, да не съдържат клевети към други физически лица, нито да нарушават правата им, обществения морал и социалната етика.

предвижда, че пресата (т.е. който и да е радио- и телевизионен оператор, вестник, периодично или онлайн издание), интернет новинарските агенции или мултимедийните радио- и телевизионни оператори в интернет не може да нарушават неприкосновеността на личния живот на гражданите. Ако все пак е налице нарушение на неприкосновеността на личния живот, то трябва да бъде своевременно отстранено в съответствие с конкретните процедури, предвидени в закона. В това отношение законът предоставя на лицата, които понасят вреди от репортаж в пресата, редица права, например да получат корекция на публикация с невярно твърдение, възможност за опровержение или допълнителен репортаж (когато репортажът в пресата се отнася за твърдения относно престъпления, за които лицето по-късно бива оправдано) ([45]). Претенциите на гражданите могат да бъдат удовлетворени директно от печатните издания (чрез омбудсман) ([46]), чрез помирение или арбитраж (пред специализирана Комисия за пресарбитраж) ([47]) или от съдилищата. Гражданите могат да получат също така обезщетение, когато претърпят парични щети, нарушение на права, свързани с личността, или друг емоционален стрес поради незаконно действие на пресата (умишлено или поради небрежност) ([48]). Съгласно закона пресата е освободена от отговорност, доколкото репортаж в нея, който засяга правата на гражданин, не противоречи на социалните ценности и е публикуван със съгласието на въпросния гражданин или в интерес на обществото (и има достатъчно основания да се смята, че този репортаж съответства на истината) ([49]).

(32) Докато обработването на лични данни в пресата във връзка с журналистически дейности е предмет на специални гаранции, които са следствие от Закона за пресата, няма такива допълнителни гаранции относно използването на изключенията за дейностите по обработване на лични данни от религиозни организации и политически партии по начин, който е сравним с членове 85, 89 и 91 от Регламент (ЕС) 2016/679. Поради това Комисията смята, че е подходящо да изключи от приложното поле на настоящото решение религиозните организации, доколкото те обработват лични данни за своите мисионерски дейности, и политическите партии, доколкото те обработват лични данни в контекста на номинирането на кандидати.

2.3. **Гаранции, права и задължения**

2.3.1. *Законосъобразност и добросъвестност на обработването*

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

(34) Този принцип е залегнал в член 3, параграфи 1 и 2 от ЗЗЛД и е подсилен в член 59 от ЗЗЛД, в който се забранява обработването на лични данни „чрез измама, с неправомерни или несправедливи средства“, „без юридически правомощия“ или „без надлежно правомощие“ ([50]). Тези общи принципи на законосъобразно обработване са доразвити в членове 15—19 от ЗЗЛД, в които се определят различните правни основания за обработването (събиране, използване и предоставяне на трети страни), включително обстоятелствата, при които това може да включва промяна на целта (член 18 от ЗЗЛД).

([45]) Членове 15—17 от Закона за пресата.

([46]) Всяко печатно издание или медия има свой омбудсман за предотвратяване и отстраняване на потенциални вреди, причинени от пресата (например чрез препоръчване на поправка на репортажи в пресата, които са неверни или увреждат репутацията на други лица), член 6 от Закона за пресата.

([47]) Комисията се състои от 40 до 90 арбитражни комисари, определени от министъра на културата, спорта и туризма, избрани измежду лица с квалификация на съдии, адвокати, лица, занимаващи се със събиране или отразяване на новини от поне 10 години, или други лица с експертни познания в областта на пресата. Арбитражните комисари не могат едновременно да бъдат държавни служители, членове на политически партии или журналисти. В съответствие с член 8 от Закона за пресата арбитражните комисари трябва изпълняват задълженията си независимо и не се подчиняват на разпореждания или инструкции във връзка с тези задължения. Освен това са въведени специални правила за предотвратяване на конфликти на интереси, например чрез изключване на отделни комисари от разглеждането на отделни случаи, в които техен съпруг или роднини са страна по случая (член 10 от Закона за пресата). Комисията може да разглежда спорове чрез помирение или арбитраж, но може да дава също така препоръки за коригиране на нарушения (раздел 5 от Закона за пресата).

([48]) Член 30 от Закона за пресата.

([49]) Член 5 от Закона за пресата.

([50]) В член 59 от ЗЗЛД се забранява на физическо лице, „което притежава или някога е притежавало лични данни“, да „придобива лични данни или да получава съгласие за обработване на лични данни чрез измама, с неправомерни или несправедливи средства“, „да разкрива лични данни, придобити в хода на дейността, или да ги предоставя за ползване на трети страни без правомощие“ или „да уврежда, унищожава, променя, подправя или да разкрива лични данни на друго лице без юридически правомощия или без надлежно правомощие.“ Неспазването на тази забрана може да доведе до наказателни санкции, вж. член 71, параграфи 5 и 6, и член 72, параграф 2 от ЗЗЛД. В член 70, параграф 2 от ЗЗЛД се предвижда също така налагането на наказателна санкция за получаване на лични данни, обработвани от трети страни, чрез измама или с други несправедливи средства или методи, или за предоставянето им на трета страна с цел печалба или за несправедливи цели, както и за подпомагане или организиране на такова поведение.

(35) Съгласно член 15, параграф 1 от ЗЗЛД администратор може да събира лични данни само въз основа на ограничен брой правни основания (в рамките на обхвата на целта за събиране). Тези основания са: 1) съгласието на субекта на данните ([51]) (точка 1); 2) необходимостта от сключване и изпълнение на договор със субекта на данните (точка 4); 3) специално разрешение по закон или необходимост от спазване на правно задължение (точка 2); необходимостта ([52]) дадена публична институция да изпълни задачите в рамките на своята юрисдикция съгласно предписанията на закона; 4) явната необходимост за защита на живота, телесните или имуществените интереси на субекта на данните или на трето лице от непосредствена опасност (само когато субектът на данните не е в състояние да изрази своето намерение или не може да бъде получено предварително съгласие) (точка 5); 5) необходимостта да се удовлетвори „оправданият интерес“ на администратора на лични данни, който има „явно предимство“ пред интересите на субекта на данните (и само когато обработването има „съществена връзка“ със законния интерес и не излиза извън рамките на разумното) (точка 6) ([53]). Тези основания за обработване по същество са равностойни на изложените в член 6 от Регламент (ЕС) 2016/679, включително основанието за „оправдан интерес“, което съответства на основанието за „законен интерес“ в член 6, параграф 1 от Регламент (ЕС) 2016/679.

(36) След като бъдат събрани, личните данни може да се използват в рамките на обхвата на целта на събирането (член 15, параграф 1 от ЗЗЛД) или „в рамките на обхвата, разумно свързан“ с целта на събирането, отчитайки вероятните неблагоприятни последствия, причинени на субекта на данните, и при условие че са приложени съответните мерки за сигурност (например криптиране) (член 15, параграф 3 от ЗЗЛД). За да се определи дали целта на използването е „разумно свързана“ с първоначалната цел на събирането, в Указа за прилагане на ЗЗЛД са предвидени конкретни критерии, подобни на тези в член 6, параграф 4 от Регламент (ЕС) 2016/679. По-конкретно трябва да има съществено отношение към първоначалната цел; допълнителното използване трябва да е предвидимо (например в контекста на обстоятелствата, при които са събрани данните); и ако е възможно, данните трябва да бъдат псевдонимизирани ([54]). Конкретните критерии, използвани от администратор при тази оценка, трябва да бъдат оповестени предварително в политиката за поверителност ([55]). Освен това от служителя по въпросите на поверителността (вж. съображение 94) се изисква да провери изрично дали в рамките на тези параметри се извършва допълнително използване.

([51]) Съгласието трябва да бъде свободно дадено, информирано, конкретно и изразено по един от няколкото начина, предвидени в закона. Във всеки случай съгласие не може да бъде получено чрез измама, неправомерни или по друг начин несправедливи средства (член 59, параграф 1 от ЗЗЛД). Първо, съгласно член 4, точка 2 от ЗЗЛД субектите на данни имат право „да се съгласят или не“ и „да изберат обхвата на съгласието“, и следва да бъдат информирани за това (член 15, параграф 2, член 16, параграфи 2 и 3, член 17, параграф 2 и член 18, параграф 3 от ЗЗЛД). Член 22, параграф 5 от ЗЗЛД съдържа допълнителна гаранция, като забранява на администратора да отказва предоставянето на стоки или услуги, когато това може да подкопае свободния избор на физическото лице да даде съгласието си. Това включва ситуации, в които само определени видове обработване изискват съгласие (докато други се основават на договор), и обхваща също така допълнителното обработване на лични данни, събрани в контекста на предоставянето на стоки или услуги. Второ, съгласно член 15, параграф 2, член 17, параграфи 2 и 3 и член 18, параграф 3 от ЗЗЛД, когато иска съгласие, администраторът трябва да информира субекта на данните за „особеностите“ на съответните лични данни (например че засягат чувствителни данни, вж. член 17, параграф 2, точка 2а от Указа за прилагане на ЗЗЛД), за целта на обработването, за периода на съхранение и за всеки получател на данните. Всяко такова искане се отправя „по изрично разпознаваем начин“, с който се прави разграничение между въпросите, които изискват съгласие, и други въпроси (член 22, параграфи 1—4 от ЗЗЛД). Трето, в член 17, параграф 1, точки 1—6 от Указа за прилагане на ЗЗЛД се посочват конкретните методи, по които администраторът получава съгласие, например чрез писмено съгласие, с подписа на субекта на данните, или съгласие по електронната поща (с отговор). Макар че в ЗЗЛД не се предоставя общо право на физическите лица да оттеглят съгласието си, вместо това те имат право да получат преустановяване на обработването на свързани с тях данни, което, когато бъде упражнено, ще доведе до прекратяване на обработването и заличаването на данните (вж. съображение 78 относно правото на преустановяване).

([52]) Съгласно получената информация от КЗЛД публичните институции могат да се позовават на това основание само ако обработването на лични данни е неизбежно, т.е. за институцията трябва да е невъзможно или необосновано трудно да изпълнява функциите си без обработването на данните.

([53]) В член 39-3 от ЗЗЛД се налагат специфични (по-строги) задължения за доставчиците на информационни и комуникационни услуги по отношение на събирането и използването на личните данни на техните ползватели. По-конкретно в него се изисква доставчикът да получи съгласието на ползвателя, след като му предостави информация за целта на събирането/използването, за категориите лични данни, които ще събира, и за периода, за който ще бъдат обработвани личните данни (член 39-3, параграф 1 от ЗЗЛД). Същото важи и при промяна на някой от тези аспекти. Неполучаването на съгласие за събирането на лични данни води до наказателни санкции (член 71, параграфи 4—5 от ЗЗЛД). По изключение лични данни на ползвателите може да се събират или използват от доставчиците на информационни и комуникационни услуги без получаване на предварително съгласие. Такъв е случаят, (1) когато е ясно, че е трудно да се получи съгласие за личните данни, които са необходими за изпълнението на договора за предоставяне на информационни и комуникационни услуги, по икономически и технологични причини (например, когато неизбежно се създават лични данни в процеса на изпълнението на договор, като данни от фактура, записи за достъп и записи за плащания); (2) когато това е необходимо за уреждането на такси след предоставянето на информационни и комуникационни услуги; или (3) ако е разрешено от други закони (например в член 21, параграф 1, точка 6 от Закона за защита на потребителите в електронната търговия се предвижда, че стопанските субекти могат да събират лични данни на законен настойник или попечител на малолетно или непълнолетно лице, за да потвърдят дали е получено неговото валидно съгласие) (член 39-3, параграф 2 от ЗЗЛД). Във всички случаи доставчиците на информационни и комуникационни услуги не могат да откажат да предоставят услуги само поради това, че ползвателят не предоставя повече лични данни от минималното изискване (т.е. информацията, която е необходима за изпълнение на съществените елементи на съответната услуга), вж. член 39-3, параграф 3 от ЗЗЛД.

([54]) Вж. член 14-2 от Указа за прилагане на ЗЗЛД.

([55]) Вж. член 14-2, параграф 2 от Указа за прилагане на ЗЗЛД.

(37) Подобни (но в известна степен по-строги) правила се прилагат по отношение на предоставянето на данни на трета страна. Съгласно член 17, параграф 1 от ЗЗЛД предоставянето на лични данни на трета страна е разрешено въз основа на съгласие ([56]) или, в рамките на целта на събирането, когато данните са събрани на едно от правните основания в член 15, параграф 1, точки 2, 3 и 5 от ЗЗЛД. Това изключва по-конкретно разкриване въз основа на „оправдан интерес“ от страна на администратора. Освен това в член 17, параграф 4 от ЗЗЛД се разрешава предоставянето им на трета страна „в рамките на обхвата, разумно свързан“ с целта на събирането, отново при отчитане на вероятните неблагоприятни последствия за субекта на данните и при условие че са приложени съответните мерки за сигурност (например криптиране) (член 15, параграф 3 от ЗЗЛД). Същите фактори като описаните в съображение 36 трябва да бъдат взети предвид, за да се оцени дали предоставянето е в рамките на обхвата, разумно свързан с целта на събирането, и дали се прилагат същите гаранции (т.е. по отношение на прозрачността чрез политиката за поверителност и участието на служителя по въпросите на поверителността).

(38) Получаването от страна на корейски администратор на лични данни от Съюза се смята за „събиране“ по смисъла на член 15 от ЗЗЛД. В Уведомление № 2021-5 (раздел I от приложение I към настоящото решение) се пояснява, че целта, поради която са прехвърлени данните от съответното образувание от ЕС, представлява целта на събирането от страна на корейския администратор на лични данни. Вследствие на това корейските администратори на лични данни, които получават лични данни от Съюза, по принцип трябва да обработват тези данни в рамките на обхвата на целта на предаването, в съответствие с член 17 от ЗЗЛД.

(39) Специални ограничения се прилагат, в случай че администраторът желае да използва личните данни или да ги предостави на трета страна за цел, различна от целта на събирането ([57]). Съгласно член 18, параграф 2 от ЗЗЛД частен администратор може по изключение ([58]) да използва лични данни или да ги предостави на трета страна за различна цел: 1) въз основа на допълнително (в смисъл на отделно) съгласие от субекта на данните; 2) когато това е предвидено в специални законови разпоредби; или 3) при явна необходимост за защита на живота, телесните или имуществените интереси на субекта на данните или на трета страна от непосредствена опасност (само когато субектът на данните не е в състояние да изрази своето намерение или не може да бъде получено предварително съгласие) ([59]).

(40) Публичните институции също могат да използват лични данни или да ги предоставят на трета страна за различна цел в определени ситуации. Това включва случаи, при които за публичните институции иначе би било невъзможно да изпълняват своите задължения, както е предписано по закон, след разрешение от КЗЛД. Освен това публичните институции може да предоставят лични данни на друг орган или съд, когато това е необходимо за разследването и наказателното преследване на престъпления или за повдигане на обвинение; за да може даден съд да изпълнява функциите си, свързани с текущи съдебни производства; или за изпълнение на наказателна санкция или разпореждане за полагане на грижи или за настойничество/попечителство ([60]). Те могат също така да предоставят лични данни на чуждестранно правителство или на международна организация за изпълнение на договор или международна конвенция, и в този случай трябва да спазят също така изискванията за трансгранично предаване на данни (вж. съображение 90).

(41) Следователно принципите на законосъобразност и добросъвестност на обработването са залегнали в корейската правна уредба по начин, който по същество е равностоен на Регламент (ЕС) 2016/679, тъй като позволява обработването да се извършва само въз основа на легитимни и ясно определени основания. Освен това във всички посочени случаи обработването е разрешено само ако няма вероятност то да „накърни несправедливо“ интересите на субекта на данните или на трета страна, което изисква балансиране на интересите. В допълнение към това в член 18, параграф 5 от ЗЗЛД се предвиждат допълнителни гаранции, когато администраторът предоставя личните данни на трета страна, което може да включва искане за ограничаване на целта и начина на използване или за прилагане на конкретни мерки за сигурност. Третата страна на свой ред е длъжна да изпълни поисканите мерки.

([56]) Нарушенията на член 17, параграф 1, точка 1 от ЗЗЛД могат да доведат до налагането на наказателни санкции (член 71, параграф 1 от ЗЗЛД).

([57]) „Предвидената цел“ е целта, за която са събрани личните данни. Например, когато личните данни се събират въз основа на съгласието на съответното физическо лице, предвидената цел е целта, която се съобщава на физическото лице съгласно член 15, параграф 2 от ЗЗЛД.

([58]) Вж. член 18, параграф 1 от ЗЗЛД. Нарушенията на член 18, параграфи 1 и 2 от ЗЗЛД могат да доведат до налагането на наказателни санкции (член 71, параграф 2 от ЗЗЛД).

([59]) Използването на лични данни или тяхното предоставяне на трета страна от доставчик на информационни и комуникационни услуги за цел, различна от първоначалната, може да се извърши само на основанията, посочени в член 18, параграф 2, точки 1 и 2 от ЗЗЛД (т.е. когато се получи допълнително съгласие или когато съществуват специални разпоредби по закон). Вж. член 18, параграф 2 от ЗЗЛД.

([60]) Освен когато обработването е необходимо за разследването на престъпления, повдигането на обвинение и наказателно преследване, от публичните институции, които използват лични данни или ги предоставят на трета страна за цел, различна от целта на събирането (например, когато това е изрично разрешено по закон или е необходимо за изпълнението на договор), се изисква да публикуват на своя уебсайт или в Официален вестник и да водят регистри за правните основания за обработването, за неговата цел и обхват (член 18, параграф 4 от ЗЗЛД и член 15 от Указа за прилагане на ЗЗЛД).

(42) Накрая, в член 28-2 от ЗЗЛД се разрешава (допълнително) обработване на псевдонимизирани данни без съгласието на съответното физическо лице за статистически цели, за научноизследователски цели ([61]) и за целите на архивирането в обществен интерес при наличие на конкретни гаранции. Следователно подобно на Регламент (ЕС) 2016/679 ([62]) ЗЗЛД улеснява (допълнително) обработването на лични данни за такива цели в рамка, в която са предвидени подходящи гаранции за защита на правата на физическите лица. Вместо да се разчита на псевдонимизацията като възможна гаранция, в ЗЗЛД тя е наложена като предварително условие за извършване на дейности по обработване за статистически цели, за научноизследователски цели и за целите на архивирането в обществен интерес (така че данните да могат да бъдат обработвани без съгласие или да се комбинират различни набори от данни).

(43) Освен това в ЗЗЛД са въведени редица конкретни гаранции, по-специално по отношение на задължителните технически и организационни мерки, воденето на регистри, ограниченията за споделянето на данни и справянето с евентуални рискове за повторна идентификация. Със съчетаването на различните гаранции, описани в съображения 44—48, се гарантира, че обработването на лични данни в този контекст е предмет на по същество равностойни защити в сравнение с тези, които биха се изисквали в съответствие с Регламент (ЕС) 2016/679.

(44) Първо и най-важно, в член 28-5, параграф 1 от ЗЗЛД се забранява обработването на псевдонимизирани данни с цел идентифициране на определено физическо лице. Ако по време на обработването на псевдонимизираните данни все пак се генерират данни, идентифициращи определено физическо лице, администраторът прекратява незабавно обработването на данните и ги унищожава (член 28-5, параграф 2 от ЗЗЛД). Неспазването на тези разпоредби подлежи на административни глоби и представлява престъпление ([63]). Това означава, че дори в тези ситуации, в които *на практика* е възможна повторна идентификация на физическото лице, има *законова* забрана за такава повторна идентификация.

(45) Второ, при (допълнително) обработване на псевдонимизирани данни за такива цели от администратора се изисква да въведе конкретни технологични, управленски и физически мерки, за да гарантира сигурността на данните (включително отделно съхранение и управление на данните, необходими за възстановяване на първоначалното състояние на псевдонимизираните данни) ([64]). Освен това трябва да се води документация за обработените псевдонимизирани данни, за целта на обработването, за историята на използването и за всички получатели трети страни (член 29-5, параграф 2 от Указа за прилагане на ЗЗЛД).

(46) Трето и последно, в ЗЗЛД са предвидени конкретни гаранции за предотвратяване на идентификацията на физически лица от трети страни в случай на споделяне на данните. По-конкретно, когато администраторите предоставят на трета страна псевдонимизирани данни за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес, те не могат да включват данни, които биха могли да бъдат използвани за идентифициране на конкретно физическо лице (член 28-2, параграф 2 от ЗЗЛД) ([65]).

(47) По-специално, макар че в ЗЗЛД се разрешава комбинирането на псевдонимизирани данни (обработени от различни администратори) за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес, това правомощие е запазено за специализирани институции, които разполагат със специални съоръжения в сферата на сигурността (член 28-3, параграф 1 от ЗЗЛД) ([66]). Когато кандидатства за комбиниране на псевдонимизирани данни, администраторът трябва да предостави, наред с другото, документация

([61]) Научните изследвания са определени в член 2, параграф 8 от ЗЗЛД като „изследвания, при които се използват научни методи, например технологично развитие и демонстрационни дейности, фундаментални научни изследвания, приложни научни изследвания и частно финансирани научни изследвания.“ Тези категории съответстват на посочените в съображение 159 от Регламент (ЕС) 2016/679.

([62]) Вж. член 5, параграф 1, буква б) и член 89, параграфи 1—2, както и съображения 50 и 157 от Регламент (ЕС) 2016/679.

([63]) Вж. член 28-6, параграф 1, член 71, параграф 4-3 и член 75, параграф 2, точка 4-4 от ЗЗЛД.

([64]) Вж. член 28-4 от ЗЗЛД и член 29-5 от Указа за прилагане на ЗЗЛД. Неспазването на това задължение подлежи на административни и наказателни санкции, вж. член 73, параграф 1 и член 75,параграф 2, точка 6 от ЗЗЛД.

([65]) Нарушенията на тези изисквания могат да доведат до налагането на наказателни санкции (член 71, параграф 2 от ЗЗЛД). Комисията за защита на личните данни започна незабавно да прилага тези нови правила, например в решението си от 28 април 2021 г., с което наложи глоба и коригиращи мерки на дружество, което, наред с другите нарушения на ЗЗЛД, не е спазило изискването на член 28-2, параграф 2 от ЗЗЛД, вж. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([66]) За да бъде определена като такава, съответната специализирана институция („Експертна агенция за комбиниране на данни“) трябва да подаде заявление до КЗЛД, заедно с подкрепящи документи, в които се описват подробно, наред с другото, наличните съоръжения и оборудване за безопасното комбиниране на псевдонимизирани данни и за потвърждение, че кандидатът използва поне трима служители на пълно работно време с квалификации или опит, свързани със защитата на личните данни (член 29-2, параграфи 1—2 от Указа за прилагане на ЗЗЛД). Подробни изисквания, например по отношение на квалификациите на персонала, наличните съоръжения, мерките за сигурност, вътрешните политики и процедури, както и финансовите изисквания, са установени в Уведомление 2020-9 на КЗЛД относно комбинирането и разкриването на псевдонимизирани данни (приложение I). Обозначението за експертна агенция за комбиниране на данни може да бъде отнето от КЗЛД (след провеждане на изслушване) на определени основания, например ако агенцията вече не отговаря на стандартите за сигурност, изисквани за определянето ѝ като такава, или ако е установено нарушение на сигурността на данните в контекста на комбинирането на данните (член 29-2, параграфи 5—6 от Указа за прилагане на ЗЗЛД). КЗЛД трябва да публикува всяко обозначение на експертна агенция за комбиниране на данни (или отнемането на този статут) (член 29-2, параграф 7 от Указа за прилагане на ЗЗЛД).

за данните, които ще бъдат комбинирани, за целта на комбинирането, както и за предложените мерки за сигурност при обработването на комбинираните данни ([67]). За да направи възможно комбинирането, администраторът трябва да изпрати на специализираната институция данните, които ще бъдат комбинирани, и да предостави „алгоритъм за комбиниране“ (т.е данните, които са били използвани за псевдонимизацията) на Корейската агенция за интернет и сигурност ([68]). Последната генерира „данни за връзка към алгоритъма за комбиниране“ (което позволява свързване на алгоритмите за комбиниране на различни кандидати, за да се постигне комбиниране на наборите от данни) и ги предоставя на специализираната институция ([69]).

(48) Администраторът, който иска комбиниране, може да анализира комбинираните данни в помещения на специализираната институция, в които се прилагат конкретни технически, физически и административни мерки (член 29-3 от Указа за прилагане на ЗЗЛД). Администраторите, които внасят набор от данни за такова комбиниране, могат да изнесат комбинираните данни извън специализираната институция само след допълнителна псевдонимизация или анонимизация на комбинираните данни и с одобрението на тази институция (член 28-3, параграф 2 от ЗЗЛД) ([70]). При разглеждане на искането за предоставяне на такова одобрение институцията ще оцени връзката между комбинираните данни и целта на обработването, както и дали е разработен конкретен план за сигурност за използването на тези данни ([71]). Изнасянето на комбинираните данни извън институцията не е разрешено, ако информацията съдържа данни, които ще позволят идентификацията на дадено физическо лице ([72]). Накрая, комбинирането и разкриването на псевдонимизирани данни от специализираната институция се извършва под надзора на КЗЛД (член 29-4, параграф 3 от Указа за прилагане на ЗЗЛД).

2.3.2. *Обработване на специални категории лични данни*

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

(50) В ЗЗЛД се съдържат специални правила за обработването на чувствителни данни ([73]), които са определени като лични данни, разкриващи информация относно идеологията, убежденията, присъединяването към или оттеглянето от синдикат или политическа партия, политическите мнения, здравето и сексуалния живот на дадено физическо лице, както и други лични данни, за които има вероятност да застрашат неприкосновеността на личния живот на субекта на данните „забележимо“ и които са определени като чувствителна информация с Президентски указ ([74]). Съгласно получените разяснения от КЗЛД тълкуването на сексуалния живот включва сексуалната ориентация или предпочитания на физическото лице ([75]). Освен това съгласно член 18 от Указа за прилагане в обхвата на чувствителните данни са добавени допълнителни категории, по-конкретно данни за ДНК, придобити от генетични изследвания, и данни, които представляват криминално досие. С последното изменение на Указа за прилагане на ЗЗЛД допълнително е разширено понятието за чувствителни лични данни с включването също така на лични данни, разкриващи расов или етнически произход и биометрични данни ([76]). След тази поправка понятието за чувствителни данни съгласно ЗЗЛД е равностойно по същество на това в член 9 от Регламент (ЕС) 2016/679.

(51) В съответствие с член 23, параграф 1 от ЗЗЛД и подобно на предвиденото в член 9, параграф 1 от Регламент (ЕС) 2016/679 обработването на чувствителни лични данни по принцип е забранено, освен ако се прилага едно от изброените изключения ([77]). В тези изключения обработването е сведено до случаи, в които администраторът информира субекта на данните в съответствие с членове 15 и 17 от ЗЗЛД и получава отделно съгласие

([67]) Член 8, параграфи 1—2 от Уведомление 2020-9 относно комбинирането и разкриването на псевдонимизирани данни.
([68]) Член 2, параграфи 3 и 6, и член 9, параграф 1 от Уведомление 2020-9 относно комбинирането и разкриването на псевдонимизирани данни.
([69]) Член 2, параграф 4, и член 9, параграфи 2—3 от Уведомление 2020-9 относно комбинирането и разкриването на псевдонимизирани данни. Специализираната институция трябва да унищожи незабавно данните за връзка към алгоритъма за комбиниране след комбинирането (член 9, параграф 4 от Уведомлението).
([70]) Нарушенията на изискванията за комбиниране на наборите от данни могат да доведат до налагането на наказателни санкции (член 71, параграф 4-2 от ЗЗЛД). Вж. също член 29-2, параграф 4 от Указа за прилагането на ЗЗЛД.
([71]) Процедурата за одобряване на разкриване на комбинираните данни е определена в член 11 от Уведомление 2020-9 относно комбинирането и разкриването на псевдонимизирани данни. По-конкретно специализираната институция трябва да създаде „комитет за преглед на разкриването“, състоящ се от членове със значителни знания и опит в областта на защитата на данните.
([72]) Вж. член 29-2, параграф 4 от Указа за прилагане на ЗЗЛД и член 11 от Уведомление № 2020-9.
([73]) Необходимостта да се предоставят специални защити при обработването на чувствителни лични данни, каквито са данните относно здравето или сексуалното поведение, е призната също така от корейския Конституционен съд, вж. Решение на Конституционния съд HunMa 1139 от 31 май 2007 г.
([74]) Член 23, параграф 1 от ЗЗЛД.
([75]) Вж. също Наръчник относно ЗЗЛД, глава III, раздел 2 относно член 23 (стр. 157—164).
([76]) Това означава лични данни, получени в резултат на специфично техническо обработване на лични данни, свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице, с цел уникалната идентификация на това физическо лице.
([77]) Неспазването на тези изисквания може да доведе до санкции съгласно член 71, точка 3 от ЗЗЛД.

(т.е. отделно от съгласието за обработването на други лични данни), или до такива, в които обработването се изисква или е разрешено по закон. Публичните органи могат също така да обработват биометрични данни, данни за ДНК, придобити от генетично изследване, лични данни, разкриващи расов или етнически произход, и данни, които представляват досие за съдимост, на основания, за които те имат изключителни правомощия (например, когато са необходими за разследването на престъпления или когато са необходими на съд за произнасяне по дело) ([78]). В този смисъл правните основания, свързани с обработването на чувствителни лични данни, са по-ограничени в сравнение с други видове лични данни и дори са по-ограничителни в корейското право, отколкото съгласно член 9, параграф 2 от Регламент (ЕС) 2016/679.

(52) Освен това в член 23, параграф 2 от ЗЗЛД — неспазване, което може да доведе до санкции ([79]) — се подчертава особената важност да се гарантира подходяща сигурност при боравенето с чувствителни лични данни, така че те „да не могат да бъдат загубени, откраднати, разкрити, подправени, изменени или повредени“. Макар че това е общо изискване съгласно член 29 от ЗЗЛД, в член 3, параграф 4 се пояснява, че нивото на сигурност трябва да бъде съобразено с вида на личните данни, които се обработват, което означава, че трябва да бъдат взети предвид конкретните рискове, свързани с обработването на чувствителни лични данни. Освен това обработването на данните винаги се извършва „по начин, който свежда до минимум възможността за нарушаване“ на неприкосновеността на личния живот на субекта на данните, и ако е възможно, „в режим на анонимност“ (член 3, параграфи 6 и 7 от ЗЗЛД). Тези изисквания са особено значими, когато обработването засяга чувствителни лични данни.

2.3.3. *Ограничаване в рамките на целта*

(53) Личните данни следва да се обработват с конкретна цел и по начин, който не е несъвместим с целта на обработването.

(54) Този принцип е залегнал в член 3, параграфи 1 и 2 от ЗЗЛД, според който администраторът „уточнява и посочва изрично“ целта на обработването, обработва личните данни по подходящ начин, необходим за целите, за които се обработват личните данни, и не ги използва извън тези цели. Общият принцип на ограничаване в рамките на целта се потвърждава също така в член 15, параграф 1, член 18, параграф 1, член 19 и — за обработващите лични данни (т.нар. „външни изпълнители“) — член 26, параграф 1, точки 1, 5 и 7 от ЗЗЛД. По-специално лични данни по принцип може да се използват и предоставят на трети страни само в рамките на обхвата на целта, за която се събират (член 15, параграф 1 и член 17, параграф 1, точка 2). Обработването за съпоставима цел, т.е. „в рамките на обхвата, свързан в разумна степен с целта на събирането“, може да се извършва само ако не засяга отрицателно съответните субекти на данни и при условие че са приложени съответните мерки за сигурност (например криптиране) (член 15, параграф 3 и член 17, параграф 4 от ЗЗЛД). За да се определи дали целта на обработването е съвместима цел, в Указа за прилагане на ЗЗЛД се посочват конкретни критерии, които са подобни на тези в член 6, параграф 4 от Регламент (ЕС) 2016/679, вж. съображение 36.

(55) Както е пояснено в съображение 38, целта на събирането на лични данни от корейските администратори, които ги получават от Съюза, е целта, за която са били предадени. Промяна на целта от администратора е разрешена само по изключение, в конкретни (изброени) случаи (член 18, параграф 2, точки 1—3 от ЗЗЛД, вж. също така съображение 39). Доколкото промяна на целта е разрешена по закон, тези закони на свой ред трябва да зачитат основното право на неприкосновеност на личния живот и на защита на личните данни, както и принципите на необходимост и пропорционалност, залегнали в корейската Конституция. Освен това в член 18, параграфи 2 и 5 от ЗЗЛД се предвиждат допълнителни гаранции, по-конкретно изискването промяната на целта да не „накърни несправедливо интереса на субекта на данните“, което винаги изисква балансиране на интересите. Това гарантира ниво на защита, което по същество е равностойно на нивото съгласно член 5, параграф 1, буква б) и член 6, във връзка със съображение 50 от Регламент (ЕС) 2016/679.

2.3.4. *Точност на данните и свеждане на данните до минимум*

(56) Личните данни следва да бъдат точни и при необходимост да се актуализират. Те следва също така да са целесъобразни, от значение за и ограничени до степента, необходима за целите, за които се обработват.

([78]) В член 18 от Указа за прилагане на ЗЗЛД се предвижда, че изброените в него категории данни са изключени от разпоредбата на член 23, параграф 1 от закона, когато се обработват от публична институция съгласно член 18, параграф 2, точки 5—9 от ЗЗЛД.
([79]) Вж. член 73, точка 1 и член 75, параграф 2, точка 6 от ЗЗЛД.

(57) Принципът на точността е отразен по подобен начин в член 3, параграф 3 от ЗЗЛД, в който се предвижда личните данни да са „точни, пълни и актуални до степента, необходима за целите“, за които се обработват данните. Свеждането на данните до минимум се изисква съгласно член 3, параграфи 1 и 6 и член 16, параграф 1 от ЗЗЛД, в които се предвижда администраторът да събира лични данни (само) „в минимално необходимата степен“ за предвидената цел, като той носи тежестта на доказване в това отношение. Ако е възможно целта на събирането да се изпълни чрез обработване на лични данни в анонимизирана форма, администраторите следва да се стремят да го извършват по този начин (член 3, параграф 7 от ЗЗЛД).

2.3.5. *Ограничение на съхранението*

(58) По принцип личните данни следва да се съхраняват не по-дълго от необходимото за целите, за които личните данни се обработват.

(59) По подобен начин принципът на ограничение на съхранението е предвиден в член 21, параграф 1 от ЗЗЛД ([80]), който изисква от администратора да „унищожи“ ([81]) личните данни незабавно след постигане на целта на обработването или след изтичане на срока на съхранение (в зависимост кое от тях настъпи по-рано), освен ако се изисква допълнително съхранение по закон ([82]). В последния случай съответните лични данни „се съхраняват и управляват отделно от другите лични данни“ (член 21, параграф 3 от ЗЗЛД).

(60) Член 21, параграф 1 от ЗЗЛД не се прилага, когато псевдонимизирани данни се обработват за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес ([83]). За да се гарантира принципът на ограничено съхранение на данните и в този случай, в Уведомление 2021-5 се изисква администраторите да анонимизират данните в съответствие с член 58-2 от ЗЗЛД, ако те не са били унищожени след изпълнението на конкретната цел на обработването ([84]).

2.3.6. *Сигурност на данните*

(61) Личните данни следва да се обработват по начин, който гарантира тяхната сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане. За тази цел стопанските субекти трябва да предприемат подходящи технически или организационни мерки за защита на личните данни от възможни заплахи. Тези мерки следва да се оценяват, като се вземат предвид достиженията на техническия прогрес, съответните разходи и естеството, обхватът, контекстът и целите на обработването, както и рисковете за правата на физическите лица.

(62) Сходен принцип на сигурността е заложен в член 3, параграф 4 от ЗЗЛД, в който администраторите се задължават да „управляват личните данни по безопасен начин в зависимост от методите на обработване, вида и др. на личните данни, като се вземат предвид възможността за нарушаване на правата на субекта на данните и сериозността на съответните рискове“. Освен това администраторът „обработва личните данни по начин, който свежда до минимум възможността за нарушаване на неприкосновеността на личния живот на субекта на данните“, и в този контекст се стреми да обработва личните данни в режим на анонимност или в псевдонимизирана форма, ако е възможно (член 3, параграфи 6 и 7 от ЗЗЛД).

(63) Тези общи изисквания са разгледани по-подробно в член 29 от ЗЗЛД, съгласно който всеки администратор „предприема технически, организационни и физически мерки, например разработване на вътрешен план за управление и запазване на записи в регистрационни файлове и др., които са необходими, за

([80]) Член 8 (във връзка с член 8-2 от Указа за прилагане), член 11 (във връзка с член 12, параграф 2 от Указа за прилагане).

([81]) Относно методите за унищожаване на лични данни вж. член 16 от Указа за прилагане на ЗЗЛД. В член 21, параграф 2 от ЗЗЛД се пояснява, че това включва „необходимите мерки за блокиране на възстановяването и възпроизвеждането“.

([82]) Неспазването на тези изисквания може да доведе до наказателни санкции (член 73, параграф 1-2 от ЗЗЛД). В член 39-6 от ЗЗЛД се предвижда допълнително изискване за доставчиците на информационни и комуникационни услуги да заличават личните данни на ползватели, които не са използвали предлаганите информационни и комуникационни услуги от поне една година (освен ако се изисква допълнително съхранение по закон или по искане на физическото лице). Физическите лица трябва да бъдат информирани за предвиждането заличаване на данните им 30 дни преди изтичането на едногодишния срок (член 39-6, параграф 2 от ЗЗЛД и член 48-5, параграф 3 от Указа за прилагане на ЗЗЛД). Ако се изисква допълнително съхранение по закон, съхранените данни трябва да бъдат съхранявани отделно от другите данни на ползвателите и могат да се използват или разкриват само в съответствие с този закон (член 48-5, параграфи 1—2 от Указа за прилагане на ЗЗЛД).

([83]) Член 28-7 от ЗЗЛД.

([84]) Уведомление 2021-5 (приложение I), раздел 4.

да се гарантира безопасността, предвидена в Президентския указ, така че личните данни да не могат да бъдат изгубени, откраднати, разкрити, подправени, променени или повредени.“ В член 30, параграф 1 от Указа за прилагане на ЗЗЛД се уточняват тези мерки, които включват (1) формулиране и прилагане на вътрешен план за управление с цел безопасно обработване на лични данни, (2) контрол и ограничения на достъпа, (3) прилагане на криптираща технология за безопасно съхранение и предаване на лични данни, (4) записи в регистрационни файлове, (5) програми за сигурност и (6) физически мерки, например система за безопасно съхранение или заключване ([85]).

(64) В допълнение се налагат специфични задължения, ако има нарушение на сигурността на данните (член 34 от ЗЗЛД във връзка с членове 39 и 40 от Указа за прилагане на ЗЗЛД) ([86]). По-специално администраторът трябва да уведоми незабавно засегнатите субекти на данните за подробностите относно нарушението ([87]), включително да им предостави информация за (задължителни) ответни мерки, предприети от администратора, както и какво може да бъде направено от субектите на данни за свеждане до минимум на риска от вреди (член 34, параграфи 1 и 2 от ЗЗЛД) ([88]). Когато нарушението на сигурността на данните засяга най-малко 1 000 субекта на данни, администраторът незабавно докладва за нарушението на сигурността на данните и за предприетите ответни мерки на КЗЛД и на Корейската агенция за интернет и сигурност, които могат да окажат техническа помощ (член 34, параграф 3 от ЗЗЛД във връзка с член 39 от Указа за прилагане на ЗЗЛД). Администраторите носят отговорност за вреда, настъпила вследствие на нарушения на сигурността на личните данни, в съответствие с разпоредбите на Гражданския закон за деликтната отговорност (вж. също така раздел 2.5 за средствата за правна защита) ([89]).

(65) При изпълнение на своите задължения за сигурност администраторът трябва да бъде подпомаган от служител по въпросите на поверителността, чиито задачи включват, наред с другото, изграждане на система за вътрешен контрол, „за да се предотвратят разкриването, злоупотребата и неправилното използване на лични данни“ (член 31, параграф 2, точка 4 от ЗЗЛД). Освен това администраторът има задължение да осъществява „подходящ контрол и надзор“ върху своите служители, които обработват лични данни, включително по отношение на тяхното безопасно управление; това включва необходимото обучение („образование“) на служители (член 28, параграфи 1 и 2 от ЗЗЛД). Накрая, в случай че администраторът възложи обработването на подизпълнител, той трябва да наложи изисквания на „външния изпълнител“, наред с другото, относно безопасното управление на личните данни („технически и управленски гаранции“) и да упражнява надзор върху изпълнението им чрез проверки (член 26, параграфи 1 и 4 от ЗЗЛД, във връзка с член 28, параграф 1, точки 3 и 4, и параграф 6 от Указа за прилагане на ЗЗЛД).

2.3.7. *Прозрачност*

(66) Субектите на данни следва да бъдат информирани за основните характеристики на обработването на техните лични данни.

([85]) Във връзка с обработването на лични данни от доставчиците на информационни и комуникационни услуги в член 39-5 от ЗЗЛД изрично се предвижда броят на лицата, които боравят с лични данни на ползвателите, да бъде сведен до минимум. Освен това доставчиците на информационни и комуникационни услуги трябва да гарантират, че личните данни на ползвателите няма да станат публично достояние чрез информационната и комуникационната мрежа (член 39-10, параграф 1 от ЗЗЛД). Станалите публично достояние данни трябва да бъдат заличени или блокирани по искане на КЗЛД (член 39-10, параграф 2 от ЗЗЛД). В по-общ план доставчиците на информационни и комуникационни услуги (и трети страни, които получават лични данни на ползватели) подлежат на допълнителни задължения за сигурност, посочени в член 48-2 от Указа за прилагане на ЗЗЛД, например разработване и прилагане на вътрешен план за управление по отношение на мерките за сигурност, мерките за гарантиране на контрол на достъпа, криптиране, използване на софтуер за откриване на зловреден софтуер и др.

([86]) В допълнение към това има обща забрана за увреждане, унищожаване, изменение, подправяне или изтичане на лични данни без законно правомощие, вж. член 59, точка 3 от ЗЗЛД.

([87]) Изискването за уведомяване на физическото лице не се прилага, когато има нарушение на защитата на личните данни по отношение на псевдонимизирани данни, обработени за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес (член 28-7 от ЗЗЛД, в който се предвижда освобождаване от прилагането на член 34, параграф 1 и член 39-4 от ЗЗЛД). Гарантирането на уведомяване на физическите лица би изисквало от съответния администратор да идентифицира физическите лица от псевдонимизирания набор от данни, което е изрично забранено съгласно член 28-5 от ЗЗЛД. Все пак общото изискване за уведомяване (на КЗЛД) относно нарушение на защитата на данни остава в сила.

([88]) Изискванията за уведомяване, включително моментът и възможността за „поетапно“ уведомяване, са уточнени допълнително в член 40 от Указа за прилагане на ЗЗЛД. По-строги правила се прилагат за доставчиците на информационни и комуникационни услуги, които трябва да уведомят субекта на данните и КЗЛД в срок до 24 часа след узнаването на факта, че лични данни са били изгубени, откраднати или са изтекли (член 39-4, параграф 1 от ЗЗЛД). Това уведомление трябва да включва подробности за личните данни, които са изтекли, момента, в който това се е случило, мерките, които могат да бъдат предприети от ползвателя, ответни мерки, приложени от доставчика, и данните за контакт на отдела, към който ползвателят може да адресира въпросите си (член 39-4, параграф 1, точки 1—5 от ЗЗЛД). Ако има основателна причина, например липса на данни за контакт на ползвателя, могат да се използват други средства за уведомяване, например чрез публикуване на информацията на уебсайт (член 39-4, параграф 1 от ЗЗЛД, във връзка с член 48-4, параграф 4 и сл. от Указа за прилагане на ЗЗЛД). В този случай КЗЛД трябва да бъде информирана за причините (член 34-4, параграф 3 от ЗЗЛД).

([89]) Вж. например решения на Върховния съд 2011Da59834, 2011Da59858 и 2011Da59841, 26 декември 2012 г. Резюме на английски език е достъпно на адрес: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Това се гарантира по различни начини в корейската система. Освен правото на информация съгласно член 4, точка 1 (по принцип) и член 20, параграф 1 от ЗЗЛД (за лични данни, събирани от трети страни), както и правото на достъп съгласно член 35 от ЗЗЛД, ЗЗЛД предвижда общо изискване за прозрачност относно целта на обработването (член 3, параграф 1 от ЗЗЛД) и специфични изисквания за прозрачност в случаите, когато обработването се основава на съгласие (член 15, параграф 2, член 17, параграф 2 и член 18, параграф 3 от ЗЗЛД) ([90]). Освен това в член 20, параграф 2 от ЗЗЛД се изисква определени администратори — тези, при които обработването надвишава определени прагове ([91]) — да уведомят субекта на данните, чиито лични данни са получили от трети страни, относно източника на информация, целта на обработването и правото на субекта на данните да иска преустановяване на обработването, освен ако уведомяването се окаже невъзможно поради липсата на данни за контакт. Изключения се прилагат за определени досиета с лични данни, поддържани от публични органи, по-конкретно досиета, които съдържат данни, обработени за целите на националната сигурност, поради други особено важни („сериозни“) национални интереси или за целите на прилагането на наказателното право, или когато има вероятност уведомлението да доведе до увреждане на живота или до телесна повреда на друго лице, или несправедливо да нанесе вреда върху имуществото и да накърни други интереси на друго лице, но само когато разглежданите публични или частни интереси са „явно по-висши“ пред правата на засегнатите субекти на данните (член 20, параграф 4 от ЗЗЛД). Това изисква балансиране на интересите.

(68) Освен това в член 3, параграф 5 от ЗЗЛД се предвижда администраторите да разкриват публично своята политика за поверителност (и други въпроси, свързани с обработването на лични данни). Това изискване е уточнено допълнително в член 30 от ЗЗЛД във връзка с член 31 от Указа за прилагане на ЗЗЛД. В съответствие с тези разпоредби публично оповестената политика за поверителност, наред с другото, трябва да включва информация за (1) видовете обработвани лични данни, (2) целта на обработването, (3) срока на съхранение, (4) дали личните данни са предоставени на трета страна ([92]), (5) дали обработването е възложено на подизпълнител, (6) информация за правата на субекта на данните и как да ги упражнява, и (7) данни за контакт (включително името на служителя по въпросите на поверителността или наименованието на вътрешния отдел, който отговаря за осигуряване на спазването на правилата за защита на личните данни и разглеждането на жалби). Политиката за поверителността трябва да бъде оповестена публично по такъв начин, че субектите на данните „да могат да я разпознаят лесно“ (член 30, параграф 2 от ЗЗЛД) ([93]), и трябва да се актуализира постоянно (член 31, параграф 2 от Указа за прилагане на ЗЗЛД).

(69) Публичните институции имат допълнително задължение да регистрират по-конкретно следната информация в КЗЛД: (1) наименованието на публичната институция, (2) основанията и целите за обработването на личните данни, (3) особеностите на регистрираните лични данни, (4) метода на обработването, (5) срока на съхранение, (6) броя на субектите на данни, чиито лични данни се съхраняват, (7) отдела, който разглежда исканията на субектите на данни, и (8) получателите на личните данни, когато данните се предоставят рутинно или повторно (член 32, параграф 1 от ЗЗЛД) ([94]). Регистрираните досиета с лични данни се разкриват публично от КЗЛД и трябва също така да бъдат посочени в политиката за поверителност на публичните институции (член 30, параграф 1 и член 32, параграф 4 от ЗЗЛД).

(70) За да се увеличи прозрачността за субектите на данни в Съюза, чиито лични данни се предават на Корея въз основа на настоящото решение, в раздел 3, подточки i) и ii) от Уведомление 2021-5 (приложение I) са предвидени допълнителни изисквания за прозрачност. Първо, при получаването на лични данни от Съюза въз основа на настоящото решение корейските администратори трябва да уведомят съответните субекти на данни без ненужно забавяне (и във всеки случай не по-късно от един месец след предаването) за името и данните за контакт на

([90]) По-специално, когато се обработват лични данни със съгласието на дадено физическо лице, администраторът трябва да информира физическото лице за целта на обработването, да посочи подробности за информацията, която ще се обработва, за получателя на личните данни, за срока, в който ще се съхраняват и използват личните данни, както и за факта, че физическото лице има право да откаже съгласие (и всички произтичащи от това недостатъци).

([91]) В съответствие с член 15-2, параграф 1 от Указа за прилагане на ЗЗЛД това засяга администратори, които обработват чувствителни лични данни на поне 50 000 субекти на данни, или „нормални“ лични данни на поне 1 милион субекти на данни. В член 15-2, параграф 2 от Указа за прилагане на ЗЗЛД се определят методите и моментът на уведомяването, а в член 15-2, параграф 3 се съдържа изискването за поддържане на съответна документация за него. Освен това специални правила се прилагат по отношение на определени категории доставчици на информационни и комуникационни услуги (тези, които са генерирали поне 10 милиарда вона от приходи от продажби за предходната година, или тези, които съхраняват/управляват лични данни на поне един милион ползватели средно за трите месеца преди края на предходната година), от които се изисква да уведомяват редовно ползвателите за използването на личните им данни, освен ако това се оказва невъзможно поради липсата на данни за контакт (член 39-8 от ЗЗЛД и член 48-6 от Указа за прилагане на ЗЗЛД).

([92]) Съгласно информацията, получена от корейското правителство, това включва задължение за индивидуално изброяване на получателя (получателите) в публично оповестената политика за поверителност.

([93]) Допълнителни условия са посочени в член 31, параграф 3 от Указа за прилагане на ЗЗЛД.

([94]) Изискването за регистрация не се прилага за определени видове досиета с лични данни, например тези, в които се отразяват въпроси, свързани с националната сигурност, дипломатически тайни, криминални разследвания, наказателно преследване, наказания, разследвания на престъпления, свързани с данъчно облагане, или досиета, които са свързани единствено с вътрешна оценка на представянето (член 32, параграф 2 от ЗЗЛД).

образуванията, които предават и получават информацията, за прехвърляните лични данни (или категории лични данни), за целта на събирането от корейския администратор, за срока на съхранение и за правата им съгласно ЗЗЛД. Второ, при предоставянето на трети страни на лични данни, получени от Съюза въз основа на настоящото решение, субектите на данни трябва да бъдат информирани, наред с другото, за получателя, за личните данни или за категориите лични данни, които ще се предоставят, за държавата, на която ще се предоставят данните (когато е приложимо), както и за правата им съгласно ЗЗЛД ([95]). По този начин с Уведомлението се гарантира, че физическите лица от ЕС ще продължат да бъдат информирани за конкретното обработване на техните данни от администраторите и ще са в състояние да упражняват правата си спрямо съответните образувания.

(71) В раздел 3, подточка iii) от уведомлението (приложение I) са предвидени определени ограничени и квалифицирани изключения от тези допълнителни задължения за прозрачност, които по същество са равностойни на изключенията, предвидени съгласно Регламент (ЕС) 2016/679. По-специално уведомяването на субектите на данни в Съюза не е задължително, (1) когато и доколкото е необходимо да се ограничи уведомяването по определени причини, свързани с обществения интерес (например когато информацията се обработва за целите на националната сигурност или за неприключили криминални разследвания), доколкото тези цели, свързани с обществения интерес, са с явно предимство пред правата на субекта на данните; (2) когато субектът на данните вече разполага с информацията; (3) когато и доколкото има вероятност уведомлението да доведе до увреждане на живота или до нанасяне на телесна повреда на това или друго лице или несправедливо да накърни имуществените интереси на друго лице, когато тези права или интереси имат явно предимство пред правата на субекта на данните; или (4) когато няма координати за връзка със засегнатите физически лица или са необходими непропорционални усилия за тяхното уведомяване. При определянето на това дали е възможно да се осъществи контакт със субекта на данните, или дали това е свързано с прекомерни усилия, се взема предвид възможността за сътрудничество с износителя на данни в Съюза.

(72) Следователно правилата в съображения 67—71 гарантират ниво на защита, което по същество е равностойно на нивото по отношение на прозрачността, предвидено в Регламент (ЕС) 2016/679.

2.3.8. *Индивидуални права*

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

(74) Съгласно член 3, параграф 5 от ЗЗЛД администраторът гарантира правата на субекта на данните, изброени в член 4 от ЗЗЛД и уточнени допълнително в членове 35—37, 39 и 39-2 от ЗЗЛД.

(75) Първо, физическите лица имат права на информация и достъп. Когато администраторът е събрал лични данни от трета страна — какъвто винаги ще бъде случаят при предаването на данни от Съюза — субектите на данните имат по принцип правото да получат информация относно 1) „източника“ на събраните лични данни (т.е. относно предаващия ги), 2) целта на обработването и 3) факта, че субектът на данните има право да поиска преустановяване на обработването (член 20, параграф 1 от ЗЗЛД). Прилагат се ограничени изключения, а именно когато има вероятност уведомлението да доведе до увреждане на живота или до телесна повреда на друго лице или несправедливо да нанесе вреда върху имуществото и да накърни други интереси на друго лице, но само когато тези права или интереси имат „явно предимство“ пред правата на субекта на данните (член 20, параграф 4, точка 2 от ЗЗЛД).

(76) В допълнение към това в член 35, параграфи 1 и 3 от ЗЗЛД, във връзка с член 41, параграф 4 от Указа за прилагане на ЗЗЛД, се дава право на достъп на субектите на данни до техните лични данни ([96]). Правото на достъп включва потвърждение за обработването, информация за вида на обработените данни, целта на обработването, срока на съхранение, всяко разкриване на трета страна, както и предоставянето на копие от обработените лични

([95]) Уведомление 2021-5, раздел 3, подточка ii) (приложение I).

([96]) Съгласно член 35, параграф 3 от ЗЗЛД, във връзка с член 42, параграф 2 от Указа за прилагане на ЗЗЛД, администраторът може да отложи достъпа по „основателна причина“ (т.е. на обосновани основания, например, ако е необходимо повече време да се направи оценка дали може да бъде предоставен достъп), но трябва да уведоми субекта на данните за това основание в срок до 10 дни и да му предостави информация как може да обжалва това решение; веднага след като основанието отпадне, трябва да му бъде предоставен достъп.

данни (член 4, точка 3 от ЗЗЛД във връзка с член 41, параграф 1 от Указа за прилагане на ЗЗЛД) ([97]). Достъпът може да бъде ограничен (частичен достъп) ([98]) или отказан само когато това се предвижда от закона ([99]), когато е вероятно да доведе до увреждане на живота или до телесна повреда на трета страна, или до необосновано увреждане на имуществото и на други интереси на друго лице (член 35, параграф 4 от ЗЗЛД) ([100]). Последното означава, че следва да има баланс между конституционно защитените права и свободи на физическото лице, от една страна, и на тези на други лица, от друга страна. Когато достъпът е ограничен или отказан, администраторът трябва да уведоми субекта на данните за основанията за това и за начините за обжалване на решението (член 41, параграф 5, член 42, параграф 2 от Указа за прилагане на ЗЗЛД).

(77) Второ, субектите на данни имат право на коригиране или изтриване ([101]) на техните лични данни, „освен ако специално е предвидено друго в други закони“ (член 36, параграфи 1 и 2 от ЗЗЛД) ([102]). При получаване на искане администраторът трябва да проучи въпроса незабавно, да предприеме необходимите мерки ([103]) и да уведоми субекта на данните за това в срок до 10 дни; когато искането не може да бъде удовлетворено, в изискването за уведомяване се посочват причините за отказа и как може да бъде обжалван (вж. член 36, параграф 4 от ЗЗЛД, във връзка с член 43, параграф 3 от Указа за прилагане на ЗЗЛД) ([104]).

(78) Накрая, субектите на данни имат правото обработването на личните им данни да бъде незабавно преустановено ([105]), освен ако се прилага едно от изброените изключения (член 37, параграфи 1 и 2 от ЗЗЛД) ([106]). Администраторът може да отхвърли искането за преустановяване, (1) когато това е специално предвидено в закон или е необходимо („неизбежно“) за спазването на законови задължения, (2) когато има вероятност преустановяването да доведе до увреждане на живота или до телесна повреда на трета страна, или до необосновано увреждане на имуществото и други интереси на друго лице, (3) когато би било невъзможно за публична институция да изпълни своя функция съгласно законовите предписания без обработването на лични данни, или (4) когато субектът на данните не прекрати изрично основния договор с администратора, макар че изпълнението на договора би било невъзможно без това обработване на лични данни. В този случай администраторът трябва незабавно да уведоми субекта на данните за причините за отказа и как може да го обжалва (член 37, параграф 2 от ЗЗЛД, във връзка с член 44, параграф 2 от Указа за прилагане на ЗЗЛД). Съгласно член 37, параграф 4 от ЗЗЛД администраторът трябва незабавно „да предприеме необходимите мерки, включително и за унищожаване на съответните лични данни“, в изпълнение на искането за преустановяване ([107]).

(79) Правото на преустановяване се прилага също така, когато лични данни се използват за целите на директния маркетинг, т.е. за да се рекламират стоки или услуги или за да се направи предложение за закупуването им. Освен това при допълнителното обработване обикновено се изисква специалното (допълнително) съгласие на субекта на данните (вж. член 15, параграф 1, точка 1, член 17, параграф 2, точка 1 от ЗЗЛД) ([108]). Когато иска такова съгласие, администраторът трябва да информира по-конкретно субекта на данните за предвидената

([97]) Достъп до лични данни, обработени от публична институция, може да бъде получен пряко от институцията или непряко с подаване на искане до КЗЛД, която препраща искането незабавно (член 35, параграф 2 от ЗЗЛД и член 41, параграф 3 от Указа за прилагане на ЗЗЛД).

([98]) В съответствие с член 42, параграф 1 от Указа за прилагане на ЗЗЛД администраторът е длъжен да предостави частичен достъп, когато поне част от информацията не е обхваната от основанията за отказ.

([99]) Този закон на свой ред трябва да зачита основното право на неприкосновеност на личния живот и на защита на личните данни, както и принципите на необходимост и пропорционалност, залегнали в корейската Конституция.

([100]) В допълнение публичните институции могат да откажат да предоставят достъп, ако това би довело до сериозни трудности за изпълнението на определени функции, включително текущи одити, или до налагането, събирането или погасяването на данъци (член 35, параграф 4 от ЗЗЛД).

([101]) В този случай администраторът трябва да предприеме мерки за предотвратяване на възстановяването на лични данни, вж. член 36, параграф 3 от ЗЗЛД.

([102]) Тези закони трябва да отговарят на изискванията на Конституцията, според която основно право може да бъде ограничавано само когато това е необходимо за националната сигурност или за поддържането на законността и реда за благото на обществото, и не може да се засяга същността на свободата или правото (член 37, параграф 2 от Конституцията).

([103]) В член 43, параграф 2 от Указа за прилагане на ЗЗЛД се предвижда специална процедура, в случай че администраторът обработва досиета с лични данни, предоставени от друг администратор.

([104]) Непредприемането на необходимите мерки за коригиране или изтриване на лични данни и продължаващото използване или предоставяне на тези данни на трета страна може да доведе до наказателни санкции (член 73, параграф 2 от ЗЗЛД).

([105]) Съгласно член 44, параграф 2 от Указа за прилагане на ЗЗЛД администраторът информира субекта на данните за факта, че е преустановил надлежно обработването в срок до 10 дни от получаването на искането.

([106]) По отношение на публичните институции правото на преустановяване на обработването може да бъде упражнено във връзка с данни, съдържащи се в регистрираните досиета с лични данни (член 37 във връзка с член 32 от ЗЗЛД). Регистрирането не е задължително в ограничен брой ситуации, например когато досиетата с лични данни са свързани с националната сигурност, с криминални разследвания, с дипломатически отношения и др. (член 32, параграф 2 от ЗЗЛД).

([107]) Непреустановяването на обработването може да доведе до наказателни санкции (член 73, параграф 3 от ЗЗЛД).

([108]) Комитетът за медиация при спорове (вж. съображение 133) е разгледал няколко случая, в които физически лица са се оплакали относно използването на техните данни за целите на директния маркетинг без съгласието им, което е довело например до изплащането на обезщетение и заличаването на лични данни от съответния администратор на лични данни (вж. например решения 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1) на Комитета за медиация при спорове).

употреба на данните за целите на директния маркетинг — т.е. за факта, че с него може да бъде осъществена връзка за рекламиране на стоки или услуги или за отправяне на предложение за закупуването им — по „изрично разпознаваем начин“ (член 22, параграфи 2 и 4 от ЗЗЛД, във връзка с член 17, параграф 2, точка 1 от Указа за прилагане на ЗЗЛД).

(80) За да улесни упражняването на индивидуалните права, администраторът трябва да установи специални процедури и да ги обяви публично (член 38, параграф 4 от ЗЗЛД) ([109]). Това включва процедури за подаване на възражения срещу отказа на искане (член 38, параграф 5 от ЗЗЛД). Администраторът трябва да гарантира, че процедурата за упражняване на права е „лесна за използване от субекта на данните“ и не е по-затрудняваща от процедурата за събирането на личните данни; това включва също така задължението да предостави информация за процедурата на своя уебсайт (член 41, параграф 2, член 43, параграф 1 и член 44, параграф 1 от Указа за прилагане на ЗЗЛД) ([110]). Физическите лица могат да упълномощят представител да подаде такова искане (член 38, параграф 1 от ЗЗЛД във връзка с член 45 от Указа за прилагането на ЗЗЛД). Доколкото администраторът има право да изиска заплащането на такса (и в случай на искане да изпрати копия на личните данни по пощата — пощенска такса), сумата трябва да бъде определена „в рамките на действителните разходи, необходими за обработването на [искането]“; не може да се изисква заплащането на такса (нито на пощенска такса), когато администраторът е отправил искането (член 38, параграф 3 от ЗЗЛД, във връзка с член 47 от Указа за прилагане на ЗЗЛД).

(81) ЗЗЛД и Указът за неговото прилагане не съдържат общи разпоредби, уреждащи въпроса за решенията, засягащи субекта на данни и основаващи се единствено на автоматизираното обработване на лични данни. Във всеки случай, що се отнася до лични данни, събрани в Съюза, всяко решение, което се основава на автоматизирано обработване, обикновено се взема от администратора на данни в Съюза (който е в пряка връзка със засегнатия субект на данни) и по този начин се подчинява на разпоредбите на Регламент (ЕС) 2016/679 ([111]). Това включва сценарии за предаване, в които обработката се извършва от чужд (например корейски) стопански субект, действащ като представител (обработващ лични данни) на администратора на данни в Съюза (или като подизпълнител, действащ от името на обработващ лични данни от Съюза, който е получил данните от администратора на данни от Съюза, който ги е събрал), който на това основание впоследствие взема решението. Следователно липсата на конкретни правила относно автоматизираното вземане на решения в ЗЗЛД е малко вероятно да се отрази върху равнището на защита на личните данни, предавани съгласно настоящото решение.

(82) По изключение разпоредбите за спазване на прозрачността при отправено искане (член 20) и индивидуалните права (членове 35—37), както и изискването за индивидуално уведомяване по отношение на доставчиците на информационни и комуникационни услуги (член 39-8 от ЗЗЛД) не се прилагат по отношение на псевдонимизирани данни, обработени за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес (член 28-7 от ЗЗЛД) ([112]). В съответствие с подхода, посочен в член 11, параграф 2 (във връзка със съображение 57) от Регламент (ЕС) 2016/679, това е обосновано от факта, че за да гарантира прозрачност или да предостави индивидуални права, администраторът ще трябва да установи дали (и ако да, кои) данни са свързани с физическото лице, отправило искането, което е изрично забранено съгласно ЗЗЛД (член 28-5, параграф 1 от ЗЗЛД). Освен това, когато тази повторна идентификация включва премахване на псевдонимизацията за целия набор от (псевдонимизирани) данни, това би изложило на повишени рискове личните данни на всички останали засегнати физически лица. Докато Регламент (ЕС) 2016/679 се отнася до ситуации, при които повторната идентификация е практически невъзможна, в ЗЗЛД е възприет по-строг подход чрез строга забрана на повторната идентификация във всички ситуации, в които се обработват псевдонимизирани данни.

(83) Корейската система, описана в съображения 74—82 следователно съдържа правила за правата на субектите на данни, които осигуряват ниво на защита, равностойно по същество на нивото съгласно Регламент (ЕС) 2016/679.

([109]) Вж. също член 30, параграф 1, точка 5 от ЗЗЛД относно политиката за поверителност, която наред с другото трябва да съдържа информация за правата на физическото лице и за начина на тяхното упражняване.

([110]) Вж. също член 39-7, параграф 2 от ЗЗЛД във връзка с доставчиците на информационни и комуникационни услуги.

([111]) И обратно, в изключителния случай, в който корейският стопански субект е в пряка връзка със субекта на данни от ЕС, това обикновено ще е в резултат от това, че стопанският субект е насочил дейността си към лицето в Европейския съюз, предлагайки му стоки или услуги или наблюдавайки неговото поведение. При този сценарий самият корейски стопански субект ще попадне в приложното поле на Регламент (ЕС) 2016/679 (член 3, параграф 2) и следователно трябва да спазва непосредствено правото на ЕС в областта на защитата на данните.

([112]) Вж. също Уведомление 2021-5, в което се потвърждава, че Раздел III от ЗЗЛД (включително член 28-7) се прилага само когато псевдонимизирани данни се обработват за научноизследователски цели, за статистически цели или за целите на архивирането в обществен интерес, вж. раздел 4 от приложение I към настоящото решение.

2.3.9. *Последващо предаване*

(84) Нивото на защита на личните данни, което се осигурява за личните данни, предавани от Съюза към администратори в Република Корея, не трябва да бъде подкопавано от по-нататъшното предаване на тези данни към получатели в трета държава.

(85) Това „последващо предаване“ представлява международно предаване от Република Корея от гледна точка на корейския администратор на лични данни. В това отношение в ЗЗЛД се прави разграничение между възлагането на обработването на външен изпълнител (т.е. обработващ лични данни) и предоставянето на лични данни на трети страни ([113]).

(86) Първо, когато обработването на лични данни е възложено на външен изпълнител, който е образувание, намиращо се в трета държава, корейският администратор трябва да осигури спазването на разпоредбите на ЗЗЛД за възлагане на обработването на външен изпълнител (член 26 от ЗЗЛД). Това включва въвеждането на правно обвързващ инструмент, с който наред с другото обработването от външния изпълнител се ограничава до рамките на целта на възложената му работа, налагат се технически и управленски гаранции и се ограничава възлагането на подизпълнител (вж. член 26, параграф 1 от ЗЗЛД); както и публикуването на информация за възложената на външен изпълнител работа. Освен това администраторът има задължение да „образова“ външния изпълнител относно необходимите мерки за сигурност и да упражнява надзор, включително чрез проверки на място, относно спазването на всички задължения на администратора съгласно ЗЗЛД ([114]), както и съгласно договора за възлагане на дейност на външен изпълнител.

(87) Ако външният изпълнител причини вреда, свързана с обработването на лични данни в нарушение на ЗЗЛД, тя се приписва на администратора за целите на отговорността, както когато вредата е причинена от служителите на администратора (член 26, параграф 6 от ЗЗЛД). Корейският администратор продължава да носи отговорност за личните данни, които са били предоставени за обработване на външен изпълнител, и трябва да гарантира, че задграничният обработващ ги обработва в съответствие със ЗЗЛД. Ако външният изпълнител обработва личните данни в нарушение на ЗЗЛД, корейският администратор носи отговорност за неспазването на своето задължение да гарантира съответствие със ЗЗЛД, например чрез надзор върху външния изпълнител. Гаранциите, включени в договора за възлагане на обработването на лични данни на външен изпълнител, и отговорността на корейския администратор за действията на външния изпълнител гарантират непрекъснатост на защитата при възлагане на обработването на лични данни на външен изпълнител, който е образувание извън Корея.

(88) Второ, корейските администратори може да предоставят лични данни на трета страна, намираща се извън Корея. Макар че в ЗЗЛД са включени редица правни основания, предвиждащи по принцип предоставянето на лични данни на трети страни, ако третата страна се намира извън Корея, администраторът по принцип ([115]) трябва да получи съгласието на субекта на данните ([116]), след като му е предоставил информация (1) за вида на личните данни, (2) за получателя на личните данни, (3) за целта на предаването във връзка със смисъла на целта на обработването, преследвана от получателя, (4) за периода на обработване от получателя, както и (5) за факта, че субектът на данните може да откаже да даде съгласието си (член 17, параграфи 2 и 3 от ЗЗЛД). В Уведомление 2021-5 в раздела за прозрачността (вж. съображение 70) се предвижда физическите лица да бъдат информирани коя е третата държава, на която ще бъдат предоставени техните данни. Това гарантира, че субектите на данни в Съюза могат да вземат напълно информирано решение дали да се съгласят с предоставянето на данните им в трета държава. Освен това администраторът не може да сключва договор с третата страна получател в нарушение на ЗЗЛД, което означава, че договорът не трябва да съдържа определени задължения, които биха били в противоречие с наложените на администратора изисквания съгласно ЗЗЛД ([117]).

([113]) Специални правила се прилагат за доставчиците на информационни и комуникационни услуги. В съответствие с член 39-12 от ЗЗЛД доставчиците на информационни и комуникационни услуги трябва по принцип да получат съгласието на ползвателя за всяко предаване на лични данни. В случай че лични данни се предават като част от предоставяне на операции по обработване на външен изпълнител, включително за съхранение, не се изисква съгласие, ако съответните физически лица са информирани предварително, пряко или чрез публично известие, по начин, който позволява лесен достъп, за (1) конкретните данни, които ще се предават, (2) държавата, към която ще бъдат предадени данните (както и за датата и начина на предаване), (3) името на получателя и (4) целта на употребата и запазването им от получателя (член 39-12, параграф 3 от ЗЗЛД). В допълнение към това в този случай приложими са общите изисквания за възлагане на външен изпълнител. За всяко предаване трябва да бъдат прилагани конкретни гаранции по отношение на сигурността, разглеждането на жалби и спорове, както и други мерки, необходими за защита на данните на ползвателите (член 48-10 от Указа за прилагане на ЗЗЛД).

([114]) Вж. също така член 26, параграф 7 от ЗЗЛД, съгласно който членове 15—25, 27—31, 33—38 и 50 се прилагат *mutatis mutandis* за обработващия лични данни.

([115]) В случай на предоставяне на третата страна на лични данни на ползватели от доставчиците на информационни и комуникационни услуги това винаги изисква съгласието на ползвателя (член 39-12, параграф 2 от ЗЗЛД).

([116]) Както е обяснено по-подробно в бележка под линия 51, за да бъде валидно, съгласието трябва да бъде свободно дадено, информирано и конкретно.

([117]) Вж. също член 39-12, параграф 1 от ЗЗЛД във връзка с доставчиците на информационни и комуникационни услуги.

(89) Без съгласието на физическото лице лични данни могат да бъдат предоставяни на трета страна (в трета държава), когато целта на разкриването продължава да бъде „разумно свързана в рамките на обхвата“ с първоначалната цел на събирането (член 17, параграф 4 от ЗЗЛД, вж. съображение 36). При вземане на решение за разкриване (или неразкриване) на лични данни за „свързана“ цел обаче администраторът трябва да прецени дали разкриването ще доведе до неблагоприятни последствия за физическото лице и дали са взети необходимите мерки за сигурност (например криптиране). Като се има предвид, че третата държава, на която ще бъдат предадени личните данни, може да не предлага защити, подобни на предоставените съгласно ЗЗЛД, в раздел 2 от Уведомление 2021-5 се посочва, че е възможно да възникнат такива последствия и те могат да бъдат избегнати само ако корейският администратор и задграничният получател гарантират, чрез правно обвързващ инструмент (например договор), ниво на защита, което е равностойно на ЗЗЛД, включително по отношение на правата на субектите на данните.

(90) Специални правила се прилагат по отношение на „несвързано с целта“ разкриване, т.е. предоставяне на данни на трета страна за нова (несвързана) цел, което може да се извърши на едно от основанията в член 18, параграф 2 от ЗЗЛД, описани в съображение 39. Дори и при тези условия обаче предоставянето на лични данни на трета страна е изключено, ако има вероятност това „да накърни несправедливо“ интересите на субекта на данните или на трета страна, което налага балансиране на интересите. В допълнение към това в член 18, параграф 5 от ЗЗЛД от администратора се изисква да приложи допълнителни гаранции, които може да включват искане до третата страна да ограничи целта и начина на обработването или да приложи специални мерки за сигурност. Отново, като се има предвид, че третата държава, на която ще се предават личните данни, може да не предлага защити, подобни на предоставените съгласно ЗЗЛД, в раздел 2 от Уведомление 2021-5 се посочва, че може да възникне такова „несправедливо нарушение“ на интересите на физическото лице или на трета страна, и това може да бъде избегнато само ако корейският администратор и задграничният получател гарантират, чрез правно обвързващ инструмент (например договор), ниво на защита, което е равностойно на ЗЗЛД, включително по отношение на правата на субектите на данните.

(91) Следователно правилата в съображения 86—90 гарантират непрекъснатост на защитата при последващо предаване на лични данни (на „външен изпълнител“ или на трета страна) от Република Корея по начин, който по същество е равностоен на предвидения в Регламент (ЕС) 2016/679.

2.3.10. *Отчетност*

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

(93) Съгласно член 3, параграфи 6 и 8 от ЗЗЛД администраторът трябва да обработва личните данни „така че да сведе до минимум възможността за нарушение“ на неприкосновеността на личния живот на субекта на данните и да се опита да получи доверието му чрез съблюдаване и изпълнение на задълженията и отговорностите си, предвидени в ЗЗЛД и в други свързани закони. Това включва създаването на вътрешен план за управление (член 29 от ЗЗЛД), както и подходящо обучение и надзор на персонала (член 28 от ЗЗЛД).

(94) Като начин за гарантиране на отчетността в член 31 от ЗЗЛД, във връзка с член 32 от Указа за прилагане на ЗЗЛД, на администраторите се вменява задължение да определят служител по въпросите на поверителността, който „поема всеобхватна отговорност за обработването на личните данни“. По-специално той е натоварен да изпълнява следните функции: (1) създаване и прилагане на план за защита на личните данни и съставяне на политика за поверителност, (2) извършване на редовни проучвания за състоянието и практиките за обработване на лични данни с цел отстраняване на недостатъците, (3) разглеждане на жалби и обезщетения за вреди, (4) създаване на система за вътрешен контрол с цел предотвратяване на разкриването, злоупотребата или неправилната употреба на лични данни, (5) изготвяне и прилагане на образователна програма, (6) защита, контрол и управление на досиетата с лични данни и (7) унищожаване на личните данни след постигане на целта на обработването им или след изтичане на срока на тяхното съхранение. При изпълнението на тези задължения служителят по въпросите на поверителността може да проверява състоянието на обработването на лични данни и свързаните системи и да иска съответна информация за тях (член 31, параграф 3 от ЗЗЛД). Ако служителят по въпросите на поверителността установи нарушение на ЗЗЛД или на други свързани закони за защита на данните, той незабавно предприема корективни мерки и докладва за тях на ръководството („ръководителя“) на администратора, ако е необходимо (член 31, параграф 4 от ЗЗЛД). Съгласно член 31, параграф 5 от ЗЗЛД за служителя по въпросите на поверителността не трябва да има неоснователни последствия като резултат от изпълнението на тези функции.

(95) В допълнение администраторите трябва активно да се опитват да направят оценка на въздействието върху неприкосновеността на личния живот, когато работата с досиетата с лични данни носи риск за неприкосновеността на личния живот (член 33, параграф 8 от ЗЗЛД). Въз основа на член 33, параграфи 1 и 2 от ЗЗЛД, във връзка с членове 35, 36 и 38 от Указа за прилагане на ЗЗЛД, фактори, като вида и естеството на обработените данни (по-конкретно дали представляват чувствителни лични данни), техния обем, срока на съхранение и вероятността от нарушаване на защитата на данните, ще бъдат от значение за оценката на степента на риска за правата на субектите на данни. Целта на оценката на въздействието върху неприкосновеността на личния живот е да се гарантира, че са анализирани рисковите фактори за неприкосновеността на личния живот, както и мерките за безопасност или противодействие, и да се посочат въпросите, които се нуждаят от подобрение (вж. член 33, параграф 1 от ЗЗЛД, във връзка с член 38 от Указа за прилагане на ЗЗЛД).

(96) Публичните институции имат задължение да извършват оценка на въздействието върху неприкосновеността на личния живот, когато обработват определени досиета с лични данни, свързани с по-висок риск от нарушения на неприкосновеността на личния живот (член 33, параграф 1 от ЗЗЛД). В съответствие с член 35 от Указа за прилагане на ЗЗЛД, наред с другото, такъв е случаят на досиета, които съдържат чувствителни лични данни на поне 50 000 субекта на данни, досиета, които при съпоставяне с други досиета и в резултат от това ще съдържат данни на поне 500 000 субекта на данни, или досиета, които съдържат данни на поне един милион субекта на данни. Резултатът от оценката на въздействието върху неприкосновеността на личния живот трябва да бъде съобщен на КЗЛД (член 33, параграф 1 от ЗЗЛД), която може да изрази становище (член 33, параграф 3 от ЗЗЛД).

(97) Накрая, в член 13 от ЗЗЛД се предвижда КЗЛД да разработи необходимите политики за насърчаване и подкрепа на „саморегулиращи се дейности за защита на данните“ от страна на администраторите, наред с другото, чрез обучение за защита на данните, чрез насърчаване и подкрепа на организации, занимаващи се със защита на данните, и чрез подпомагане на администраторите в създаването и внедряването на правила за саморегулация. Освен това тя трябва да въведе и посредничи при използването на системата ePRIVACY Mark. В това отношение в член 32-2 от ЗЗЛД във връзка с членове 34-2—34-8 от Указа за прилагане на ЗЗЛД се предвижда възможност за сертифициране, че обработването на лични данни от даден администратор и защитната(ите) му система(и) съответстват на изискванията на ЗЗЛД. Съгласно тези правила може да бъде предоставено сертифициране ([118]) (за период от 3 години), ако администраторът отговаря на критериите за сертифициране, определени в ЗЗЛД, включително по отношение на наличието на управленски, технически и физически гаранции за защита на личните данни ([119]). Комисията за защита на личните данни трябва да проверява системите на администратора във връзка със сертифицирането поне веднъж годишно с цел поддържане на неговата ефективност, което може да доведе до отнемане на сертифицирането (член 32, параграф 4 от ЗЗЛД във връзка с член 34-5 от Указа за прилагане на ЗЗЛД; т.нар. „проследяващо управление“).

(98) Следователно в корейската уредба принципът на отчетност се прилага по начин, който гарантира ниво на защита, равностойно по същество на нивото в Регламент (ЕС) 2016/679, включително чрез осигуряване на различни механизми за гарантиране и доказване на съответствие със ЗЗЛД.

2.3.11. *Специални правила за обработването на лична кредитна информация*

(99) Както е описано в съображение 13, в ЗКИ се предвиждат специфични правила за обработването на кредитна информация от търговски оператори. Следователно при обработването на лична кредитна информация търговските оператори трябва да спазват общите изисквания на ЗЗЛД, освен ако ЗКИ съдържа по-специфични правила. Такъв е случаят например, когато те обработват информация, свързана с кредитна карта или банкова сметка в контекста на търговска операция с физическо лице. Като секторно законодателство за обработването на кредитна информация (както лична, така и нелична) в ЗКИ не само са предвидени специфични гаранции за защита на данните (например по отношение на прозрачността и сигурността), но като цяло са регламентирани конкретните обстоятелства, при които може да се обработва лична кредитна информация. По-специално това е отразено в подробните изисквания за използването, предоставянето на данни на трета страна и за запазването на такива данни.

(100) Подобно на ЗЗЛД в ЗКИ е отразен принципът на законосъобразността и пропорционалността. Първо, като общо изискване в член 15, параграф 1 от ЗКИ се разрешава събирането на лична кредитна информация само с разумни и добросъвестни средства и в най-малката степен, необходима за постигането на определена цел, в съответствие с член 3, параграфи 1—2 от ЗЗЛД. Второ, в ЗКИ по-конкретно се урежда законосъобразността на обработването на лична кредитна информация чрез ограничаване на нейното събиране, употреба и предоставяне на трета страна и като цяло обвързването на дейностите по обработването ѝ с изискването за съгласие от засегнатото лице.

([118]) В допълнение, ако администраторът възнамерява да се позовава или да насърчава сертифицирането в своите стопански операции, той може да използва знак за защита на личните данни, определен от КЗЛД. Вж. член 34-7 от Указа за прилагане на ЗЗЛД.

([119]) От ноември 2018 г. е разработена „Система за управление на личните данни и сигурността на информацията“ (ISMS-P) за сертифициране на администратори, които използват комплексна система за управление.

(101) Личната кредитна информация може да бъде събирана на някое от основанията, предвидени в ЗЗЛД, или на специфични основания, определени в ЗКИ. С оглед на това, че член 45 от Регламент (ЕС) 2016/679 предполага предаване на лични данни от администратор или обработващ лични данни в Съюза, но не обхваща пряко събиране (например от физическото лице или от уебсайт) от администратор на лични данни в Корея, от значение за настоящото решение са само съгласието и основанията, предвидени в ЗЗЛД. Тези основания включват по-конкретно сценарии, при които предаването е необходимо за изпълнението на договор с физическото лице или във връзка с легитимните интереси на корейския администратор на лични данни (член 15, параграф 1, точки 4 и 6 от ЗЗЛД) ([120]).

(102) След като бъде събрана, личната кредитна информация може да се използва (1) за първоначалната цел, за която е била (пряко) предоставена от физическото лице ([121]); (2) за цел, която е съвместима с първоначалната цел на събирането ([122]); (3) за да се определи дали да се създаде или поддържа търговско взаимоотношение, поискано от физическото лице ([123]); (4) за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес ([124]), ако информацията е псевдонимизирана ([125]); (5) ако бъде получено допълнително съгласие или (6) в съответствие със закона.

(103) Ако търговски оператор възнамерява да разкрие лична кредитна информация на трета страна, той трябва да получи съгласието на физическото лице ([126]), след като го информира за получателя на данните, за целта на обработването им от получателя, за елементите на данните, които ще бъдат предоставени, за срока на съхранение от получателя и за правото на отказ за даване на съгласие (член 32, параграф 1 от ЗКИ и член 28, параграф 2 от Указа за прилагане на ЗКИ) ([127]). Изискването за съгласие не се прилага в някои специфични ситуации, а именно когато личната кредитна информация се разкрива ([128]): (1) на външен изпълнител за целите на възлагането на дейности на външен изпълнител ([129]); (2) на трета страна в случай на прехвърляне, разделяне или сливане на предприятия; (3) за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес, когато информацията е псевдонимизирана; (4) за цел, която е съвместима с първоначалната цел на събирането; (5) на трета страна, която използва информацията за събирането на дълг, дължим от физическото лице ([130]); (6) в изпълнение на

([120]) В ЗКИ се съдържат и други основания за събиране, т.е. когато то се изисква по закон, когато публична институция е оповестила публично информацията съгласно законодателството за свобода на информацията или когато информацията е достъпна в социалната мрежа. За да може търговският оператор да се позове на последното основание, той трябва да е в състояние да докаже, че събирането остава в обхвата на съгласието на субекта на данните въз основа на разумно („обективно“) тълкуване и при отчитане на естеството на данните, на намерението и на целта на предоставянето на достъп до тях в социалната мрежа, както и дали целта на събирането е „от важно значение“ за тази цел и т.н. (член 13 от Указа за прилагане на ЗКИ). Както е обяснено в съображение 101 обаче, тези основания по принцип не са от значение при сценарий с предаване на данни.

([121]) Например, когато кредитна информация е генерирана/предоставена в контекста на търговска операция с физическото лице. Не е възможна употребата на лична кредитна информация обаче за целите на директния маркетинг (вж. член 33, параграф 1, точка 3 от ЗКИ).

([122]) За да се определи дали целта на употребата е съвместима с първоначалната цел на събирането, трябва да се вземат предвид следните фактори: 1) взаимоотношението („относимостта“) между двете цели; 2) начинът, по който е била събрана информацията; 3) въздействието на употребата ѝ върху физическото лице и 4) дали са взети подходящи мерки за сигурност, като например псевдонимизация (вж. член 32, параграф 6, точка 9-4 от ЗКИ).

([123]) Например даден администратор може да вземе предвид лична кредитна информация, която е получил от физическо лице, за да реши дали да удължи срока на заема за това физическо лице.

([124]) Член 33 от ЗКИ, във връзка с член 32, параграф 6, точки 9-2, 9-4 и 10 от ЗКИ.

([125]) Псевдонимизацията се определя в член 2, параграф 15 като обработване на лична кредитна информация по начин, по който физическите лица вече не могат да бъдат идентифицирани от информацията, освен в комбинация с допълнителна информация. Въпреки че ЗКИ съдържа специфични гаранции за обработването на псевдонимизирана информация за статистически цели, за научноизследователски цели и за целите на архивирането в обществен интерес (член 40-2 от ЗКИ), тези правила не се прилагат за търговските организации. Вместо това спрямо тях продължават да се прилагат специфичните изисквания на раздел III от ЗЗЛД, както е описано в съображения 42—48. Освен това съгласно член 40-3 от ЗКИ обработването на псевдонимизирана кредитна информация е изключено — когато се извършва за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес — от изискванията за прозрачност и индивидуални права, подобно на изключението в член 28-7 от ЗЗЛД и при спазване на гаранциите в раздел III от ЗЗЛД, както е описано по-подробно в съображения 42—48.

([126]) Това не важи, когато информацията се предоставя на трета страна с цел да се поддържа личната кредитна информация точна и актуална, доколкото предоставянето ѝ остава в рамките на първоначалната цел на обработването (член 32, параграф 1 от ЗКИ). Например това може да се случи, когато актуална информация се предоставя на агенция за кредитен рейтинг, за да се гарантира точността на съхраняваните от нея данни.

([127]) Ако е невъзможно да се предостави горепосочената информация, може да е достатъчно да се посочи физическото лице на третата страна получател във връзка с изискваната информация.

([128]) Като се има предвид, че ЗКИ не съдържа специални разпоредби относно задграничните разкривания на лична кредитна информация, тези разкривания трябва да съответстват на гаранциите за последващо предаване, предвидени в раздел 2 от Уведомление № 2021-5.

([129]) Възлагането на обработването на лична кредитна информация на външен изпълнител може да се извърши само въз основа на писмен договор и в съответствие с изискванията на член 26, параграфи 1—3 и 5 от ЗЗЛД, както е описано в съображение 20 (член 17 от ЗКИ и член 14 от Указа за прилагане на ЗКИ). Външният изпълнител не може да използва информацията извън обхвата на възложените задължения, а възлагащото дружество трябва да въведе специални изисквания за сигурност (например криптиране) и да обучи външния изпълнител за това как да предотврати загубата, кражбата, разкриването, промяната или компрометирането на кредитната информация.

([130]) Вж. също член 28, параграф 10, точки 1, 2 и 6 от Указа за прилагане на ЗКИ.

съдебно разпореждане; (7) на прокурор/съдебен полицейски служител в спешна ситуация, когато животът на физическото лице е в опасност или се очаква то да получи телесна повреда и няма време за издаване на съдебна заповед ([131]); (8) на компетентните данъчни органи за спазване на данъчните закони; или (9) в съответствие с други закони. В случай на разкриване на едно от тези основания субектът на данните трябва да бъде уведомен за това предварително (член 32, параграф 7 от ЗКИ).

(104) В ЗКИ по-конкретно се урежда също така продължителността на обработването на личната кредитна информация на едно от основанията за използването или предоставянето ѝ на трета страна след края на търговското взаимоотношение с физическото лице ([132]). Само информация, която е била необходима за създаването или поддържането на взаимоотношението, може да бъде съхранявана, при спазване на допълнителни гаранции (да бъде отделена от кредитната информация, свързана с физически лица, с които търговското взаимоотношение продължава, да бъде защитена със специални мерки за сигурност и да бъде достъпна само за упълномощени физически лица) ([133]). Всички други данни трябва да бъдат заличени (член 17-2, параграф 1, точка 2 от Указа за прилагане на ЗКИ). За да се определи кои данни са били необходими за търговското взаимоотношение, трябва да се вземат предвид различни фактори, включително дали е било възможно взаимоотношението да бъде създадено без данните и дали е пряко свързано със стоките или услугите, предоставяни на физическото лице (член 17-2, параграф 2 от Указа за прилагане на ЗКИ).

(105) Дори в случаите, когато лична кредитна информация по принцип може да се съхранява след края на търговското взаимоотношение, тя трябва да бъде заличена в срок от три месеца след постигането на допълнителната цел на обработването ([134]) или във всеки случай след пет години (член 20-2 от ЗКИ). В ограничен брой обстоятелства личната кредитна информация по принцип може да се съхранява повече от пет години, по-конкретно когато това е необходимо да се спази правно задължение; когато това е необходимо за жизненоважните интереси на живота, телесните или имуществените интереси на физическото лице; за архивирането на псевдонимизирана информация (която е била използвана за научноизследователски цели, за статистически цели или за целите на архивирането в обществен интерес); или за застрахователни цели (по-конкретно за застрахователни плащания или за предотвратяване на застрахователна измама) ([135]). В тези изключителни случаи се прилагат специални гаранции (като уведомяване на физическото лице за допълнителната употреба, разделяне на съхранената информация от информацията за физически лица, с които търговското взаимоотношение все още продължава, вж. член 17-2, параграфи 1—2 от Указа за прилагане на ЗКИ).

(106) В ЗКИ се уреждат също така принципите за точност и качество на данните, като се изисква „регистриране, изменение и управление“ на личната кредитна информация, за да остане тя точна и актуална (член 18, параграф 1 от ЗКИ и член 15, параграф 3 от Указа за прилагане на ЗКИ) ([136]). Във връзка с предоставянето на кредитна информация на определени други образувания (например агенции за кредитен рейтинг) към търговските оператори има специални изисквания да проверяват също така точността на информацията, за да се гарантира, че получателят регистрира и управлява само точна информация (член 15, параграф 1 от Указа за прилагане на ЗКИ, във връзка с член 18, параграф 1 от ЗКИ). В по-общ смисъл ЗКИ съдържа изисквания за съхранение на документи за събирането, използването, разкриването на трети страни и унищожаването на лична кредитна информация (член 20, параграф 2 от ЗКИ) ([137]).

(107) Освен това обработването на лична кредитна информация подлежи на специални изисквания по отношение на сигурността на данните. По-специално ЗКИ изисква въвеждането на технически, физически и организационни мерки за предотвратяване на незаконния достъп до компютърни системи, както и на изменението, унищожаването или всеки друг риск за обработваните данни (например чрез контрол на достъпа, вж. член 19 от ЗКИ и член 16 от Указа за прилагане на ЗКИ). В допълнение при обмена на лична кредитна информация с трета страна трябва да бъде сключено споразумение, в което да се определят специални мерки за сигурността (член 19, параграф 2 от ЗКИ). Ако има нарушение на сигурността на лична кредитна информация, трябва да се приложат мерки за свеждане до минимум на вредата и засегнатите физически лица трябва да бъдат уведомени незабавно (член 39-4, параграфи 1—2 от ЗКИ). В допълнение КЗЛД трябва да бъде информирана за извършеното уведомление на физическите лица и за приложените мерки (член 39-4, параграф 4 от ЗКИ).

([131]) В този случай заповедта трябва да бъде поискана незабавно. Ако заповедта не бъде издадена в срок от 36 часа, получените данни трябва да бъдат заличени незабавно (член 32, параграф 6, точка 6 от ЗКИ).

([132]) Например поради изпълнението на договорните задължения една от страните е упражнила правото си на прекратяване и т.н., вж. член 17-2, параграф 5 от Указа за прилагане на ЗКИ.

([133]) Член 20-2, параграф 1 от ЗКИ и член 17-2, параграф 1, точка 1 от Указа за прилагане на ЗКИ.

([134]) Този срок е съобразен с факта, че заличаването често не е възможно да бъде извършено веднага, а обикновено изисква определени стъпки (например отделяне на данните, които ще се заличават, от другите данни и извършване на заличаването, без да се засяга стабилността на информационните системи), което изисква определено време за изпълнение.

([135]) Член 20-2, параграф 2 от ЗКИ.

([136]) Член 18, параграф 2 от ЗКИ и член 15, параграф 4 от Указа за прилагане на ЗКИ съдържат по-конкретни правила по отношение на изискването за съхранение на документи, например на документи относно информация, която може да постави дадено физическо лице в неблагоприятно положение, като информация за престъпни деяния или несъстоятелност.

([137]) Що се отнася до другите механизми за отчетност, ЗКИ съдържа изисквания към определени организации (например кооперации и публични дружества, вж. член 21, параграф 2 от Указа за прилагане на ЗКИ) да определят „администратор/пазител на кредитната информация“, който отговаря за наблюдаване на спазването на ЗКИ и за изпълнението на задачите на „служителя по въпросите на поверителността“ съгласно ЗЗЛД (член 20, параграфи 3 и 4 от ЗКИ).

(108) В ЗКИ се налагат също така задължения за прозрачност при получаването на съгласие за използването или предоставянето на лична кредитна информация (член 32, параграф 4 и член 34-2 от ЗКИ и член 30-3 от Указа за прилагането на ЗКИ) и най-общо преди предоставянето на информация на трета страна (член 32, параграф 7 от ЗКИ) ([138]). В допълнение към това физическите лица имат право да получат информация при поискване относно използването или предоставянето на тяхната лична кредитна информация на трети страни за последните три години, предхождащи искането (включително за целта и датите на това използване/предоставяне) ([139]).

(109) Съгласно ЗКИ физическите лица имат също така право на достъп до личната си кредитна информация (член 38, параграф 1 от ЗКИ), както и на корекция на неточни данни (член 38, параграфи 2—3 от ЗКИ) ([140]). Освен това в допълнение към общото право на изтриване на данните съгласно ЗЗЛД (вж. съображение 77) в ЗКИ се предвижда специално право на изтриване на лична кредитна информация, запазена след изтичането на сроковете, посочени в съображение 104, т.е. пет години (за лична кредитна информация, която е била необходима за създаването или поддържането на дадено търговско взаимоотношение) или три месеца (за други видове лична кредитна информация) ([141]). Искане за изтриване може да бъде отказано по изключение, когато е необходимо допълнително съхранение поради обстоятелствата, описани в съображение 105. Ако дадено физическо лице поиска изтриване, но е приложимо едно от изключенията, по отношение на съответната кредитна информация трябва да бъдат приложени специални гаранции (член 38-3, параграф 3 от ЗКИ и член 33-3 от Указа за прилагане на ЗКИ). Например информацията трябва да бъде съхранявана отделно от друга информация, само упълномощено лице може да има достъп до нея и спрямо нея трябва да се прилагат специални мерки за сигурност.

(110) Освен правата, посочени в съображение 109, разпоредбите на ЗКИ гарантират на физическите лица правото да искат от даден администратор да спре да осъществява контакт с тях за целите на директния маркетинг (член 37, параграф 2 от закона) и правото на преносимост на данните. По отношение на последното в ЗКИ се разрешава на физическите лица да искат тяхната лична кредитна информация да им бъде предадена или да бъде предадена на определени трети страни (например финансови институции и дружества за кредитен рейтинг). Личната кредитна информация трябва да бъде обработвана и предавана на трета страна във формат, който може да бъде обработен от устройство за обработване на информация (например компютър).

(111) Поради това, доколкото ЗКИ съдържа специфични правила в сравнение със ЗЗЛД, Комисията смята, че всички тези правила гарантират ниво на защита, което по същество е равностойно на гарантираното от Регламент (ЕС) 2016/679.

2.4. **Надзор и изпълнение**

(112) С цел да се гарантира, че адекватното ниво на защита на данните се осигурява и на практика, следва да има независим надзорен орган с правомощия за наблюдение и осигуряване на спазването на правилата за защита на данните. Този орган следва да действа с пълна независимост и безпристрастност при изпълнението на своите задължения и при упражняването на правомощията си.

2.4.1. *Независим надзор*

(113) В Република Корея независимият орган, който отговаря за наблюдението и привеждането в изпълнение на ЗЗЛД, е КЗЛД. КЗЛД се състои от председател, заместник-председател и седем членове. Председателят и заместник-председателят се назначават от президента по препоръка на министър-председателя. Двама от определените членове на КЗЛД се назначават от президента по препоръка на председателя, а петима се назначават по препоръка на Националното събрание (от които двама по препоръка на политическата партия, към която принадлежи президента, и трима по препоръка на три други партии (член 7 и член 2, параграф 2 от ЗЗЛД), което спомага за

([138]) Това включва общо изискване за уведомяване (член 32, параграф 7 от ЗКИ) и специално задължение за прозрачност в случай на предоставяне на определени образувания на информация, въз основа на която може да се определи кредитоспособността на дадено физическо лице, като агенции за кредитен рейтинг и агенции за събиране на кредитна информация (член 35-3 от ЗКИ и член 30-3 от Указа за прилагане на ЗКИ), или при отказ или прекратяване на взаимоотношение на търговска операция въз основа на лична кредитна информация, получена от трета страна (член 36 от ЗКИ и член 31 от Указа за прилагане на ЗКИ).

([139]) Член 35 от ЗКИ. Определени търговски организации, например кооперации и публични дружества (член 21, параграф 2 от Указа за прилагане на ЗКИ), подлежат на допълнителни изисквания за прозрачност, например да разкриват публично определена информация (член 31 от ЗКИ) и да информират физическите лица за възможни неблагоприятни последици за техния кредитен рейтинг, когато извършват финансови операции, носещи кредитни рискове (член 35-2 от ЗКИ).

([140]) По отношение на условията и изключенията от правата на достъп и корекция се прилагат правилата на ЗЗЛД (описани в съображения 76—77). Освен това са предвидени допълнителни условия в член 38, параграфи 4—8 от ЗКИ и в член 33 от Указа за прилагане на ЗКИ. По-специално търговски оператор, който е коригирал или заличил неправилна кредитна информация, трябва да уведоми физическото лице за това. В допълнение към това всяка трета страна, на която е оповестена такава информация в рамките на предходните шест месеца, трябва да бъде уведомена и съответното физическо лице трябва да бъде информирано за това. Ако дадено физическо лице не е удовлетворено от начина, по който е разгледано искането му за корекция, то може да подаде искане до КЗЛД, която проверява действията на администратора и може да наложи коригиращи мерки.

([141]) Член 38-3 от ЗКИ.

неутрализиране на партийните пристрастия в процеса на назначаването им) ([142]). Тази процедура е в съответствие с изискванията, приложими за назначаването на членове на органите за защита на личните данни в Съюза (член 53, параграф 1 от Регламент (ЕС) № 2016/679). Освен това всички членове на КЗЛД трябва да се въздържат от извършване на дейност, свързана с печалба, от политически дейности и от заемане на позиции в публичната администрация или в Националното събрание (член 7-6 и член 7-7, параграф 1, точка 3 от ЗЗЛД) ([143]). Всички членове на КЗЛД също така се подчиняват на специални правила, които възпрепятстват тяхното участие в обсъжданията в случай на възможен конфликт на интереси (член 7-11 от ЗЗЛД). Комисията за защита на личните данни се подпомага от секретариат (член 7-13) и може да създава подкомисии (в които влизат по трима членове на Комисията) за разглеждане на малки нарушения и повтарящи се въпроси (член 7-12 от ЗЗЛД).

(114) Всеки член на КЗЛД се назначава за срок от три години и може да бъде преназначен веднъж (член 7-4, параграф 1 от ЗЗЛД). Членовете могат да бъдат освобождавани само при специални обстоятелства, а именно: ако вече не са в състояние да изпълняват задълженията си поради трайно психическо или физическо увреждане, ако действат в нарушение на закона или ако отговарят на едно от условията за отстраняване от длъжност ([144]) (член 7-5 от ЗЗЛД). Това им осигурява институционална закрила при упражняването на техните функции.

(115) В по-общ план в член 7, параграф 1 от ЗЗЛД изрично се гарантира независимостта на КЗЛД, а в член 7-5, параграф 2 от ЗЗЛД от членовете на КЗЛД се изисква да изпълняват задълженията си независимо, в съответствие със закона и със своята съвест ([145]). Описаните институционални и процедурни гаранции, включително по отношение на назначаването и освобождаването на нейните членове, гарантират на КЗЛД свобода да действа в пълна независимост, без външна намеса или указания. Освен това като централна административна агенция КЗЛД предлага ежегодно свой собствен бюджет (който се разглежда от Министерството на финансите като част от общия национален бюджет преди приемането му от Националното събрание) и отговаря за управлението на собствения си персонал. Комисията за защита на личните данни има текущ бюджет от близо 35 милиона евро и персонал от 154 души (включително 40 специалисти в областта на информационните и комуникационните технологии, 32 служители, занимаващи се предимно с разследвания и 40 правни експерти).

(116) Задачите и правомощията на КЗЛД са определени главно в членове 7-8 и 7-9, както и в членове 61—66 от ЗЗЛД ([146]). По-специално задачите на КЗЛД включват консултиране относно законите и подзаконовите актове, свързани със защитата на данните, разработване на политики и насоки за защита на данните, разследване на нарушения на конкретни права, разглеждане на жалби и медиация при спорове, гарантиране на спазването на ЗЗЛД, гарантиране на обучение и поощряване в областта на защитата на данните и обмен и сътрудничество с органи на трети страни за защита на данните ([147]).

(117) Въз основа на член 68 от ЗЗЛД, във връзка с член 62 от Указа за прилагане на ЗЗЛД, определени задачи на КЗЛД са делегирани на Корейската агенция за интернет и сигурност, а именно: (1) образование и връзки с обществеността, (2) обучение на специалисти и разработване на критерии за оценки на въздействието върху неприкосновеността на личния живот, (3) разглеждане на искания за даване на статут на т.нар. институция за оценка на въздействието върху неприкосновеността на личния живот, (4) разглеждане на искания за непряк достъп до лични

([142]) За членове на Комисията могат да бъдат назначавани само физически лица, които отговарят на следните условия: да са висши държавни служители, които се занимават с въпросите на личните данни; да са бивши съдии, прокурори или адвокати с опит най-малко 10 години; да са бивши ръководители с опит в защитата на данни и да са работили в публична институция или организация над три години или да са препоръчани от такава институция или организация; и да са бивши доценти с професионални знания в областта на защитата на данните, които да са работили поне пет години в академична институция (член 7-2 от ЗЗЛД).

([143]) Вж. също член 4-2 от Указа за прилагане на ЗЗЛД.

([144]) Вж. член 7-7 от ЗЗЛД, съгласно който чужденци и членове на политически партии не могат да бъдат членове на КЗЛД. Същото се отнася до физически лица, на които са били наложени определени видове наказателни санкции, които са били отстранени дисциплинарно от длъжност през последните пет години и др. (член 7-7 от ЗЗЛД, във връзка с член 33 от Закона за държавните служители).

([145]) Макар че член 7, параграф 2 от ЗЗЛД се отнася до общото правомощие на министър-председателя по член 18 от Закона за държавната организация да преустановява или отменя — с одобрението на президента — всяко незаконосъобразно разпореждане на агенция на централната администрация, той няма такова правомощие по отношение на КЗЛД във връзка с нейните правомощия за разследване или изпълнение (вж. член 7, параграф 2, точки 1 и 2 от ЗЗЛД). Според пояненията, получени от корейското правителство, член 18 от Закона за държавната организация е предназначен да осигури възможност на министър-председателя да действа в изключителни обстоятелства, например да посредничи при разногласие между различни държавни органи. Министър-председателят обаче никога досега не се е възползвал от това свое правомощие от приемането на разпоредбата през 1963 г.

([146]) Когато е необходимо да изпълнява задачите съгласно член 7-9, параграф 1 от ЗЗЛД, КЗЛД може да търси становищата на съответните държавни длъжностни лица, на експерти по защита на данните, на граждански организации и на съответните стопански субекти. В допълнение КЗЛД може да поиска съответни материали, може да дава препоръки за подобрение и да прави проверки дали те се изпълняват (член 7-9, параграфи 2—5 от ЗЗЛД).

([147]) Вж. също член 9 от ЗЗЛД (тригодишен Генерален план за защита на личните данни), член 12 от ЗЗЛД (Стандартни насоки относно защитата на личните данни), член 13 от ЗЗЛД (политики за насърчаване и подкрепа на саморегулирането)

данни, съхранявани от публични органи (член 35, параграф 2 от ЗЗЛД) и (5) задачата за искане на материали и извършване на проверки на място във връзка с жалби, получени чрез т.нар. Информационен център по въпросите на поверителността. В контекста на разглеждането на жалби чрез Информационния център по въпросите на поверителността Корейската агенция за интернет и сигурност предава случая на КЗЛД или на прокуратурата, ако установи, че има нарушение на закона. Възможността за подаване на жалба до Информационния център по въпросите на поверителността не възпрепятства физическите лица да подават пряко жалба до КЗЛД или да се свързват с КЗЛД, ако смятат, че жалбата им не е разгледана по задоволителен начин от Корейската агенция за интернет и сигурност.

2.4.2. *Правоприлагане, включително санкции*

(118) С цел да се гарантира спазването на ЗЗЛД законодателят е предоставил на КЗЛД правомощия както за разследване, така и за правоприлагане, вариращи от препоръки до административни глоби. Тези правомощия са допълнени от режим на наказателни санкции.

(119) Що се отнася до разследващите правомощия, ако има съмнение за нарушение на ЗЗЛД или ако е докладвано за такова нарушение, или когато това е необходимо за защита на субекта на данните срещу нарушения, КЗЛД може да извършва проверки на място и да иска всички съответни материали (статии и документи) от администраторите на лични данни (член 63 от ЗЗЛД, във връзка с член 60 от Указа за прилагане на ЗЗЛД) ([148]).

(120) По отношение на правоприлагането, съгласно член 61, параграф 2 от ЗЗЛД, КЗЛД може да дава съвети на администраторите на лични данни как да подобрят нивото на защита на личните данни при конкретни дейности за обработване на лични данни. Администраторите на лични данни трябва да полагат добросъвестни усилия да изпълняват подобни съвети и са задължени да информират КЗЛД за резултата. Освен това, когато има разумни основания да се смята, че е налице нарушение на ЗЗЛД и че непредприемането на действия може да причини трудно поправими вреди, КЗЛД може да наложи корективни мерки (член 64, параграф 1 от ЗЗЛД) ([149]). В раздел 5 от Уведомление 2021-5 (приложение I), което има обвързващо действие, се пояснява, че тези условия са изпълнени във връзка с нарушението на разпоредба на ЗЗЛД за защита на правата на неприкосновеност на личния живот на физическите лица по отношение на личните им данни ([150]). Мерките, които КЗЛД има правомощие да приложи, включват разпореждане за спиране на извършването на нарушението, преустановяване на обработването на личните данни или други необходими мерки. Неспазването на дадена корективна мярка може да доведе до санкция под формата на глоба в максимален размер от 50 милиона вона (член 75, параграф 2, точка 13 от ЗЗЛД).

(121) Що се отнася до другите механизми за отчетност, ЗКИ съдържа изисквания към определени организации (например кооперации и публични дружества, вж. член 21, параграф 2 от Указа за прилагане на ЗКИ) да определят „администратор/пазител на кредитната информация“, който отговаря за наблюдаване на спазването на ЗКИ и за изпълнението на задачите на „служителя по въпросите на поверителността“ съгласно ЗЗЛД (член 20, параграфи 3 и 4 от ЗКИ). Съгласно раздел 5 от Уведомление 2021-5 това се отнася до извънредни фактически и правни обстоятелства, с които КЗЛД не е запозната, когато прави препоръката. Съответният публичен орган може да се позове на такива извънредни обстоятелства само ако докаже категорично, че има нарушение и КЗЛД реши, че няма такова нарушение. Иначе публичният орган трябва да следва препоръката на КЗЛД и „да предприеме корективна мярка, включително незабавно да спре действието, както и да предостави обезщетение за вредите в изключителния случай, когато все пак е било извършено незаконно действие.“

(122) Комисията за защита на личните данни може да поиска също така от други административни агенции със специфична компетентност по силата на секторно законодателство (например в сферата на здравеопазването, образованието) да извършат разследване — самостоятелно или съвместно с КЗЛД — за (предполагаеми) нарушения на неприкосновеността на личния живот от страна на администратори под тяхната юрисдикция и да наложат корективни мерки (член 63, параграфи 4—5 от ЗЗЛД). В този случай КЗЛД определя основанията, предмета и обхвата на разследването ([151]). На свой ред съответната административна агенция трябва да предостави на КЗЛД план за проверка на място и да я уведоми за резултата от нея. Комисията за защита на личните данни може да препоръча да бъде предприета конкретна корективна мярка, а съответната агенция трябва да се опита да я изпълни. Във всеки случай това искане не ограничава правомощието на КЗЛД да извърши свое разследване или да наложи санкции.

([148]) Освен това КЗЛД може да влезе в помещенията на администратора, за да провери състоянието на стопанските дейности, регистрите, документите и др. (член 63, параграф 2 от ЗЗЛД). Вж. също член 45-3 от ЗКИ и член 36-4 от Указа за прилагане на ЗКИ по отношение на правомощията на КЗЛД по този закон.

([149]) Вж. също член 45-4 от ЗКИ по отношение на правомощията на КЗЛД по ЗКИ.

([150]) В раздел 5 от Уведомлението се предвижда, че „сериозно основание да се смята, че е извършено нарушение по отношение на личните данни и че непредприемането на действия може да причини трудно поправими вреди по смисъла на параграфи 1 и 2 от член 64 от ЗЗЛД, е свързано с нарушението на някой от принципите, правата и задълженията, включени в закона с цел защита на правата на физическите лица по отношение на личните данни.“ Същото се отнася за правомощията на КЗЛД по член 45-4 от ЗКИ.

([151]) Член 60 от Указа за прилагането на ЗЗЛД

(123) Освен правомощията да изисква корекции КЗЛД може да налага административни глоби в размер от 10 до 50 милиона вона за нарушения на различни изисквания на ЗЗЛД (член 75 от ЗЗЛД) ([152]). Наред с другото, това включва неспазване на изискванията за законосъобразност на обработването, неприлагане на необходимите мерки за сигурност, неуведомяване на субектите на данни в случай на нарушение на сигурността на данните им, неспазване на изискванията за възлагане на обработването на външен изпълнител, несъздаване и неразкриване на политиката за поверителност, неопределяне на отговорник по въпросите на поверителността или бездействие в случай на искане от субекта на данните за упражняване на индивидуалните му права, както и определени процедурни нарушения (отказ от сътрудничество по време на разследване). В случай на нарушения на няколко разпоредби от ЗЗЛД от един и същ администратор на лични данни може да бъде наложена глоба за всяко нарушение и броят на засегнатите физически лица ще бъде взет предвид при определяне на размера на глобата.

(124) Освен това, когато съществуват разумни основания да се предполага, че има нарушение на ЗЗЛД или на други „закони, свързани със защитата на данните“, КЗЛД може да подаде наказателна жалба до компетентната разследваща агенция (например прокурор, вж. член 65, параграф 1 от ЗЗЛД). Освен това КЗЛД може да посъветва администратора да открие дисциплинарно производство срещу отговорното лице (включително срещу отговорния ръководител, вж. член 65, параграф 2 от ЗЗЛД). След като получи такъв съвет, администраторът трябва да го изпълни ([153]) и да уведоми КЗЛД писмено за резултата (член 65 от ЗЗЛД във връзка с член 58 от Указа за прилагане на ЗЗЛД).

(125) По отношение на съвет съгласно член 61, корективни мерки съгласно член 64, обвинение или съвет за дисциплинарно производство съгласно член 65 и налагането на административни глоби съгласно член 75 от ЗЗЛД КЗЛД може да оповести публично фактите — т.е. нарушението, образуването, което е нарушило закона, и наложените) мерки — чрез публикуването им на своя уебсайт или в национален всекидневник (член 66 от ЗЗЛД, във връзка с член 61, параграф 1 от Указа за прилагане на ЗЗЛД) ([154]).

(126) Накрая, спазването на изискванията за защита на личните данни, изложени в ЗЗЛД (както и в „други закони, свързани със защитата на личните данни“), е подкрепено с режим на наказателни санкции. В това отношение членове 70—73 от ЗЗЛД съдържат наказателни разпоредби, които могат да доведат до налагането на глоба (в размер от 20 до 100 милиона вона) или до лишаване от свобода (максималната присъда варира от 2 до 10 години). Съответните нарушения включват, наред с другото, използването на лични данни или предоставянето на такива данни на трета страна без необходимото съгласие, обработването на чувствителни данни въпреки забраната в член 23, параграф 1 от ЗЗЛД, неспазване на приложимите изисквания за безопасност, в резултат на което лични данни са изгубени, откраднати, разгласени, подправени, изменени или повредени, неприлагане на необходимите мерки за коригиране, изтриване или преустановяване на лични данни или незаконно предаване на лични данни на трета страна ([155]). Съгласно член 74 от ЗЗЛД във всички тези случаи отговорност носят служителят, агентът или представителят на администратора, както и самият администратор ([156]).

(127) Освен наказателните санкции, предвидени в ЗЗЛД, неправилното използване на личните данни може също така да представлява престъпление по Наказателния закон. По-специално такъв е случаят с нарушаването на тайната на кореспонденцията, на документи или на електронни регистри (член 316), разкриването на информация, която е предмет на професионална тайна (член 317), измамата чрез използването на компютри (член 347-2), както и присвояването и нарушаването на доверието (член 355).

(128) Следователно корейската система съчетава различни видове санкции — от корективни мерки и административни глоби до наказателни санкции, за които има вероятност да окажат особено силен възпиращ ефект върху администраторите и физическите лица, обработващи данните. Комисията за защита на личните данни започна да

([152]) Освен това, когато е сертифицирано, че управляваните от даден администратор системи за обработване и защита на личните данни съответстват на ЗЗЛД, но в действителност не са изпълнени критериите за сертифициране съгласно член 34-2, параграф 1 от Указа за прилагане на ЗЗЛД, или в случай на сериозно нарушение на „закон, свързан със защитата на [личните] данни“, КЗЛД може да отнеме сертификацията (член 32-2, параграфи 3 и 5 от ЗЗЛД). Комисията за защита на личните данни уведомява администратора за отмяната и я обявява публично или публикува информация за нея на своя уебсайт или в Официален вестник (член 34-4 от Указа за прилагане на ЗЗЛД). За нарушение на ЗКИ се предвиждат също така административни глоби (член 52 от ЗКИ) и наказателни санкции (член 50 от ЗКИ).

([153]) В съответствие с член 58, параграф 2 от Указа за прилагане на ЗЗЛД, в случай че специални обстоятелства не позволяват съветът да бъде изпълнен, администраторът е длъжен да представи аргументирани мотиви на КЗЛД.

([154]) При вземането на решение дали да направи публично разкриване КЗЛД взема предвид същността и сериозността на нарушението, неговата продължителност и честота, както и последиците от него (степен на увреждане). На засегнатото образувание се дава предизвестие и възможност да се защити. Вж. член 61, параграфи 2 и 3 от Указа за прилагане на ЗЗЛД.

([155]) Вж. член 71, точка 2 във връзка с член 18, параграф 1 от ЗЗЛД (неспазване на условията в член 17, параграф 3, за който се отнася член 18, параграф 1). Вж. също така член 75, параграф 2, точка 1, във връзка с член 17, параграф 2 от ЗЗЛД (непредоставяне на необходимата информация на засегнатото физическо лице съгласно член 17, параграф 2 от ЗЗЛД, за който се отнася член 17, параграф 3).

([156]) Освен това в член 74-2 от ЗЗЛД се разрешава конфискуването на пари, стоки или други печалби, придобити в резултат от нарушението, или, ако конфискацията е невъзможна — „събирането“ на незаконно получената полза.

упражнява правомощията си веднага след като бе създадена през 2020 г. Годишният доклад на КЗЛД за 2021 г. показва, че КЗЛД вече е издала редица препоръки, административни глоби и заповеди за корекция както срещу публичния сектор (близо 34 публични органа), така и срещу частни оператори (близо 140 дружества) ([157]). Например през декември 2020 г. КЗЛД наложи глоба от 6,7 милиарда вона на дружество за нарушаване на различни разпоредби на ЗЗЛД (включително на изискванията за сигурност, на изискванията за съгласие за предоставяне на данни на трета страна и за прозрачност) ([158]) и глоба от 103,3 милиона вона през април 2021 г. на дружеството AI technology (за нарушаване, наред с други разпоредби, на правилата за законосъобразност на обработването, по-конкретно във връзка със съгласието, и на обработването на псевдонимизирана информация) ([159]). През август 2021 г. КЗЛД приключи друго разследване на дейността на три дружества, което доведе до коративни мерки и налагането на глоби в размер на до 6,47 милиарда вона (наред с другото, за неинформиране на физически лица за разкриването на лични данни на трети лица, включително предаване на трети държави) ([160]). Също така Южна Корея имаше доказани резултати в правоприлагането още преди извършването на неотдавнашната реформа, като отговорните органи използваха пълния набор от действия по правоприлагане, включително административни глоби, коративни мерки и „посочване и споделяне“ по отношение на различни администратори, включително доставчиците на комуникационни услуги (Корейска комисия по комуникациите), както и търговски оператори, финансови институции, публични органи, университети и болници (Министерство на вътрешните работи и безопасността) ([161]). Въз основа на това Комисията стига до заключението, че корейската система осигурява ефективно спазване на правилата за защита на личните данни на практика, като по този начин гарантира ниво на защита, което по същество е равностойно на нивото съгласно Регламент (ЕС) 2016/679.

2.5. **Средства за правна защита**

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

(130) Корейската система предоставя на физическите лица различни механизми за ефективно упражняване на техните права и за получаване на (съдебни) средства за правна защита.

(131) Като първа стъпка физическите лица, които смятат, че правата им на защита на личните им данни и на интересите им са били нарушени, могат да се обърнат към съответния администратор. Съгласно член 30, параграф 1, точка 5 от ЗЗЛД политиката за поверителност на администратора трябва включва, наред с останалото, информация за правата на субектите на данни и за начина на упражняването им. Освен това тя трябва да съдържа информация за контакт — име и телефонен номер на служителя по въпросите на поверителността или отдела, който отговаря за защитата на данните — което дава възможност за подаване на жалби („оплаквания“). В рамките на организацията на администратора служителят по въпросите на поверителността е натоварен с разглеждането на жалби, прилагането на коративни мерки в случай на нарушение на неприкосновеността на личния живот и обезщетение за вреди (член 31, параграф 2, точка 3, параграф 4 от ЗЗЛД). Последното има значение например в случай на нарушение на сигурността на личните данни, тъй като администраторът трябва да информира субекта на данните за звеното(звената) за контакт, до които може да се докладва за вреди, наред с другото (член 34, параграф 1, точка 5 от ЗЗЛД).

(132) Освен това в ЗЗЛД се осигуряват средства за правна защита на физическите лица спрямо администраторите. Първо, всяко физическо лице, което смята, че правата или интересите му по отношение на защитата на личните данни са били нарушени от администратора, може да докладва за това на КЗЛД и/или на една от специализираните институции, определени от КЗЛД да получават и разглеждат жалби; това включва Корейската агенция за интернет и сигурност, която за целта разполага с информационен център по въпросите на личните данни (т.нар. „Информационен център по въпросите на поверителността“) (член 62, параграфи 1—2 от ЗЗЛД във връзка с член 59 от Указа за прилагане на ЗЗЛД). Информационният център по въпросите на поверителността разследва и установява нарушения, предоставя консултации във връзка с обработването на лични данни (член 62,

([157]) Вж. годишния доклад на КЗЛД за 2021 г., стр. 50—55 (на разположение само на корейски език) на следния адрес: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Вж. (на разположение само на корейски език) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Вж. (на разположение само на корейски език) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4l7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Вж. (на разположение само на корейски език): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Вж. например годишния доклад за 2020 г. в (на разположение само на корейски език) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 и примерите, предоставени на английски език, в https://www.privacy.go.kr/eng/enforcement_02.do.

параграф 3 от ЗЗЛД) и може да докладва за нарушения на КЗЛД (но самият той не може да предприема принудителни мерки). Информационният център по въпросите на поверителността получава голям брой жалби/искания (например 177 457 през 2020 г., 159 255 през 2019 г. и 164 497 през 2018 г.) ([162]). Съгласно информация, получена от КЗЛД, самата КЗЛД е получила близо 1 000 жалби в периода август 2020—август 2021 г. В отговор на жалба КЗЛД може да предоставя съвети за подобрения, корективни мерки, „обвинение“ към компетентната разследваща агенция (включително прокурор) или съвет за дисциплинарно производство (вж. членове 61, 64 и 65 от ЗЗЛД). Решенията на КЗЛД (например отказ за разглеждане на жалба или отхвърляне на жалба по същество) могат да бъдат оспорени съгласно Закона за административното съдопроизводство ([163]).

(133) Второ, съгласно членове 40—50 от ЗЗЛД, във връзка с членове 48-14—57 от Указа за прилагане на ЗЗЛД, субектите на данни могат да завеждат искове пред т.нар. „Комитет за медиация при спорове“, който се състои от представители, назначени от председателя на ЗЗЛД измежду членовете на Висшата изпълнителна служба на КЗЛД, и физически лица, назначени въз основа на опита им в областта на защитата на личните данни измежду определени допустими групи (вж. член 40, параграфи 2, 3 и 7 от ЗЗЛД, член 48-14 от Указа за прилагане на ЗЗЛД) ([164]). Възможността да се използва медиация пред Комитета за медиация при спорове осигурява алтернативна възможност за получаване на средства за правна защита, но не ограничава правото на физическото лице вместо това да се обърне към КЗЛД или към съдилищата. За да разгледа случаят, Комитетът може да поиска от спорещите страни да предоставят необходимите материали и/или да призове свидетели, които да се явят пред него (член 45 от ЗЗЛД). След изясняването на въпроса Комитетът изготвя проект на медиационно решение ([165]), по което мнозинството от членовете му трябва да са съгласни. Проектът на медиационното решение може да включва преустановяване на нарушението, необходими средства за правна защита (включително възстановяване или обезщетение за вреди), както и мерки, които са необходими за недопускане на повторение на същото или на подобно нарушение (нарушения) (член 47, параграф 1 от ЗЗЛД). Когато двете страни са съгласни с медиационното решение, то ще има същото действие като съдебно споразумение (член 47, параграф 5 от ЗЗЛД). Всяка от страните може да заведе съдебен иск, докато продължава медиацията, като в този случай тя ще бъде преустановена (вж. член 48, параграф 2 от ЗЗЛД) ([166]). Годишният брой издадени решения от КЗЛД показва, че физическите лица редовно прибягват до процедурата пред Комитета за медиация при спорове, което често води до успешен резултат. Например през 2020 г. Комитетът е разгледал 126 случая, от които 89 са били разрешени от Комитета (77 случая, в които страните са постигнали споразумение преди приключването на процеса на медиация и 12 случая, в които страните са приели предложението за медиация), което представлява дял на медиация от 70,6 % ([167]). По подобен начин през 2019 г. Комитетът е разгледал 139 случая, от които 92 са били разрешени, което представлява дял на медиация от 62,2 %.

(134) Освен това, когато поне 50 физически лица са понесли вреда или правата им на защита на личните им данни са били нарушени по същия или по подобен начин вследствие на същия (вид) инцидент ([168]), даден субект на данни или дадена организация за защита на личните данни могат да кандидатстват за колективна медиация на спора от името на такъв колектив; други субекти на данни могат да кандидатстват да се присъединят към медиацията, която ще бъде обявена публично от Комитета за медиация при спорове (член 49, параграфи 1—3 от ЗЗЛД, във връзка с членове 52—54 от Указа за прилагане на ЗЗЛД) ([169]). Комитетът за медиация при спорове може да избере

([162]) Вж. годишния доклад на КЗЛД за 2021 г., стр. 174. През 2020 г. такива жалби са били свързани например със събирането на данни без разрешение, неспазването на задълженията за прозрачност, нарушения на ЗЗЛД от обработващи лични данни, недостатъчни мерки за сигурност, липса на отговор на искания от субекти на данни, както и на общи запитвания.

([163]) По-специално физическите лица могат да обжалват упражняването или отказа на административна агенция от упражняване на публично правомощие (член 2, параграф 1, точка 1, член 3, точка 1 от Закона за административното съдопроизводство). По-подробна информация за процедурните аспекти, включително за изискванията за допустимост, е предоставена в съображение 181.

([164]) Всички членове са с фиксиран мандат и могат да бъдат освободени само по основателна причина (член 40, параграф 5, член 41 от ЗЗЛД). Освен това в член 42 от ЗЗЛД се съдържат гаранции за защита срещу конфликт на интереси.

([165]) Вж. член 44 от ЗЗЛД. В допълнение той може да предложи проект за уреждане и да препоръча уреждане без медиация (вж. член 46 от ЗЗЛД).

([166]) В допълнение Комитетът може да отхвърли медиацията, ако сметне, че не е подходящо да посредничи в спора с оглед на неговото естество, или поради това, че заявлението за медиация е подадено без основателна цел (член 48 от ЗЗЛД).

([167]) Вж. годишния доклад на КЗЛД за 2021 г., стр. 179—180. Тези случаи са свързани, наред с другото, с нарушения на изискването за получаване на съгласие за събирането на данни, на принципа за ограничаване на целта и на правата на субектите на данни.

([168]) Вж. член 49, параграф 1 от ЗЗЛД, съгласно който субектите на данни трябва да са понесли вреда или нарушение на техните права „по идентичен или подобен начин“, и член 52, точка 2 от Указа за прилагане на ЗЗЛД, в който се поставя изискването „[о]сновните въпроси от инцидента да са общи от фактическа или правна гледна точка“.

([169]) Освен това дори лица, които не са страна по спора, могат да се възползват от решение на колективна медиация при спор, доколкото Комитетът за медиация при спорове може да посъветва администратора да изготви и да представи план за обезщетение, който обхваща и тях (член 49, параграф 5 от ЗЗЛД).

за представляваща страна поне едно лице, което представлява най-добре общия интерес (член 49, параграф 4 от ЗЗЛД). Когато администраторът отхвърли колективна медиация във връзка със спор или не желае да приеме медиационното решение, определени организации ([170]) могат да заведат колективен иск във връзка с нарушението (членове 51—57 от ЗЗЛД).

(135) Трето, в случай на нарушение на неприкосновеността на личния живот, причинило „вреда“ на физическото лице, субектът на данните има право на подходящо средство за правна защита в „надлежна и добросъвестна процедура“ (член 4, точка 5, с член 39 от ЗЗЛД) ([171]). Администраторът може да се оневини, като докаже липсата на вина („умисъл“ или груба небрежност). Когато субектът на данни претърпи вреда в резултат на загуба, кражба, разкриване, фалшифициране, промяна или повреда на личните му/ѝ данни, съдът може да определи обезщетение в размер до три пъти по-голям от действителната вреда, вземайки предвид редица фактори (член 39, параграфи 3—4 от ЗЗЛД). Като алтернативна възможност субектът на данни може да поиска „разумна сума“ на обезщетение за вреди, чийто размер не надхвърля 3 милиона вона (член 39-2, параграфи 1—2 от ЗЗЛД). Освен това в съответствие с Гражданския закон обезщетение за вреди може да се предяви срещу всяко лице, „което причинява загуби или увреждане на друго лице чрез незаконно действие, умишлено или поради небрежност“ ([172]), или от лице, „което е причинило увреждане на лицето, на свободата или на славата на друго лице или е причинило душевни страдания на друго лице“ ([173]). Тази деликтна отговорност, породена от нарушението на правилата за защита на личните данни, е потвърдена от Върховния съд ([174]). Ако вредата е причинена от незаконосъобразно действие на публичен орган, иск за обезщетение за вреда може да се подаде също така в съответствие със Закона за държавните обезщетения ([175]). Иск в съответствие със Закона за държавните обезщетения може да се подаде до специализиран „Съвет за обезщетение за вреди“ или пряко до корейските съдилища ([176]). Държавната отговорност обхваща също така нематериални вреди (например душевно страдание) ([177]). Ако жертвата е чужденец, Законът за държавните обезщетения се прилага, доколкото неговата/нейната държава по произход гарантира равностойно обезщетение за корейските граждани ([178]).

(136) Четвърто, Върховният съд е признал, че физическите лица имат право да подават искове за преустановяване на нарушения при нарушения на техните права съгласно Конституцията, включително правото на защита на личните данни ([179]). В този контекст даден съд може да разпореди на администраторите да преустановят или да спрат всяко незаконно действие. В допълнение към това правата за защита на личните данни, включително правата, които са защитени съгласно ЗЗЛД, могат да бъдат приведени в изпълнение чрез граждански искове. Това хоризонтално прилагане на конституционната защита на неприкосновеността на личния живот спрямо взаимоотношения между частни страни е признато от Върховния съд ([180]).

([170]) А именно, потребителски групи или неправителствени организации с определена големина по отношение на членство, чиято заявена цел е защита на личните данни (макар че в последния случай има допълнително изискване поне 100 субекти на данни, които са пострадали от същото (по вид) нарушение, да са подали искане за завеждане на колективен иск). Вж. член 51 от ЗЗЛД.

([171]) Членове 43—43-3 от ЗКИ също уреждат отговорността за обезщетяване за вреди, настъпили в резултат от нарушение на този закон.

([172]) Член 750 от Гражданския закон.

([173]) Член 751, параграф 1 от Гражданския закон.

([174]) Вж. например Решение на Върховния съд 2015Da251539, 251546, 251553, 251560, 251577, 30 май 2018 г. В допълнение Върховният съд е потвърдил, че нарушенията на сигурността на личните данни може да доведат до присъждане на вреди по Гражданския закон, вж. Решение на Върховния съд 2011Da59834, 59858, 59841, 26 декември 2012 г. (резюме на английски език е достъпно на адрес: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). В този случай Върховният съд е пояснил, че за оценката на това дали дадено физическо лице е пострадало от емоционален стрес, който се квалифицира като подлежаща на обезщетение вреда, е необходимо да се разгледат няколко фактора, като видът и характеристиките на изтеклите данни, възможността за идентификация на физическото лице поради нарушението, възможността за достъп до данните от трети страни, степента на разпространение на личните данни, дали това е довело до допълнителни нарушения на индивидуалните права, как са били управлявани и защитени личните данни и др.

([175]) Въз основа на Закона за държавните обезщетения физическите лица могат да подават заявления за обезщетение за вреди, нанесени от държавни служители при изпълнението на задълженията им в нарушение на закона (член 2, параграф 1 от този закон).

([176]) Членове 9 и 12 от Закона за държавните обезщетения. В този закон се предвижда създаването на районни съвети (които се председателстват от заместник-прокурор на съответната прокуратура), Централен съвет (който се председателства от заместник-министър на правосъдието) и Специален съвет (който отговаря за исковете за обезщетение за вреди, нанесени на военен персонал или на цивилни служители във военните формирования, и се председателства от заместник-министър на националната отбрана). Исканията за обезщетение за вреди по принцип се разглеждат от районните съвети, които при определени обстоятелства трябва да препратят случаите към Централния/Специалния съвет, например ако обезщетението надхвърля определена сума или в случай че дадено физическо лице иска повторно разглеждане. Всички съвети се състоят от членове, назначени от министъра на правосъдието (например държавни служители от Министерството на правосъдието, съдебни изпълнители, адвокати и лица с опит по въпросите на държавните обезщетения), които са длъжни да спазват конкретни правила за конфликт на интереси (вж. член 7 от Указа за прилагане на Закона за държавните обезщетения).

([177]) Вж. член 8 от Закона за държавните обезщетения (който препраща към Гражданския закон), както и член 751 от Гражданския закон.

([178]) Вж. член 7 от Закона за държавните обезщетения.

([179]) Решение на Върховния съд 93Da40614, 12 април 1996 г., и Решение на Върховния съд 2008Da42430, 2 септември 2011 г. (резюме на английски език е достъпно на адрес: https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Вж. например Решение на Върховния съд 2008Da42430, 2 септември 2011 г. (резюме на английски език е достъпно на адрес: https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Накрая, физическите лица могат да подадат наказателна жалба съгласно Наказателнопроцесуалния закон (член 223) до прокурор или до съдебен полицейски служител ([181]).

(138) Следователно корейската система предоставя различни механизми за получаване на правна защита — от лесно-достъпни, евтини варианти (например чрез установяване на контакт с Информационния център по въпросите на поверителността или чрез (колективна) медиация) до административни (пред КЗЛД) и съдебни механизми, включително възможността да се получи обезщетение за вреди.

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

(139) Комисията извърши също така оценка на ограниченията и гаранциите, включително на предвидените от корейското законодателство механизми за надзор и индивидуална правна защита във връзка със събирането и последващото използване от корейските публични органи на лични данни, предадени на администратори в Корея в обществен интерес, по-специално за целите на наказателното правоприлагане и националната сигурност („достъп на държавните органи“). В това отношение корейското правителство предостави на Комисията официални изявления, гаранции и ангажименти, подписани на равнище министри и ръководители на държавни ведомства, които се съдържат в приложение II към настоящото решение.

(140) При оценката дали условията, при които достъпът на държавните органи до данни, предавани на Корея съгласно настоящото решение, отговарят на критерия за „равностойност по същество“ съгласно член 45, параграф 1 от Регламент (ЕС) 2016/679, както се тълкува от Съда на Европейския съюз в светлината на Хартата на основните права, Комисията взе предвид по-специално следните критерии.

(141) Първо, всяко ограничаване на упражняването на правото на защита на личните данни трябва да бъде предвидено в закон, а самото правно основание, позволяващо намеса в това право, трябва да определя обхвата на ограничението при упражняване на съответното право ([182]).

(142) Второ, за да удовлетвори изискването за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се прилагат само доколкото са строго необходими в едно демократично общество, за да се постигнат конкретни цели от общ интерес, равностойни на тези, признати от Съюза, законодателството на въпросната трета държава, позволяващо намесата, трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданите мерки и да налагат минимални изисквания, така че лицата, чиито данни са били предадени, да разполагат с достатъчно гаранции, позволяващи ефективна защита на техните лични данни срещу рискове от злоупотреби ([183]). Законодателството трябва в частност да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на такива данни ([184]), както и да предвиди над изпълнението на такива изисквания да се упражнява независим надзор ([185]).

(143) Трето, това законодателство и неговите изисквания трябва да бъдат правно обвързващи съгласно вътрешното законодателство. Това се отнася преди всичко до органите на въпросната трета държава, но тези правни изисквания трябва да бъдат също така подлежащи на изпълнение пред съдилищата спрямо тези органи ([186]). По-специално субектите на данни трябва да имат възможността да заведат дело пред независим и безпристрастен правораздавателен орган, за да получат достъп до отнасящи се до тях лични данни или да коригират или изтриват такива данни ([187]).

3.1. Обща правна уредба

(144) Ограниченията и гаранциите, които се прилагат по отношение на събирането и последващото използване на лични данни от корейските публични органи, произтичат от общата конституционна рамка, от специалните закони, с които се уреждат техните дейности в областите на наказателното правоприлагане и националната сигурност, както и от правилата, които се прилагат специално във връзка с обработването на личните данни.

([181]) Както е пояснено в съображение 127, неправилната употребата на данни може да представлява престъпление съгласно Наказателния закон.

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

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

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

([185]) Вж. *решение по дело Schrems II*, точка 179.

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

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

(145) Първо, достъпът до лични данни от корейските публични органи се урежда от общите принципи на законност, необходимост и пропорционалност, които произтичат от корейската Конституция ([188]). По-специално основните права и свободи (включително правото на неприкосновеност на личния живот и правото на поверителност на кореспонденцията) ([189]) могат да бъдат ограничени само със закон и когато това е необходимо за националната сигурност или за поддържането на законността и реда за благото на обществото. Тези ограничения не могат да засягат същността на разглежданото право или свобода. По-специално по отношение на претърсванията и изземванията Конституцията предвижда, че те могат да се извършват само в съответствие с разпоредбите на закона, въз основа на заповед, издадена от съдия, и в съответствие със законосъобразна процедура ([190]). Накрая, физическите лица могат да се позовават на правата и свободите си пред Конституционния съд, ако смятат, че те са били нарушени от публични органи при упражняване на техните правомощия ([191]). По подобен начин физическите лица, които са понесли вреди поради незаконосъобразен акт, извършен от държавен служител при изпълнение на официалните му задължения, имат право да предявят искане за справедливо обезщетение ([192]).

(146) Второ, както е описано по-подробно в раздели 3.2.1 и 3.3.1, общите принципи, посочени в съображение 145, са отразени също така в специалните закони, с които се уреждат правомощията на органите за правоприлагане и национална сигурност. Например по отношение на наказателните разследвания в Наказателнопроцесуалния закон (НПЗ) се предвижда предприемането на принудителни мерки само ако това е изрично предвидено в НПЗ и в най-малката необходима степен за постигане на целта на разследването ([193]). По подобен начин в член 3 от Закона за защита на поверителността на комуникациите (ЗЗПК) се забранява достъпът до частни комуникации, освен въз основа на закона и при спазване на предвидените в него ограничения и гаранции. В областта на националната сигурност в Закона за националната разузнавателна служба (ЗНРС) се предвижда, че достъпът до информация за комуникации и местонахождения трябва да се извършва в съответствие със закона, и се предвижда налагане на наказателни санкции за злоупотреба с правомощия и нарушения на закона ([194]).

(147) Трето, обработването на лични данни от публични органи, включително за целите на правоприлагането и националната сигурност, подлежи на правилата за защита на личните данни съгласно ЗЗЛД ([195]). Като общ принцип в член 5, параграф 1 от ЗЗЛД от публичните органи се изисква да разработят политики за предотвратяване на „злоупотреба с лични данни и тяхната неправилна употреба, недискретно наблюдение и проследяване и др., както и за укрепване на достойнството на човешките същества и неприкосновеността на личния живот на физическите лица.“ В допълнение към това администраторът трябва да обработва личните данни по начин, който свежда до минимум възможността за нарушаване на неприкосновеността на личния живот на субекта на данните (член 3, параграф 6 от ЗЗЛД).

(148) Всички изисквания на ЗЗЛД, описани подробно в раздел 2, се отнасят до обработването на лични данни за целите на правоприлагането. Това включва основните принципи (като законосъобразност и добросъвестност, ограничаване на целта, точност, свеждане на данните до минимум, ограничаване на съхранението, сигурност и прозрачност), задълженията (например по отношение на уведомлението за нарушаване на сигурността на данните и чувствителни данни) и правата (за получаване на достъп, корекция, заличаване и спиране на използването).

(149) Докато обработването на лични данни за целите на националната сигурност подлежи на по-ограничен набор от разпоредби съгласно ЗЗЛД, основните принципи, както и правилата за надзор, правоприлагането и средствата за правна защита са приложими ([196]). По-специално в членове 3 и 4 от ЗЗЛД се уреждат общите принципи на защита на личните данни (законосъобразност и добросъвестност, ограничаване на целта, точност, свеждане на данните до минимум, сигурност и прозрачност) и индивидуалните права (правото да бъдеш информиран, правото на достъп и правата на корекция, заличаване и спиране на използването) ([197]). В член 4, параграф 5 от ЗЗЛД се предвижда също така правото на физическите лица на подходящи средства за правна защита за вреда, произтичаща от обработването на личните им данни, в надлежна и добросъвестна процедура. Това се допълва от по-конкретни задължения за обработване на лични данни само в минималната степен, необходима за постигане на предвидената цел, и за

([188]) Вж. приложение II, раздел 1.1.

([189]) Член 37, параграф 2 от Конституцията.

([190]) Член 16 и член 12, параграф 3 от Конституцията. Освен това в член 12, параграф 3 от Конституцията се определят извънредните обстоятелства, при които може да се извършват претърсвания и изземвания без заповед (макар че все пак се изисква *ex post* заповед), т.е. при flagrante delicto за престъпления, наказуеми с лишаване от свобода за срок от три години, ако има риск от унищожаване на доказателства и от това заподозряното лице да се укрие.

([191]) Член 68, параграф 1 от Закона за Конституционния съд.

([192]) Член 29, параграф 1 от Конституцията.

([193]) Член 199, параграф 1 от НПЗ. В по-общ план при упражняването на правомощията им по ЗКИ публичните органи трябва да зачитат основните права на заподозрените в престъпления и всяко друго засегнато лице (член 198, параграф 2 от НПЗ).

([194]) Член 14 от ЗНРС.

([195]) Вж. приложение II, раздел 1.2.

([196]) Член 58, параграф 1, точка 2 от ЗЗЛД. Вж. също така раздел 6 от Уведомление № 2021-5 (приложение I). Това изключение от определени разпоредби на ЗЗЛД се прилага само когато лични данни се обработват „за целите на националната сигурност“. След като ситуацията с националната сигурност, обуславяща обработването на личните данни приключи, не може да се прави позоваване на това изключение и се прилагат всички изисквания на ЗЗЛД.

([197]) Тези права могат да бъдат ограничавани само когато това се предвижда по закон и доколкото е необходимо и пропорционално за защитата на важна цел от обществен интерес или когато предоставянето на правото може да доведе до увреждане на живота или до телесна повреда на трета страна, или до неоправдано нарушаване на имуществени и други интереси на трета страна. Вж. раздел 6 от Уведомление № 2021-5.

минимален срок, за въвеждане на необходимите мерки за осигуряване на безопасно управление и подходящо обработване на данните (например технически, управленски и физически гаранции), както и въвеждането на мерки за надлежното разглеждане на индивидуални оплаквания (жалби) ([198]). Накрая, общите принципи на законност, необходимост и пропорционалност съгласно Конституцията (вж. съображение 145) се прилагат също така за обработването на лични данни за целите на националната сигурност.

(150) Физическите лица могат да се позовават на тези общи ограничения и гаранции пред независими надзорни органи (например КЗЛД и/или Националната комисия за човешки права, вж. съображения 177—178), както и пред съдилищата (вж. съображения 179—183) за получаване на правна защита.

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

(151) Законодателството на Република Корея налага редица ограничения на достъпа и използването на личните данни за целите на наказателното правоприлагане и осигурява механизми за надзор и правна защита в тази област, които са в съответствие с изискванията, посочени в съображения 141—143 от настоящото решение. Условията, при които може да се осъществи такъв достъп, и гаранциите, приложими за упражняването на тези правомощия, са разгледани подробно в следващите раздели.

3.2.1. *Правни основания, ограничения и гаранции*

(152) Обработваните от корейски администратори лични данни, които ще бъдат предавани от Съюза в съответствие с настоящото решение ([199]), могат да бъдат събирани от корейските органи за целите на наказателното правоприлагане в контекста на претърсването и изземването (въз основа на НПЗ), чрез достъп до данни от комуникации (въз основа на ЗЗПК) или чрез получаване на данни на абонати чрез искания за доброволно разкриване (въз основа на Закона за телекомуникационните дейности, „ЗТД“) ([200]).

3.2.1.1 Претърсвания и изземвания

(153) В НПЗ се предвижда, че претърсване или изземване може да се извърши само ако дадено лице е заподозряно в извършването на престъпление, ако това е необходимо за разследването и ако бъде установена връзка между разследването и лицето, което трябва да бъде претърсено или по отношение на което ще се извършва изземване ([201]). Освен това претърсване или изземване (като всяка принудителна мярка) може да се разреши/извърши само в най-малката необходима степен ([202]). Ако претърсването е свързано с компютърен диск или с друг носител за съхранение на данни, по принцип се изземват само самите данни (копирани или разпечатани), а не целият носител ([203]). Последният може да бъде изъят само когато се смята за съществено неизпълнимо съответните данни да бъдат разпечатани или копирани отделно или когато се смята за съществено неизпълнимо да бъде постигната по друг начин целта на претърсването ([204]). Следователно в НПЗ са предвидени ясни и точни правила за обхвата и прилагането на тези мерки, с което се гарантира, че намесата в правата на физическите лица в случай на претърсване или изземване ще бъде ограничена до необходимото за конкретното криминално разследване и пропорционално на преследваната цел.

([198]) Член 58, параграф 4 от ЗЗЛД.

([199]) Вж. приложение II, раздел 2.1. В официалното изявление на корейското правителство (раздел 2.1 от приложение II) се посочва също така възможността за събиране на информация за финансови операции с цел предотвратяване на изпирането на пари и финансирането на тероризма въз основа на Закона за докладване и използване на определена информация за финансови операции (ЗДИОИФО). С този закон обаче се налагат само задължения за разкриване на администраторите, които обработват кредитна информация съгласно ЗКИ и които подлежат на надзор от Комисията за финансов надзор (КФН) (вж. съображение 13). Тъй като обработването на лична кредитна информация от тези администратори е изключено от приложното поле на настоящото решение, ЗДИОИФО не е приложим за настоящата оценка.

([200]) В член 3 от ЗЗПК се споменава също така за Закона за военните съдилища като възможна правна основа за събирането на данни от комуникации. В този закон се урежда обаче събирането на информация за военен персонал и той може да се прилага по отношение на цивилни лица само в ограничен брой случаи (например ако военен персонал и цивилни лица биха извършили съвместно престъпление или ако физическо лице извърши престъпление срещу военнослужещи, може да бъде образувано производство пред военен съд, вж. член 2 от Закона за военните съдилища). Във всеки случай в него се предвиждат общи разпоредби, уреждащи претърсванията и изземванията, подобни на тези в НПЗ (вж. например членове 146—149 и 153—156 от Закона за военните съдилища), и в тях например се предвижда, че пощенски съобщения могат да се събират само за целите на дадено разследване и въз основа на заповед от Военния съд. Доколкото въз основа на този закон ще се събират електронни съобщения, ще се прилагат ограниченията и гаранциите на ЗЗПК. Вж. приложение II, раздел 2.2.2 и бележка под линия 50.

([201]) Член 215, параграфи 1 и 2 от НПЗ. Вж. също така член 106, параграф 1, членове 107 и 109 от НПЗ, в които се предвижда, че съдилищата могат да извършват претърсвания и изземвания, доколкото съответните предмети или лица се смятат за свързани с конкретния случай. Вж. приложение II, раздел 2.2.1.2.

([202]) Член 199, параграф 1 от НПЗ.

([203]) Член 106, параграф 3 от НПЗ.

([204]) Член 106, параграф 3 от НПЗ.

(154) По отношение на процедурните гаранции НПЗ съдържа изискване за получаване на заповед от съда за извършване на претърсване или изземване ([205]). Претърсване или изземване се разрешава само по изключение, а именно при спешни обстоятелства ([206]), *in loco* в момента на ареста или на задържането на заподозрян в извършване на престъпление ([207]), или когато предмет се изхвърля или се показва доброволно от заподозряно в извършване на престъпление лице или от трета страна (по отношение на лични данни — от самото физическо лице) ([208]). Незаконните претърсвания и изземвания подлежат на наказателни санкции ([209]) и всяко доказателство, получено в нарушение на НПЗ, се смята за недопустимо ([210]). Накрая, засегнатите физически лица винаги трябва да бъдат уведомявани за претърсването или изземването незабавно (включително за изземване на техни данни) ([211]), което на свой ред ще улесни упражняването на техните материални права и правото им на правна защита (вж. по-конкретно възможността за обжалване на изпълнението на заповед за изземване, вж. съображение 180).

3.2.1.2. Достъп до информация от комуникации

(155) Въз основа на ЗЗПК корейските органи за наказателно правоприлагане могат да прилагат два вида мерки ([212]): от една страна, събирането на „данни за потвърждаване на комуникации“ ([213]), което включва датата на електронните съобщения, началния и крайния им час, броя на изходящите и входящите повиквания, както и абонатния номер на другата страна, честотата на използване, регистрационни файлове за използването на телекомуникационни услуги и информация за местоположението (например от предавателните кули, където се приемат сигнали); и от друга страна, „мерки за ограничаване на комуникациите“, които обхващат както събирането на съдържанието на традиционните пощенски съобщения, така и прякото прихващане на съдържанието на електронни съобщения ([214]).

(156) Достъп до данни за потвърждаване на комуникация може да бъде предоставен само когато това е необходимо за провеждане на наказателно разследване или изпълнение на присъда ([215]) въз основа на заповед, издадена от съд ([216]). В това отношение в ЗЗПК се изисква предоставянето на подробна информация както в искането за издаване на заповедта (например относно причините за искането, връзката с целта/абоната и необходимите данни), така и в самата заповед (например относно целта, абоната и обхвата на мярката) ([217]). Събирането без заповед може да се извърши само ако е невъзможно да се получи съдебно разрешение поради спешност, като в

([205]) Член 215, параграфи 1 и 2 от НПЗ, член 113 от НПЗ. Когато подава искане за издаване на заповед, съответният орган трябва да представи материали, доказващи основанията за подозрението, че дадено физическо лице е извършило престъпление, че претърсването, огледът или изземването са необходими и че съответните предмети, които трябва да бъдат иззети, съществуват (член 108, параграф 1 от Правилника за наказателното производство). В самата заповед трябва да се посочат, наред с другото, имената на заподозряното в извършване на престъпление лице и престъплението; мястото, лицето или предметите, които трябва да бъдат претърсени, или предметите, които трябва да бъдат иззети; датата на издаване; и ефективният период на прилагане (член 114, параграф 1 във връзка с член 219 от НПЗ). Вж. приложение II, раздел 2.2.1.2.

([206]) Тоест, когато е невъзможно на мястото на престъплението да се получи заповед поради неотложност (член 216, параграф 3 от НПЗ), като в този случай все пак трябва да бъде получена заповед впоследствие и без забавяне (член 216, параграф 3 от НПЗ).

([207]) Член 216, параграфи 1 и 2 от НПЗ.

([208]) Член 218 от НПЗ. Освен това, както е пояснено в раздел 2.2.1.2 от приложение II, доброволно предоставени предмети се приемат като доказателство в съдебното производство само ако не съществува основателно съмнение относно доброволния характер на разкриването, което трябва да се докаже от прокурора.

([209]) Член 321 от Наказателния закон.

([210]) Член 308-2 от НПЗ. В допълнение към това дадено физическо лице (и неговият/нейният адвокат) може да присъства при изпълнението на заповед за претърсване или изземване и съответно също може да възрази по време на изпълнението на заповедта (членове 121 и 219 от НПЗ).

([211]) Членове 121 и 122 от НПЗ (по отношение на претърсвания) и член 219, във връзка с член 106, параграф 4 от НПЗ (по отношение на изземвания).

([212]) Вж. също приложение II, раздел 2.2.2.1. Тези мерки може да се прилагат с принудителната помощ на телекомуникационните оператори, като им се предостави писмено разрешение, получено от съд (член 9, параграф 2 от ЗЗПК), което трябва да бъде спазвано от операторите (член 15-2 от ЗЗПК и член 12 от Указа за прилагане на ЗЗПК). Доставчиците на телекомуникационни услуги могат да откажат съдействие, когато информацията за засегнатото физическо лице, посочена в писменото разрешение на съда (например телефонният номер на физическото лице), е невярна и те нямат право при никакви обстоятелства да разкриват пароли, използвани в електронните съобщения (член 9, параграф 4 от ЗЗПК).

([213]) Член 2, параграф 11 от ЗЗПК.

([214]) Вж. член 2, параграф 6 от ЗЗПК, който се отнася до „цензура“ (отваряне на писмо без съгласието на засегнатата страна или придобиване на знания, записване или задържане на съдържанието им с други средства), и член 2, параграф 7 от ЗЗПК, който се отнася до „подслушване“ (придобиване или записване на съдържанието на електронни съобщения чрез прослушване или кумулативно четене на звуците, думите, символите или изображенията на комуникациите чрез електронни и механични устройства без съгласието на засегнатата страна или с намеса в предаването и приемането им).

([215]) Член 13, параграф 1 от ЗЗПК. Вж. също приложение II, раздел 2.2.2.3. В допълнение данните за проследяване на местонахождението в реално време и данните за потвърждаване на комуникацията относно конкретна базова станция могат да бъдат събирани само за разследването на тежки престъпления или когато е трудно по друг начин да се предотврати извършването на престъпление или да се съберат доказателства (член 13, параграф 2 от ЗЗПК). Това отразява необходимостта от предоставяне на допълнителни гаранции в случай на нарушаващи неприкосновеността на личния живот мерки в съответствие с принципа на пропорционалността.

([216]) Членове 13 и 6 от ЗЗПК.

([217]) Вж. член 13, параграфи 3 и 9 във връзка с член 6, параграфи 4 и 6 от ЗЗПК.

този случай разрешението трябва да бъде получено и да бъде предоставено на доставчика на телекомуникационни услуги незабавно след изискването на данните ([218]). Ако съдът откаже да предостави последващо разрешение, събраните данни трябва да бъдат унищожени ([219]).

(157) По отношение на допълнителните гаранции във връзка със събирането на данни за потвърждаване на комуникации ЗЗПК съдържа специални изисквания за поддържане на архив и за прозрачност ([220]). По-специално органите за наказателно правоприлагане ([221]) и телекомуникационните доставчици ([222]) трябва да поддържат архив на направените искания и разкривания. В допълнение органите за наказателно правоприлагане трябва по принцип да уведомяват физическите лица за факта, че са събрани техни данни за потвърждаване на комуникации ([223]). Уведомяването може да бъде отложено само в извънредни обстоятелства въз основа на разрешение от директора на компетентната районна прокуратура ([224]). Това разрешение може да бъде предоставено само ако има вероятност уведомлението (1) да застраши националната сигурност, обществената сигурност и обществения ред, (2) да причини смърт или телесна повреда, (3) да попречи на справедливото съдебно производство (например да доведе до унищожаването на доказателства или до заплашването на свидетели) или (4) да оклевети заподозряното лице, жертвите или други лица, свързани със случая, или да накърни неприкосновеността на личния им живот. В тези случаи уведомлението трябва да бъде извършено в срок от 30 дни след като престане(ат) да съществува(т) основанието(основанията) за отлагането ([225]). След уведомяването физическите лица имат право да получат информация относно причините за събирането на техните данни ([226]).

(158) Прилагат се по-строги правила по отношение на мерките за ограничаване на комуникациите, които могат да се използват само когато има сериозно основание да се подозира, че се планират, извършват или са извършени определени тежки престъпления, изрично изброени в ЗЗПК ([227]). Освен това мерките за ограничаване на комуникациите могат да се прилагат само като мярка от последна инстанция и когато е трудно по друг начин да се предотврати извършването на престъпление, да се арестува престъпникът или да се съберат доказателства ([228]). Те трябва незабавно да бъдат прекратени, след като вече не са необходими, за да се гарантира, че нарушаването на неприкосновеността на комуникациите е възможно най-ограничено ([229]). Информация, която е била незаконно получена чрез мерки за ограничаване на комуникациите, не се допуска като доказателство в съдебно или дисциплинарно производство ([230]).

(159) По отношение на процедурните гаранции в ЗЗПК се съдържа изискване за получаване на заповед от съда за прилагане на мерки за ограничаване на комуникациите ([231]). Отново в ЗЗПК се изисква искането за издаване на заповед и самата заповед да съдържат подробна информация ([232]), включително относно обосновката на искането, както и относно комуникациите, които ще се събират (тези на заподозрения в разследването) ([233]). Тези мерки могат да бъдат приложени без заповед в случай на непосредствена заплаха от организирана престъпност или когато друго тежко престъпление, което може пряко да причини смърт или сериозна вреда, е неизбежно и е налице

([218]) Член 13, параграф 2 от ЗЗПК.
([219]) Член 13, параграф 3 от ЗЗПК.
([220]) Вж. приложение II, раздел 2.2.2.3.
([221]) Член 13, параграфи 5 и 6 от ЗЗК.
([222]) Член 13, параграф 7 от ЗЗПК. Освен това доставчиците на телекомуникационни услуги трябва да докладват на министъра на науката и ИКТ два пъти годишно за предоставянето на данни за потвърждаване на комуникации.
([223]) Вж. член 13-3, параграф 7 във връзка с член 9-2 от ЗЗПК. По-специално физическите лица трябва да бъдат уведомени в срок от 30 дни след вземането на решение да (не) се открие наказателно преследване или в срок от 30 дни след изтичането на една година от вземането на решение за прекратяване на обвинението (макар че уведомление се дава във всеки случай в срок от 30 дни след изтичането на една година от събирането на данните), вж. член 13-3, параграф 1 от ЗЗПК.
([224]) Член 13-3, параграфи 2—3 от ЗЗПК.
([225]) Член 13-3, параграф 4 от ЗЗПК.
([226]) Член 13-3, параграф 5 от ЗЗПК. По искане на физическото лице прокурор или съдебен полицейски служител трябва да представи причините в писмен вид в срок от 30 дни след получаване на искането, освен ако се прилага някое от горепосочените основания за отлагане на уведомлението (член 13-3, параграф 6 от ЗЗПК).
([227]) Например бунт, престъпления, свързани с наркотици или експлозиви, както и престъпления, свързани с националната сигурност, дипломатическите отношения или военните бази и съоръжения, вж. член 5, параграф 1 от ЗЗПК. Вж. също приложение II, раздел 2.2.2.2.
([228]) Член 3, параграф 2 член 5, параграф 1 от ЗЗПК.
([229]) Член 2 от Указа на прилагане на ЗЗПК.
([230]) Член 4 от ЗЗПК.
([231]) Член 6, параграфи 1— 2 и 5—6 от ЗЗПК.
([232]) В заявлението за издаване на заповед трябва да се посочат (1) съществените основания (prima facie) за съмнението, че се планира, извършва или е извършено някое от изброените престъпления, както и всички подкрепящи материали; (2) мерките за ограничаване на комуникациите, както и тяхната цел, обхват, задача и срок на действие; и (3) мястото, където ще се прилагат мерките, и начинът, по който ще се прилагат (член 6, параграф 4 от ЗЗПК и член 4, параграф 1 от Указа за прилагане на ЗЗПК). В самата заповед трябва да се посочат мерките, както и тяхната цел, обхват, срок на действие, място и начин на изпълнение (член 6, параграф 6 от ЗЗПК).
([233]) Целта на дадена мярка за ограничаване на комуникациите трябва да бъде насочена към конкретни пощенски пратки или електронни съобщения, изпратени или получени от заподозрения, или към пощенски пратки или електронни съобщения, изпратени или получени от заподозрения в определен период от време (член 5, параграф 2 от ЗЗПК).

извънредна ситуация, която прави невъзможно преминаването през редовната процедура ([234]). В този случай обаче заявлението за заповедта трябва да бъде подадено веднага след прилагането на мярката ([235]). Мерките за ограничаване на комуникациите могат да бъдат прилагани само за максимален срок от два месеца ([236]), който може да бъде удължен само с одобрение на съд, ако условията за прилагането им продължават да се спазват ([237]). Удължеият срок не може да надвишава общо една година или три години за някои особено тежки престъпления (например престъпления, свързани с бунт, с външна агресия, с националната сигурност) ([238]).

(160) Подобно на случая със събирането на данни за потвърждаване на комуникации ЗЗПК съдържа изисквания към доставчиците на телекомуникационни услуги ([239]) и към правоприлагащите органи ([240]) да поддържат архив на приложените мерки за ограничаване на комуникациите, както и изискване за уведомяване на засегнатото физическо лице, което може да бъде отложено по изключение, когато това е необходимо по съображения от важен обществен интерес ([241]).

(161) Накрая, неспазването на няколко от ограниченията и гаранциите на ЗЗПК (включително например задълженията за получаване на заповед, за поддържане на архив и за уведомяване на физическото лице), както по отношение на събирането на данни за потвърждаване на комуникациите, така и по отношение на използването на мерките за ограничаване на комуникациите, подлежи на наказателни санкции ([242]).

(162) Правомощията на органите за наказателно правоприлагане за събиране на данни от комуникации въз основа на ЗЗПК (както на съдържанието на комуникациите, така и на данни за потвърждаване на комуникациите) следователно са ограничени от ясни и точни правила и изискват прилагането на редица гаранции. По-специално с тези гаранции се гарантира надзорът върху изпълнението на мерките, както ex ante (чрез предварително съдебно одобрение), така и ex post (чрез изисквания за поддържане на архив и докладване), и се улеснява достъпът на физическите лица до ефективни средства за правна защита (като се осигурява те да са информирани за събирането на техните данни).

3.2.1.3. Искане за доброволно разкриване на данни на абонат

(163) Освен че се позовават на задължителните мерки, описани в съображения 153—162, корейските правоприлагащи органи могат да поискат от доставчиците на телекомуникационни услуги доброволно да изпълнят искане за „данни от комуникации“ в подкрепа на наказателно производство, разследване или изпълнение на присъда (член 83, параграф 3 от ЗТД). Тази възможност съществува само по отношение на ограничени набори от данни, т.е. името, регистрационния номер на местно лице, адреса и телефонния номер на ползвателите, датите, на които ползвателите се абонират или прекратяват абонамента си, както и идентификационните кодове на ползвателите (т.е. кодове, използвани за идентифициране на законния ползвател на компютърни системи или комуникационни мрежи) ([243]). Тъй като само физически лица, които сключват преки договори с корейски доставчик на телекомуникационни услуги, се смятат за „ползватели“ ([244]), физическите лица от ЕС, чиито данни се предават на Република Корея, обикновено не биха попаднали в тази категория ([245]).

(164) Различни ограничения се прилагат за такива доброволни разкривания както по отношение на упражняването на правомощията от правоприлагащия орган, така и по отношение на отговора на телекомуникационния оператор. В по-общ план правоприлагащите органи трябва да действат в съответствие с конституционните принципи за необходимост и пропорционалност (член 12, параграф 1 и член 37, параграф 2 от Конституцията), включително когато искат информация на доброволна основа. В допълнение те трябва да спазват ЗЗЛД, по-специално като събират само минимални лични данни до степента, необходима за постигане на предвидената цел, по такъв начин, че да сведат до минимум въздействието върху неприкосновеността на личния живот на физическите лица (член 3, параграфи 1

([234]) Член 8, параграф 1 от ЗЗПК. Събирането на информация при извънредни ситуации обаче винаги трябва да се извършва в съответствие с „изявление за извънредна цензура/извънредно подслушване“, а органът, който извършва събирането, трябва да води регистър за всяка спешна мярка (член 8, член 4 от ЗЗПК).

([235]) Събирането трябва да бъде прекратено незабавно, ако правоприлагащият орган не успее да получи разрешение от съда в рамките на 36 часа (член 8, параграф 2 от ЗЗПК), и в този случай, както е пояснено в раздел 2.2.2.2 от приложение II, събраните данни по принцип ще бъдат унищожени. Съдът трябва да бъде уведомен също така в случаите, когато спешните мерки са завършени в толкова кратък срок, че необходимостта от разрешение отпада (например ако заподозреният е арестуван веднага след започване на прихващането, вж. член 8, параграф 5 от ЗЗПК). В този случай на съда трябва да бъде предоставена информация относно целта, предмета, обхвата, периода, мястото на изпълнение и метода на събиране, както и относно основанията за неподаване на искане за съдебно разрешение (член 8, параграфи 6—7 от ЗЗПК).

([236]) Член 6, параграф 7 от ЗЗПК. Ако целта на мерките бъде постигната по-рано в рамките на този период, мерките трябва да бъдат преустановени незабавно.

([237]) Член 6, параграфи 7—8 от ЗЗПК.

([238]) Член 6, параграф 8 от ЗЗПК.

([239]) Член 9, параграф 3 от ЗЗПК.

([240]) Член 18, параграф 1 от Указа на прилагане на ЗЗПК.

([241]) По-специално прокурорът трябва да уведоми физическото лице в срок от 30 дни от издаването на присъдата или от разпореждането за неподвеждане под отговорност или за отказ от арест (член 9-2, параграф 1 от ЗЗПК). Уведомлението може да бъде отсрочено с одобрението на ръководителя на районната прокуратура, ако има вероятност то сериозно да застраши националната сигурност или да нарушени обществената сигурност и обществения ред, или когато има вероятност да причини значителни увреждания на живота и телесни повреди на други хора (член 9-2, параграфи 4—6 от ЗЗПК).

([242]) Членове 16 и 17 от ЗЗПК.

([243]) Член 83, параграф 3 от ЗТД. Вж. също приложение II, раздел 2.2.3.

([244]) Член 2, параграф 9 от ЗТД.

([245]) Вж. също приложение II, раздел 2.2.3.

и 6 от ЗЗЛД). По-специално исканията за получаване на данни от комуникации въз основа на ЗТД трябва да бъдат направени в писмен вид и да съдържат причините за искането, връзката със съответния ползвател и обхвата на исканите данни ([246]).

(165) Доставчиците на телекомуникационни услуги не са задължени да изпълняват тези искания и могат да сторят това само в съответствие със ЗЗЛД. По-специално това означава, че те трябва да балансират различните засегнати интереси и не могат да предоставят данните, ако има вероятност това да накърни недобросъвестно интересите на физическото лице или на трета страна. ([247]) Такъв би бил например случаят, в който е ясно, че отправящият искането орган е злоупотребил с правомощието си ([248]). Телекомуникационните оператори трябва да поддържат архив на разкриваните данни съгласно ЗТД и да докладват на министъра на науката и ИКТ два пъти годишно ([249]).

(166) В допълнение към това, в съответствие с раздел 3 от Уведомление № 2021-5 (приложение I), доставчиците на телекомуникационни услуги по принцип трябва да уведомят съответното физическо лице, когато доброволно изпълнят искането ([250]). На свой ред това ще даде възможност на лицето да упражни правата си и, в случай че данните му бъдат разкрити неправомерно, да получи правна защита срещу администратора (например за разкриването на данните в нарушение на ЗЗЛД или в отговор на искане, за което е ясно, че е било непропорционално) или срещу правоприлагащия орган (например за извършване на действие извън границите на необходимото и пропорционалното или за неспазване на процедурните изисквания на ЗТД.)

3.2.2. *По-нататъшно използване на събраната информация*

(167) Обработването на лични данни, събрани от корейските органи за наказателно правоприлагане, подлежи на спазване на всички изисквания на ЗЗЛД, включително по отношение на ограничаването на целите (член 3, параграфи 1—2 от ЗЗЛД), законосъобразността на използването и предоставянето им на трети страни (членове 15, 17 и 18 от ЗЗЛД), международното предаване (членове 17 и 18 от ЗЗЛД във връзка с раздел 2 от Уведомление 2021-5) ([251]), пропорционалността/свеждането на данните до минимум (член 3, параграфи 1 и 6 от ЗЗЛД) и ограничаване на съхранението (член 21 от ЗЗЛД) ([252]).

(168) По отношение на съдържанието на комуникациите, придобити чрез прилагането на мерки за ограничаване на комуникациите, в ЗЗПК по-специално се предвижда ограничаването им до възможното им използване в разследването, наказателно преследване или предотвратяване на тежки престъпления ([253]); в дисциплинарни производства за същите престъпления; в искове за вреди, заведени от страна по комуникацията или когато това е изрично разрешено съгласно други закони ([254]). Освен това събраното съдържание на комуникации, предадени по интернет, може да бъде запазено с одобрението на съда, който е разрешил мерките за ограничаване на комуникациите ([255]), с оглед на тяхното използване в разследването, наказателно преследване или предотвратяване на тежки престъпления ([256]). В по-общ план в ЗЗПК се забранява разкриването на поверителна информация, получена от мерки за ограничаване на комуникациите, както и използването на такава информация за увреждане на репутацията на тези, спрямо които са били приложени мерките ([257]).

3.2.3. *Надзор*

(169) В Корея различни органи упражняват надзор върху дейностите на органите за наказателно правоприлагане ([258]).

([246]) Член 83, параграф 4 от ЗТД. Когато е невъзможно да се предостави писмено искане поради спешност, то трябва да бъде предоставено веднага щом отпадне причината за спешността (член 83, параграф 4 от ЗТД).

([247]) Член 18, параграф 2 от ЗЗЛД.

([248]) Решение на Върховния съд № 2012Da105482, 10 март 2016 г. Вж. също приложение II, раздел 2.2.3 относно това решение на Върховния съд.

([249]) Член 83, параграфи 5—6 от ЗТД.

([250]) Това изискване подлежи на ограничени и квалифицирани изключения, по-специално ако и доколкото уведомлението би застрашило текущо наказателно разследване или има вероятност да навреди на живота или да нанесе телесна повреда на друго лице, когато тези права или интереси са явно по-висши от правата на субекта на данните. Вж. раздел 3, подточка iii) (1) от Уведомлението.

([251]) По-конкретно корейските публични органи трябва да гарантират чрез правно обвързващ инструмент ниво на защита, което е равностойно на ЗЗЛД, вж. също съображение 90.

([252]) Вж. също приложение II, раздел 1.2.

([253]) Вж. съображение 158.

([254]) Член 12 от ЗЗПК. Вж. приложение II, раздел 2.2.2.2.

([255]) Прокурорът или полицейският служител, който изпълнява мерките за ограничаване на комуникациите, трябва да избере електронните съобщения, които трябва да бъдат запазени, в рамките на 14 дни след края на мерките и да поиска одобрение от съда (когато става въпрос за полицейски служител молбата трябва да бъде подадена до прокурора, който от своя страна подава искането до съда), вж. член 12-2, параграфи 1 и 2 от ЗЗПК.

([256]) Искането за такова разрешение трябва да съдържа информация относно мерките за ограничаване на комуникациите, резюме на резултатите от мерките, причините за запазването (заедно с подкрепящи материали) и електронните съобщения, които трябва да бъдат запазени (член 12-2, параграф 3 от ЗЗПК). При липса на такова искане придобитите данни трябва да бъдат заличени в рамките на 14 дни след приключване на мерките за ограничаване на комуникациите (член 12-2, параграф 5 от ЗЗПК), а ако искането бъде отхвърлено — в рамките на седем дни (член 12-2, параграф 5 от ЗЗПК). И в двата случая до съда, разрешил събирането, трябва да бъде подаден доклад в рамките на седем дни.

([257]) Член 11, параграф 2 от Указа за прилагане на ЗЗПК.

([258]) Вж. приложение II, раздел 2.3.

(170) Първо, полицията подлежи на вътрешен надзор от генерален инспектор ([259]), който контролира законосъобразността, включително по отношение на възможни нарушения на правата на човека. Функцията на генерален инспектор е създадена в изпълнение на Закона за одитите в публичния сектор, с който се насърчава създаването на самоодитиращи се органи, и съдържа специални изисквания към техния състав и задачи. По-конкретно законът изисква ръководителят на самоодитиращия се орган да се назначава измежду външни за съответния орган лица (например бивши съдии, професори) за период от две до пет години ([260]), да може да бъде освободен само по основателни причини (например когато не е в състояние да изпълнява задълженията си по здравословни причини, когато е обект на дисциплинарно производство) ([261]) и да се гарантира независимостта му във възможно най-голяма степен ([262]). Възпрепятстването на вътрешния одит подлежи на административни глоби ([263]). Одитните доклади (които могат да включват препоръки, искания за дисциплинарно производство и искания за обезщетение за вреди или корекции) са съобщават на ръководителя на съответния публичен орган, т.е. на Съвета за одит и инспекции (СОИ) ([264]) и по-принцип се оповестяват публично ([265]). Резултатите от изпълнението на доклада трябва да бъдат съобщени на СОИ ([266]) (вж. съображение 173 относно ролята и правомощията за надзор на СОИ).

(171) Второ, КЗЛД упражнява надзор върху спазването от страна на органите за наказателно правоприлагане на обработването на данни съгласно ЗЗЛД и други закони за защита на неприкосновеността на личния живот на физическите лица, включително законите за уреждане на събирането на (електронни) доказателства за целите на наказателното правоприлагане, както е описано в раздел 3.2.1 ([267]). По-специално, тъй като надзорът на КЗЛД обхваща законосъобразността и добросъвестността на събирането и обработването на данни (член 3, параграф 1 от ЗЗЛД), които ще бъдат нарушени, ако достъпът до личните данни и използването им са в нарушение на тези закони ([268]), КЗЛД може да разследва и да осигури спазването също така на ограниченията и гаранциите, описани в раздел 3.2.1 ([269]). При упражняването на тази надзорна роля КЗЛД може да използва всички свои правомощия за разследване и коригиране, описани подробно в раздел 2.4.2. Още преди неотдавнашното изменение на ЗЗЛД (т.е. в предишната си надзорна роля по отношение на публичния сектор) КЗЛД осъществи няколко надзорни дейности, свързани с обработването на лични данни от органите за наказателно правоприлагане, например в контекста на разпита на заподозрени лица (дело № 2013-16, 26 август 2013 г.), по отношение на даването на известия на физически лица относно налагането на административни глоби (дело № 2015-02-04, 26 януари 2015 г.), споделянето на данни с други органи (дело № 2018-15-146, 9 юли 2018 г., дело № 2018-25-308, 10 декември 2018 г.; дело № 2019-02-015, 29 януари 2019 г.), събирането на пръстови отпечатъци или снимки (дело № 2019-17-273, 9 септември 2019 г.), използването на дронове (дело № 2020-01-004, 13 януари 2020 г.). В тези случаи КЗЛД разследва спазването на няколко разпоредби на ЗЗЛД (например законосъобразността на обработването, принципите за ограничаване на целта и за свеждане на данните до минимум), но така също и съответни разпоредби на други закони, като Наказателнопроцесуалния закон, и където е необходимо, е издала препоръки за привеждане на обработването в съответствие с изискванията за защита на данните.

(172) Трето, независим надзор се осъществява от Националната комисия по правата на човека (НКПЧ) ([270]), която може да разследва нарушения на правата на неприкосновеност на личния живот и на поверителността на кореспонденцията като част от своя мандат за защита на основните права по членове 10—22 от Конституцията. Националната комисия по правата на човека се състои от 11 комисари, които трябва да притежават конкретни квалификации ([271]) и които се назначават по предложение на президента в съответствие с предвидените по закон процедури. По-специално четирима комисари се назначават по предложение на Националното събрание, четирима — по предложение на президента, и трима се назначават по предложение на главния съдия на Върховния съд ([272]). Председателят се назначава от президента измежду комисарите и трябва да бъде утвърден от Националното събрание ([273]). Комисарите (включително председателят) се назначават за срок от три години,

([259]) Вж. приложение II, раздел 2.3.1. Вж. също https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) По същия начин одиторите се назначават въз основа на специфични условия, определени в закона, вж. членове 16 и сл. от Закона за одитите в публичния сектор.
([261]) Членове 8—11 от Закона за одитите в държавния сектор.
([262]) Член 7 от Закона за одитите в държавния сектор.
([263]) Член 41 от Закона за одитите в държавния сектор.
([264]) Член 23, параграф 1 от Закона за одитите в държавния сектор.
([265]) Член 26 от Закона за одитите в държавния сектор.
([266]) Член 23, параграф 3 от Закона за одитите в държавния сектор.
([267]) Вж. член 7-8, параграфи 3 и 4 и член 7-9, параграф 5 от ЗЗЛД.
([268]) Вж. също Уведомление на КЗЛД № 2021-5, раздел 6 (приложение I).
([269]) Вж. също приложение II, раздел 2.3.4.
([270]) Член 1 от Закона за Комисията по правата на човека (наричан по-долу „Закон за НКПЧ“).
([271]) За да бъде назначен, комисарят трябва (1) да е работил най-малко десет години в университет или в упълномощен научноизследователски институт, поне като доцент; (2) да е работил като съдия, прокурор или адвокат в продължение на поне десет години; (3) да е участвал в дейности, свързани с правата на човека, в продължение на поне десет години (например в организация с нестопанска цел, неправителствена организация или международна организация); или 4) да е бил препоръчан от групи на гражданското общество (член 5, параграф 3 от Закона за НКПЧ). След назначаването им на комисарите в НКПЧ е забранено да заемат паралелна длъжност в Националното събрание, местните съвети или в който и да е държавен орган или орган на местното самоуправление (в качество на държавни служители), вж. член 10 от Закона за НКПЧ.
([272]) Член 5, параграфи 1 и 2 от Закона за НКПЧ.
([273]) Член 5, параграф 5 от Закона за НКПЧ.

който може да се подновява, и могат да бъдат освободени от длъжност само в случай че им е наложено наказание лишаване от свобода или вече не са в състояние да изпълняват задълженията си поради продължителна физическа или психическа слабост (в този случай две трети от комисарите трябва да се съгласят с освобождаването от длъжност) ([274]). Като част от разследването си НКПЧ може да поиска предоставяне на съответните материали, да извършва проверки и да призовава физически лица да дават показания ([275]). По отношение на правомощията за корекции НКПЧ може да издава (публични) препоръки за подобряване или коригиране на конкретни политики и практики, на които публичните органи трябва да отговорят с предложен план за изпълнение ([276]). Ако съответният орган не изпълни препоръките, той трябва да информира Комисията за това ([277]), като тя на свой ред може да оповести неизпълнението на Националното събрание и/или да го оповести публично. Съгласно официалното изявление на корейското правителство (раздел 2.3.5 от приложение II) корейските органи като цяло изпълняват препоръките на НКПЧ и имат силен стимул да го правят, тъй като тяхното изпълнение се преценява като част от общата, постоянна оценка, извършвана под ръководството на кабинета на министър-председателя. Годишните данни за дейността ѝ показват, че НКПЧ упражнява активен надзор върху дейностите на органите за наказателно правоприлагане въз основа на индивидуални петиции или посредством служебни разследвания ([278]).

(173) Четвърто, общият надзор на законосъобразността на дейностите на публичните органи се извършва от СОИ, който проверява приходите и разходите на държавата, но като цяло упражнява също така надзор върху спазването на задълженията на публичните органи с оглед подобряване на функционирането на публичната администрация ([279]). Съветът за одит и инспекции е създаден официално под ръководството на президента на Република Корея, но запазва независим статут по отношение на задълженията си ([280]). Освен това той има пълна независимост по отношение на назначаването, освобождаването и организирането на служителите си, както и по отношение на съставянето на бюджета си ([281]). Съветът за одит и инспекции се състои от председател (назначен от президента, със съгласието на Националното събрание) ([282]) и шестима комисари (назначени от президента по препоръка на председателя) ([283]), които трябва да имат специфични квалификации, определени по закон ([284]), и могат да бъдат освобождавани от длъжност само в случай на импийчмънт, на осъждане на лишаване от свобода или на невъзможност да изпълняват задълженията си поради продължителна умствена или физическа слабост ([285]). Съветът за одит и инспекции извършва общ одит на годишна база, но може да извършва и конкретни одити по въпроси от особен интерес. При извършването на одит или инспекция Съветът за одит и инспекции може да поиска представянето на документи и да изиска присъствието на физически лица ([286]). Съветът за одит и инспекции може да издава препоръки, да изисква дисциплинарни производства или да подава наказателни жалби ([287]).

(174) Накрая, Националното събрание може да разследва и проверява ([288]) дейностите ([289]) на публичните органи чрез парламентарен контрол. То може да изисква разкриването на документи, задължителното явяване на свидетели ([290]), да препоръчва корективни мерки (ако установи, че са извършени незаконосъобразни или

([274]) Член 7, параграф 1 и член 8 от Закона за НКПЧ.

([275]) Член 36 от Закона за НКПЧ. В съответствие с член 6, параграф 7 от Закона предоставянето на материали или статии може да бъде отказано, ако това би накърнило държавна тайна, което може да окаже съществено въздействие върху държавната сигурност или дипломатическите отношения, или би представлявало сериозна пречка за наказателно разследване или висящ съдебен процес. В такива случаи НКПЧ може да поиска допълнителна информация от ръководителя на съответната агенция (който трябва да спазва добросъвестно изискванията), когато това е необходимо, за да провери дали отказът за предоставяне на информация е обоснован.

([276]) Член 25, параграфи 1и 3 от Закона за НКПЧ.

([277]) Член 25, параграф 4 от Закона за НКПЧ.

([278]) Например в периода 2015—2019 г. НКПЧ е получавала между 1 380 и 1 699 петиции срещу органите на наказателното правоприлагане годишно и е обработила също толкова голям брой (например през 2018 г. тя е разгледала 1 546 жалби срещу полицията, а през 2019 г. те са 1 249); тя е провела също така няколко служебни разследвания, описани по-подробно в годишния доклад на НКПЧ за 2018 г. (достъпен на следния адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) и в годишния доклад за 2019 г. (достъпен на следния адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Членове 20 и 24 от Закона за Съвета за одити и инспекции (наричан по-долу „Закона за СОИ“). Вж. приложение II, 2.3.2.

([280]) Член 2, параграф 1 от Закона за СОИ.

([281]) Член 2, параграф 2от Закона за СОИ.

([282]) Член 4, параграф 1 от Закона за СОИ.

([283]) Член 5, параграф 1 и член 6 от Закона за СОИ.

([284]) Например да са работили като съдия, прокурор или адвокат в продължение на поне десет години, да са работили като държавен служител, преподавател или на по-висока длъжност в университет в продължение на поне осем години или да са работили в продължение на поне десет години в дружество, чиито акции се търгуват на фондовата борса, или в институция с държавно участие (от които поне пет години като изпълнителен директор), вж. член 7 от Закона за СОИ. Освен това на комисарите е забранено да участват в политически дейности, както и да заемат едновременно длъжности в Националното събрание, административни органи, организации, подлежащи на одити и инспекции от СОИ, или други длъжности или позиции, за които се получава възнаграждение (член 9 от Закона за СОИ).

([285]) Член 8 от Закона за СОИ.

([286]) Вж. например член 27 от Закона за СОИ.

([287]) Членове 24 и 31—35 от Закона за СОИ.

([288]) Член 128 от Закона за Националното събрание и членове 2, 3 и 15 от Закона за инспекцията и разследването на държавната администрация. Това включва годишни инспекции на държавните дела като цяло и разследване на конкретни въпроси.

([289]) Вж. приложение, раздел 2.2.3.

([290]) Член 10, параграф 1 от Закона за инспекцията и разследването на държавната администрация. Вж. също членове 128 и 129 от Закона за Националното събрание.

неправомерни действия) ([291]) и да разкрива публично резултатите от своите констатации ([292]). Ако Националното събрание поиска прилагането на корективни мерки — които например може да включват присъждане на обезщетение, провеждане на дисциплинарно производство или подобряване на вътрешните процедури — съответният публичен орган трябва да действа незабавно и да докладва за резултата на Националното събрание ([293]).

3.2.4. *Средства за правна защита*

(175) Корейската система предоставя различни (съдебни) механизми за получаване на средства за правна защита, включително обезщетение за вреди.

(176) Първо, в съответствие със ЗЗЛД физическите лица могат да упражняват правото си на достъп, коригиране, заличаване и спиране на използването на лични данни, обработени за целите на наказателното правоприлагане ([294]).

(177) Второ, физическите лица могат да използват различни механизми за правна защита съгласно ЗЗЛД, ако техните данни са обработени от орган за наказателно правоприлагане в нарушение на ЗЗЛД или в нарушение на ограниченията и гаранциите, уреждащи събирането на лични данни в други закони (например ЗКИ или ЗЗПК, вж. съображение 171). По-специално физическите лица могат да подадат жалба до КЗЛД (включително чрез Информационния център по въпросите на поверителността, управляван от Корейската агенция за интернет и сигурност ([295])) или до Комитета за медиация при спорове ([296]). Тези възможности за използване на средства за правна защита не подлежат на допълнителни изисквания за допустимост. Въз основа на Закона за административното съдопроизводство физическите лица могат допълнително да обжалват/оспорват решенията или бездействието на КЗЛД (вж. съображение 132).

(178) Трето, всяко физическо лице ([297]) може да подаде жалба до НКПЧ относно нарушаване на правото на неприкосновеност на личния му живот и на защита на данните от корейски орган за наказателно правоприлагане. Националната комисия по правата на човека може да препоръча коригирането или подобряването на съответен закон, институция, политика или практика ([298]) или прилагането на средства за правна защита, като медиация ([299]), спиране на нарушаването на правата на човека, обезщетение за вреди и мерки за предотвратяване на повтарянето на същото или на подобно нарушение ([300]). В съответствие с официалното изявление на корейското правителство (раздел 2.4.2 от приложение II) това може да включва заличаването на незаконно събрани данни. Макар че НКПЧ няма правомощие да издава обвързващи решения, тя предлага по-неформален, по-евтин и леснодостъпен механизъм за защита, по-конкретно, както е пояснено в приложение II, раздел 2.4.2, поради това че не изисква доказване на действителна вреда, за да бъде разследвана дадена жалба ([301]). С това се гарантира, че жалбите на физически лица относно събирането на техни данни могат да бъдат разследвани, дори ако засегнатото физическо лице не може да докаже дали в действителност данните му/ѝ са били събрани (например поради това, че физическото лице все още не е било уведомено). Годишните доклади за дейността на НКПЧ показват, че физическите лица се възползват от този механизъм на практика, за да оспорят дейностите на органите за наказателно правоприлагане, включително по отношение на обработването на лични данни ([302]). Ако дадено физическо лице не е удовлетворено от резултата от

([291]) Член 16, параграф 2 от Закона за инспекцията и разследването на държавната администрация.
([292]) Член 12-2, параграф 3 от Закона за инспекцията и разследването на държавната администрация.
([293]) Член 16, параграф 3 от Закона за инспекцията и разследването на държавната администрация.
([294]) Това право може да бъде упражнено пряко спрямо компетентния орган или косвено чрез КЗЛД (член 35, параграф 2 от ЗЗЛД). Както е описано в съображения 76—78, изключения от тези права са възможни само когато е необходимо за защита на важни (обществени) интереси.
([295]) Член 62 от ЗЗЛД.
([296]) Членове 40—50 от ЗЗЛД и членове 48-2—57 от Указа за прилагане на ЗЗЛД. Вж. също приложение II, раздел 2.4.1.
([297]) Както е пояснено в приложение II, раздел 2.4.2, въпреки че член 4 от Закона за НКПЧ се отнася за граждани и чужденци, пребиваващи в Република Корея, терминът „пребиваващ“ отразява по-скоро понятието за юрисдикция, отколкото за територия. Ето защо, ако основните права на чужденец извън Корея са нарушени от национални институции в Корея, това физическо лице може да подаде жалба до НКПЧ. Такъв би бил случаят, ако корейските публични органи са получили незаконен достъп до личните данни на чужденец, предадени на Корея. Вж. по-специално пояснението, предоставено на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Член 44 от Закона за НКПЧ.
([299]) Физическо лице може също така да поиска жалбата да бъде решена чрез медиация, вж. членове 42 и сл. от Закона за НКПЧ.
([300]) Член 42, параграф 4 от Закона за НКПЧ. Освен това НКПЧ може да приеме спешни мерки за облекчение в случай на текущо нарушение, което има вероятност да причини трудно поправими вреди, вж. член 48 от Закона за НКПЧ.
([301]) По принцип жалбата трябва да бъде подадена в рамките на една година от нарушението, но НКПЧ все пак може да реши да разследва жалба, която е подадена след този срок, стига да не е изтекъл давностният срок по наказателното или гражданското право (член 32, параграф 1, точка 4 от Закона за НКПЧ).
([302]) Например НКПЧ в миналото е разглеждала жалби и е издавала препоръки по отношение на незаконни изземвания и нарушение на изискването за информиране на физическите лица за изземване (вж. стр. 80 и 91 от годишния доклад на НКПЧ за 2018 г., достъпен на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), както и незаконното обработване на лични данни от полицията, прокуратурата и съдилищата (вж. стр. 157—158 от годишния доклад на НКПЧ за 2019 г., достъпен на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, и стр. 76 от годишния доклад на НКПЧ за 2019 г., достъпен на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

процедурата пред НКПЧ, то може да оспори решенията на НКПЧ (например решение да не се продължава разследването на жалба ([303])) и препоръките на НКПЧ пред корейските съдилища съгласно Закона за административното съдопроизводство (вж. съображение 181) ([304]). Освен това процедурата пред НКПЧ може да улесни допълнително достъпа до съдилищата, тъй като физическото лице може да потърси допълнителна правна защита срещу публичния орган, който неправомерно е обработил неговите лични данни, въз основа на констатациите на НКПЧ в съответствие с процедурите, описани в съображения 181—183.

(179) Накрая, физическите лица разполагат с различни средства за съдебна защита, които им позволяват да се позоват на ограниченията и гаранциите, описани в раздел 3.2.1, за да получат защита ([305]).

(180) По отношение на изземванията (включително на данни) в НПЗ се предвижда възможност за възразяване или оспорване на заповед чрез „квазижалба“, като се подаде петиция до компетентния съд с искане за отмяна или промяна на разпореждането на прокурор или на полицейски служител ([306]).

(181) Най-общо физическите лица могат да оспорват действията ([307]) или бездействията ([308]) на публичните органи (включително на органите за наказателно правоприлагане) по реда на Закона за административното съдопроизводство ([309]). Дадено административно действие се смята за „подлежащо на оспорване разпореждане“, ако има пряко въздействие върху гражданските права и задължения ([310]), какъвто е случаят, както се потвърждава от корейското правителство (раздел 2.4.3 от приложение II), с мерките за събирането на лични данни, било то пряко (например с прихващане на комуникации) или чрез обвързващи искания за разкриване (например към доставчик на услуги), или чрез искания за доброволно сътрудничество. За да бъде допустима жалба по реда на Закона за административното съдопроизводство, физическото лице трябва да има правен интерес от завеждане на иска ([311]). Съгласно съдебната практика на Върховния съд „правен интерес“ се тълкува като „правно защитен интерес“, т.е. пряк и конкретен интерес, защитен от закони и подзаконови актове, на които се основават административните разпореждания (т.е. не общи, косвени и абстрактни интереси на обществото) ([312]). Физическите лица имат правен интерес в случай на нарушаване на ограничения и гаранции, приложими по отношение на събирането на техните лични данни за целите на наказателното правоприлагане (съгласно специални закони или ЗЗЛД). Въз основа на Закона за административното съдопроизводство даден съд може да реши да отмени или да измени незаконно разпореждане, да издаде констатация за нищожност (т.е. констатация, че разпореждането няма правно действие или че не съществува в правния ред) или да издаде констатация, че бездействието е незаконно ([313]). Окончателното съдебно решение по Закона за административните спорове е задължително за страните ([314]).

([303]) Например, ако НКПЧ по изключение не може да провери определени материали или съоръжения, поради това че те касаят държавни тайни, които могат да окажат съществено въздействие върху държавната сигурност или дипломатическите отношения, или ако проверката би представлявала сериозна пречка за наказателно разследване или висящ съдебен процес и когато това възпрепятства НКПЧ да извърши необходимото разследване за оценка по същество на подаденото оплакване, тя ще информира физическото лице за причините за отхвърлянето на жалбата в съответствие с член 39 от Закона за НКПЧ. В този случай физическото лице може да оспори решението на НКПЧ по реда на Закона за административното съдопроизводство.

([304]) Вж. например Решение 2007Nu27259 на Върховния съд на Сеул, 18 април 2008 г., потвърдено с Решение 2008Du7854 на Върховния съд, 9 октомври 2008 г.; Решение 2017Nu69382 на Върховния съд на Сеул, 2 февруари 2018 г.

([305]) Вж. приложение II, 2.4.3.

([306]) Член 417 от НПЗ във връзка с член 414, параграф 2 от НПЗ. Вж. също Решение № 97Mo66 на Върховния съд от 29 септември 1997 г.

([307]) Законът за административното съдопроизводство се позовава на „разпореждане“, т.е. упражняването или отказа от упражняване на публично правомощие в конкретен случай.

([308]) Съгласно Закона за административното съдопроизводство това се отнася до продължително неизпълнение на разпореждане от страна на административна агенция противно на законово задължение за това.

([309]) Административно обжалване може да бъде подадено за пръв път пред комисии за административни обжалвания, създадени към определени публични органи (например НРС, НКПЧ), или пред Централната комисия за административни обжалвания, създадена към Комисията за борба с корупцията и гражданските права (член 6 от Закона за административните обжалвания и член 18, параграф 1 от Закона за административното съдопроизводство) като по-неформален начин на защита. Въпреки това иск може да бъде предявен и директно пред корейските съдилища съгласно Закона за административното съдопроизводство.

([310]) Решение 98Du18435 на Върховния съд, 22 октомври 1999 г., Решение 99Du1113 на Върховния съд, 8 септември 2000 г., и Решение 2010Du3541 на Върховния съд, 27 септември 2012 г.

([311]) Членове 12, 35 и 36 от Закона за административното съдопроизводство. В допълнение искането за отмяна/изменение на разпореждане и искането за потвърждаване на незаконосъобразността на бездействие трябва да бъдат подадени в срок от 90 дни от датата, на която физическото лице е узнало за разпореждането/бездействието, и по принцип не по-късно от една година от датата на издаване на разпореждането/настъпване на бездействието, освен ако няма основателни причини (член 20 и член 38, параграф 2 от Закона за административното съдопроизводство). Върховният съд тълкува широко понятието „основателни причини“ и изисква да се прецени дали е социално приемливо да се допусне закъсняла жалба с оглед на всички обстоятелства по делото (Решение 90Nu6521 на Върховния съд, 28 юни 1991 г.). Както е потвърдено от корейското правителство в раздел 2.4.3 от приложение II, това включва (но не се ограничава до) причини за забавяне, за които съответната страна не може да бъде държана отговорна (т.е. ситуации, които са извън контрола на жалбоподателя, например когато той/тя не е бил уведомен/а за събирането на неговите/нейните лични данни), или форсмажорни обстоятелства (например природно бедствие, война).

([312]) Решение № 2006Du330 на Върховния съд, 26 март 2006 г.

([313]) Членове 2 и 4 от Закона за административното съдопроизводство.

([314]) Член 30, параграф 1 от Закона за административното съдопроизводство.

(182) В допълнение към оспорването на действие на държавни органи чрез административно съдопроизводство физическите лица могат да подадат конституционна жалба до Конституционния съд относно нарушение на техните основни права поради упражняването или неупражняването на държавно правомощие (с изключение на решенията на съдилищата) ([315]). Ако са налични други средства за правна защита, първо те трябва да бъдат изчерпани. Съгласно съдебната практика на Конституционния съд чужденците могат да подадат конституционна жалба, доколкото техните основни права са признати от корейската Конституция (вж. обясненията в раздел 1.1) ([316]). Конституционният съд може да обяви за недействително упражняването на държавното правомощие, което е довело до нарушението, или да потвърди, че конкретно бездействие е противоконституционно ([317]). В този случай съответният орган е длъжен да предприеме мерки за изпълнение на решението на Съда.

(183) Освен това физическите лица могат да получат обезщетение за вреди пред корейските съдилища. Преди всичко това включва възможността да се предяви обезщетение за нарушения на ЗЗЛД, извършени от органите за наказателно правоприлагане, в съответствие с член 39 (вж. също съображение 135). По-общо физическите лица могат да подадат искане за обезщетение за вреди, нанесени от държавни служители при изпълнението на задълженията им в нарушение на закона въз основа на Закона за държавните обезщетения (вж. също съображение 135) ([318]).

(184) Механизмите, описани в съображения 176—183, осигуряват на субектите на данни ефективни административни и съдебни средства за правна защита, като им дават възможност по-специално да защитят правата си, включително правото на достъп до личните им данни или правото на коригиране или заличаване на такива данни.

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

(185) Законодателството на Република Корея съдържа редица ограничения и гаранции по отношение на достъпа и използването на лични данни за целите на националната сигурност и осигурява механизми за надзор и правна защита в тази област, които са в съответствие с изискванията, посочени в съображения 141—143 от настоящото решение. Условията, при които може да се осъществи такъв достъп, и гаранциите, приложими за упражняването на тези правомощия, са подробно разгледани в следващите раздели.

3.3.1. *Правни основания, ограничения и гаранции*

(186) В Република Корея достъп до лични данни може да бъде получен за целите на националната сигурност въз основа на ЗЗПК, ЗТД и Закона за борба с тероризма за защита на гражданите и обществената сигурност („Закона за борба с тероризма“) ([319]). Основният орган ([320]) с правомощия в областта на националната сигурност е Националната разузнавателна служба (НРС) ([321]). Събирането и използването на лични данни от НРС трябва да съответства на

([315]) Член 68, параграф 1 от Закона за Конституционния съд. Конституционните жалби трябва да бъдат подавани в срок от 90 дни, след като физическото лице е узнало за нарушението, и в срок от една година след извършването му. Както е пояснено също така в приложение II, раздел 2.4.3, като се има предвид, че процедурата от Закона за административното съдопроизводство се прилага за съдебни спорове по Закона за Конституционния съд съгласно член 40 от Закона за Конституционния съд, жалбата все пак ще бъде допустима, ако са налице „основателни причини“, както се тълкуват в съответствие с описаната в бележка под линия 312 съдебна практика на Върховния съд. Ако първо трябва да бъдат изчерпани други средства за правна защита, конституционната жалба трябва да бъде подадена в срок от 30 дни след окончателното решение за такова средство за правна защита (член 69 от Закона за Конституционния съд).

([316]) Решение № 99HeonMa194 на Конституционния съд от 29 ноември 2001 г.

([317]) Член 75, параграф 3 от Закона за Конституционния съд.

([318]) Член 2, параграф 1 от Закона за държавните обезщетения.

([319]) Вж. приложение II, раздел 3.1.

([320]) По изключение полицията и прокуратурата също могат да събират лични данни за целите на националната сигурност (вж. бележка под линия 327 и приложение II, раздел 3.2.1.2). В допълнение корейската агенция за военно разузнаване (Командването за поддържане на сигурността в областта на отбраната, създадено към Министерството на отбраната) има правомощия в областта на националната сигурност. Както е пояснено в приложение II, раздел 3.1 обаче, тя отговаря само за военното разузнаване и извършва наблюдение на граждански лица само ако това е необходимо за изпълнение на военните ѝ функции. По-конкретно тя може да разследва само военнослужещи, граждански лица — служители в армията, лица, преминаващи военно обучение, лица от запаса или на наборна военна служба и военнопленници (член 1 от Закона за военните съдилища). Когато събира информация за комуникациите за целите на националната сигурност, Командването за поддържане на сигурността в областта на отбраната се подчинява на ограниченията и гаранциите, предвидени в ЗЗПК и в указа за неговото прилагане.

([321]) Мандатът на НРС е да събира, съставя и разпространява информация за чужди държави (т.е. обща информация за тенденции и развития във връзка с чужди държави или относно дейността на държавните участници); разузнавателни сведения, свързани с противодействие на шпионаж (включително военен и промишлен шпионаж), тероризъм и дейностите на международните престъпни синдикати; разузнавателни сведения за определени видове престъпления, насочени срещу обществената и националната сигурност (например вътрешни бунтове, чуждестранна агресия), и разузнавателни сведения, свързани с осигуряването на киберсигурността и предотвратяването или противодействието на кибератаки и заплахи (член 4, параграф 2 от Закона за НРС). Вж. също приложение II, раздел 3.1.

съответните правни изисквания (включително ЗЗЛД и ЗЗПК) ([322]) и на общите насоки, изготвени от президента и преразгледани от Националното събрание ([323]). Като общ принцип НРС трябва да поддържа политически неутралитет и да защитава свободата и правата на физическите лица ([324]). В допълнение към това служителите на НРС не трябва да злоупотребяват със служебното си положение, като принуждават институция, организация или физическо лице да направят нещо, което не са задължени да направят (по закон), нито да възпрепятстват упражняването на правата на което и да е лице ([325]).

3.3.1.1. Достъп до информация от комуникации

(187) Въз основа на ЗЗПК корейските публични органи ([326]) могат да събират данни за потвърждаване на комуникациите (т.е. за датата на електронните съобщения, началния и крайния им час, броя на изходящите и входящите повиквания, както и абонатния номер на другата страна, честотата на използване, регистрационни файлове за използването на телекомуникационни услуги и информация за местоположението, вж. съображение 155) и за съдържанието на комуникациите (чрез мерки за ограничаване на комуникациите, вж. съображение 155) за целите на националната сигурност (съгласно определения мандат на НРС, вж. бележка под линия 322 по-горе). Тези правомощия се отнасят до два вида информация: 1) комуникации, по които едната или двете страни са корейски граждани ([327]); и 2) комуникации на а) държави, враждебни на Република Корея, б) чуждестранни агенции, групи или граждани, заподозрени в участие в антикорейски дейности ([328]), или в) членове на групи в рамките на Корейския полуостров, които ефективно са извън суверенитета на Република Корея, и групи под тяхната „шапка“, базирани в чужди държави ([329]). Следователно комуникации на физически лица от ЕС, които се предават от Съюза на Република Корея въз основа на настоящото решение, могат да бъдат събирани съгласно ЗЗПК само за целите на националната сигурност (при спазване на условията, изложени в съображения 188—192), ако се извършват между физическо лице от ЕС и корейски гражданин или ако засягат комуникации само между некорейски граждани, които попадат в една от трите категории, посочени в 2а), б) и в).

(188) И в двата сценария събирането на данни за потвърждаване на комуникациите може да се извършва само с цел предотвратяване на заплахи за националната сигурност ([330]), докато мерките за ограничаване на комуникациите може да се прилагат, когато съществува сериозен риск за националната сигурност и събирането на сведения е необходимо за предотвратяването му ([331]). В допълнение към това достъпът до съдържанието на комуникациите може да се осъществява само като крайна мярка и трябва да бъдат положени усилия за свеждане до минимум на нарушенията в областта на поверителността на комуникациите ([332]), за да се гарантира, че те остават пропорционални на преследваната цел за националната сигурност. Събирането на съдържанието на комуникациите и на данни за потвърждаване на комуникациите може да продължи за максимален период от четири месеца и трябва да бъде прекратено веднага, ако преследваната цел е постигната по-рано ([333]). Ако съответните условия продължават да се спазват, периодът може да бъде удължен с предварителното разрешение на съд (за мерките, описани в съображение 189) или на президента (за мерките, описани в съображение 190) ([334]) с до четири месеца.

(189) Същите процедурни гаранции се прилагат за събирането на данни за потвърждаване на комуникациите и за съдържанието на комуникациите ([335]). По-специално, когато поне едно от физическите лица, участващи в комуникацията, е корейски гражданин, разузнавателната агенция трябва да представи писмено искане до Върховната

([322]) Вж. също членове 14, 22 и 23 от Закона за НРС.
([323]) Член 4, параграф 2 от Закона за НРС.
([324]) Член 3, параграф 1, член 6, параграф 2, членове 11 и 21 от Закона за НРС. Вж. също правилата за конфликт на интереси, и по-специално членове 10 и 12 от Закона за НРС.
([325]) Член 13 от Закона за НРС.
([326]) Това включва разузнавателните агенции (например НРС и Командването за поддържане на сигурността в областта на отбраната) и полицията/прокуратурата.
([327]) Член 7, параграф 1, точка 1 от ЗЗПК.
([328]) Както е пояснено от корейското правителство в бележка под линия 244 от приложение II, това се отнася за дейности, които застрашават съществуването и сигурността на нацията, демократичния ред или оцеляването и свободата на хората.
([329]) Член 7, параграф 1, точка 2 от ЗЗПК.
([330]) Член 13-4 от ЗЗПК.
([331]) Член 7, параграф 1 от ЗЗПК.
([332]) Член 3, параграф 2 от ЗЗПК. Освен това мерките за ограничаване на комуникациите трябва да бъдат преустановени незабавно, след като вече не са необходими, като по този начин се гарантира, че всяко нарушение на тайните на комуникациите на физическото лице е ограничено до минимум (член 2 от Указа за прилагане на ЗЗПК).
([333]) Член 7, параграф 2 от ЗЗПК.
([334]) Искането за получаване на одобрение за удължаване на мерките за наблюдение трябва да бъде подадено в писмена форма, като в него се посочват причините, поради които се иска удължаването, и се прилагат подкрепящи материали (член 7, параграф 2 от ЗЗПК и член 5 от Указа за прилагане на ЗЗПК).
([335]) Вж. също член 13-4, параграф 2 от ЗЗПК и член 37, параграф 4 от Указа за прилагане на ЗЗПК, в които се посочва, че процедурите, приложими към събирането на съдържанието на комуникациите, се прилагат mutatis mutandis към събирането на данни за потвърждаване на комуникациите. Вж. също приложение II, раздел 3.2.1.1.1.

прокуратура, която на свой ред трябва да подаде искане за заповед пред старши главен съдия от Върховния съд ([336]). В ЗЗПК е посочена информацията, която трябва да бъде представена в искането до прокурора, в искането за издаване на заповедта и в самата заповед, което включва по-конкретно обосновката за искането и основните основания за съмнението, подкрепящи материали, както и информация за целта, предмета (т.е. физическото(ите) лице(а), към което(които) е насочена), обхвата и продължителността на предложената мярка ([337]). Събиране без заповед може да се извърши само ако има конспиративен акт, който застрашава националната сигурност, и ако е налице извънредна ситуация, която прави невъзможно провеждането на гореспоменатите процедури ([338]). В този случай обаче искането за заповедта трябва да бъде подадено веднага след прилагането на мярката ([339]). Следователно в ЗЗПК ясно са определени обхватът и условията за тези видове събиране и са установени специални (процедурни) гаранции (включително предварително съдебно одобрение), с което се гарантира, че използването на тези мерки е ограничено до необходимото и пропорционалното. Освен това изискването за предоставяне на подробна информация както в искането, така и в самата заповед, изключва възможността за безразборен достъп.

(190) За комуникациите между чужденци, които попадат в една от специфичните категории, посочени в съображение 187, трябва да се подаде искане до директора на НРС, който след преглед за целесъобразност на предложените мерки трябва да поиска предварително писмено одобрение от президента на Република Корея ([340]). Искането, изготвено от разузнавателната агенция, трябва да включва същата подробна информация като информацията в искането за съдебна заповед (вж. съображение 189), по-конкретно относно обосновката на искането и основните основания за съмнението, подкрепящи материали, както и информация за целта, физическото(ите) лице(а), към което(които) е насочена, обхвата и продължителността на предложените мерки ([341]). При извънредни ситуации ([342]) трябва да се получи предварително одобрение от министъра, в чийто ресор се намира съответната разузнавателна агенция, въпреки че разузнавателната агенция трябва да подаде искане за одобрение до президента незабавно след предприемането на спешните мерки ([343]). Следователно, що се отнася до събирането на комуникации само между чужденци, в ЗЗПК прилагането на тези мерки е ограничено до необходимото и пропорционалното, чрез ясно регламентиране на ограничените категории физически лица, които могат да бъдат обект на тези мерки, и чрез определяне на подробни критерии, които трябва да бъдат изпълнени от разузнавателните агенции, за да обосноват искането си за събирането на информация. Освен това отново се изключва възможността за безразборен достъп. Макар че не се изисква предварително независимо одобряване на тези мерки, независимият надзор е гарантиран ex-post, по-конкретно от КЗЛД и НКПЧ (вж. например съображения 199—200).

(191) В ЗЗПК освен това се предвиждат няколко допълнителни гаранции, които дават възможност за последващ надзор и улесняват достъпа на физическите лица до ефективни средства за правна защита. Първо, по отношение на вида на събирането за целите на националната сигурност в ЗЗПК се предвиждат изисквания за поддържане на архив и за докладване. По-конкретно, когато искат съдействието на частни субекти, разузнавателните агенции трябва да им представят съдебната заповед/разрешението на президента или копие от заглавната страница на изявление за спешна цензура, което принуденият да съдейства субект трябва да съхранява в досието си ([344]). Когато частни субекти са задължени да оказват съдействие, трябва да се водят регистри, както от изискващия орган, така

([336]) Член 6, параграфи 5 и 8, член 7, параграф 1, точка 1 и параграф 3 от ЗЗПК, във връзка с член 7, параграфи 3—4 от Указа за прилагане на ЗЗПК.

([337]) Вж. член 7, параграф 3 и член 6, параграф 4 от ЗЗПК (за искането от разузнавателната агенция), член 4 от Указа за прилагане на ЗЗПК (за искането от страна на прокурора) и член 7, параграф 3 и член 6, параграф 6 от ЗЗПК (за заповедта).

([338]) Член 8 от ЗЗПК.

([339]) Член 8, параграфи 2 и 8 от ЗЗПК. Ако разрешението от съда не бъде получено в рамките на 36 часа от предприемането на мерките, събирането трябва да бъде преустановено незабавно. В случаите, когато наблюдението приключва в кратък срок, без да е необходимо разрешение от съда, ръководителят на компетентната Върховна прокуратура трябва да изпрати уведомление за извънредна мярка, изготвено от разузнавателната агенция, до ръководителя на компетентния съд, който въз основа на това може да разгледа законосъобразността на събирането (член 8, параграфи 5 и 7 от ЗЗПК). В уведомлението трябва да се посочат целта, предметът, обхватът, периодът, мястото на изпълнение и начинът на наблюдение, както и основанията за неподаване на искане преди предприемане на мярката (член 8, параграф 6 от ЗЗПК). Като цяло разузнавателните агенции могат да прилагат спешни мерки само в съответствие с „изявление за извънредна цензура/извънредно подслушване“, както и да водят регистър за тези мерки (член 8, параграф 4 от ЗЗПК).

([340]) Член 8, параграфи 1 и 2 от Указа за прилагане на ЗЗПК.

([341]) Член 8, параграф 3 от Указа за прилагане на ЗЗПК, във връзка с член 6, параграф 4 от ЗЗПК.

([342]) Това означава случаите, когато мярката е насочена към конспиративен акт, който застрашава националната сигурност, няма достатъчно време за получаване на одобрение от президента и неприемането на спешни мерки може да навреди на националната сигурност (член 8, параграф 8 от ЗЗПК).

([343]) Член 8, параграф 9 от ЗЗПК. Ако разрешението не бъде получено в рамките на 36 часа от подаването на искането, събирането трябва да бъде преустановено незабавно.

([344]) Член 9, параграф 2 от ЗЗПК и член 12 от Указа за прилагане на ЗЗПК. Вж. член 13 от Указа за прилагане на ЗЗПК относно възможността за изискване на съдействие от пощенските служби и доставчиците на телекомуникационни услуги. Частните субекти, от които е поискано да оповестят информация, могат да откажат да го направят, когато заповедта/разрешението или изявлението за спешна цензура се отнасят до грешен идентификатор (например телефонен номер, принадлежащ на лице, различно от идентифицираното). Освен това при всякакви обстоятелства им е забранено да разкриват пароли, използвани за осъществяване на комуникации (член 9, параграф 4 от ЗЗПК).

и от съответния частен субект, относно целта и предмета на мерките, както и за датата на изпълнението ([345]). В допълнение към това разузнавателните агенции трябва да докладват за събраната от тях информация и за резултатите от наблюдението на директора на НРС ([346]).

(192) Второ, физическите лица трябва да бъдат уведомени за събирането на техните данни (данни за потвърждаване на комуникациите или за съдържанието на комуникациите) за целите на националната сигурност, ако това засяга комуникации, в които поне едната страна е корейски гражданин ([347]). Уведомлението трябва да бъде дадено в писмена форма в срок от 30 дни от датата, на която е приключило събирането (включително когато данните са получени в съответствие със спешната процедура), и може да бъде отложено само ако и доколкото би изложило на риск националната сигурност или би имало вредни последствия за живота и физическата безопасност на хората ([348]). Независимо от уведомлението физическите лица могат да получат защита чрез различни механизми, обяснени по-подробно в раздел 3.3.4.

3.3.1.2. Събиране на информация за заподозрени в тероризъм лица

(193) В Закона за борба с тероризма се предвижда, че НРС може да събира данни за заподозрени в тероризъм лица ([349]) в съответствие с ограниченията и гаранциите, уредени в други закони ([350]). По-конкретно НРС може да получи данни от комуникации (въз основа на ЗЗПК) и други лични данни (чрез искане за доброволно разкриване) ([351]). Ограниченията и гаранциите, описани в раздел 3.3.1.1, се прилагат по отношение на събирането на информация за комуникациите (включително за съдържанието на комуникациите или за данните за потвърждаване на комуникациите), включително изискването за получаване на одобрена от съда заповед. Що се отнася до исканията за доброволно разкриване на други видове лични данни на заподозрени в тероризъм лица, НРС трябва да спази изискванията на Конституцията и ЗЗЛД относно необходимостта и пропорционалността (вж. съображение 164) ([352]). Администраторите, които получават такива искания, могат да ги изпълнят доброволно съгласно условията, предвидени в ЗЗЛД (например в съответствие с принципа за свеждане до минимум на данните и чрез ограничаване на въздействието върху неприкосновеността на личния живот на физическото лице) ([353]). В този случай те също трябва да спазят изискването за уведомяване на засегнатото физическо лице съгласно Уведомление № 2021-5 (вж. съображение 166).

([345]) По отношение на мерките за ограничаване на комуникациите такива регистри се съхраняват три години, вж. член 9, параграф 3 от ЗЗПК и член 17, параграф 2 от Указа за прилагане на ЗЗПК. По отношение на данни за потвърждаване на комуникации разузнавателните агенции трябва да съхраняват документация за факта, че е отправено искане за тези данни, както и самото писмено искане и за институцията, която се е позовала на него (член 13, параграф 5 и член 13-4, параграф 3 от ЗЗПК). Доставчиците на телекомуникационни услуги трябва да поддържат регистри в продължение на седем години и да докладват два пъти годишно на министъра на науката и ИКТ за честотата на тези разкрития (член 9, параграф 3 от ЗЗПК, във връзка с член 13, параграф 7 от ЗЗПК и член 37, параграф 4 и член 39 от Указа за прилагане на ЗЗПК).

([346]) Член 18, параграф 3 от Указа за прилагане на ЗЗПК.

([347]) Член 9-2, параграф 3 и член 13-4 от ЗЗПК. В уведомлението трябва да се посочат (1) фактът, че информацията е събрана, (2) изпълнителният орган и (3) периодът на изпълнение.

([348]) Член 9-2, параграф 4 от ЗЗПК. В този случай уведомлението трябва да бъде изпратено в срок от 30 дни, след като основанията за отсрочване престанат да съществуват, вж. член 13-4, параграф 2 и член 9-2, параграф 6 от ЗЗПК.

([349]) Това означава членове на терористична група (както е определена от Организацията на обединените нации, вж. член 2, параграф 2 от Закона за борба с тероризма.); лица, които популяризират или разпространяват идеи или тактики на терористична група, събират или предоставят средства за тероризъм или участват в други дейности по подготовка, заговор, пропагандиране или подстрекаване към тероризъм; или лица, за които има основателни причини да бъдат подозирани, че са извършвали такива дейности (член 2, параграф 3 от Закона за борба с тероризма). „Тероризъм“ се определя в член 2, параграф 1 от Закона за борба с тероризма като действие, извършено с цел да се попречи на упражняването на властта на държавата, на местна власт или на чуждо правителство (включително на международни организации), или имащо за цел да ги принуди да предприемат действие, без да имат правно задължение за това, или са заплаха за обществото. Например това действие може да включва убийство, отвличане или вземане на човек за заложник; отвличане/превземане, унищожаване или повреждане на кораб или въздухоплавателно средство; използване на биохимични, взривни или запалителни оръжия с намерение за причиняване на смърт, тежко увреждане или вреда; и злоупотреба с ядрени или радиоактивни материали.

([350]) Член 9, параграфи 1 и 3 от Закона за борба с тероризма.

([351]) Макар че в Закона за борба с тероризма се посочва също така възможността за събиране на информация относно влизането и напускането на Република Корея въз основа на Закона за имиграцията и Закона за митниците, тези закони понастоящем не предвиждат такива правомощия (вж. раздел 3.2.2.1 от приложение II). Във всеки случай по принцип те не биха се прилагали за данни, предадени въз основа настоящото решение, тъй като обикновено касаят информация, която се събира пряко от корейските органи (а не са свързани с достъпа до данни, които преди това са били предавани от Съюза на корейските администратори). В допълнение към това в Закона за борба с тероризма като правна основа за събирането на информация за финансови операции се посочва ЗДИОИФО. Както е пояснено в бележка под линия 200, видовете данни, които могат да бъдат получени въз основа на този закон, не попадат в приложното поле на настоящото решение. Накрая, в Закона за борба с тероризма се предвижда, че НРС може да събира информация за местонахождение чрез незадължителни искания, като в този случай доставчиците на информация за местонахождението биха могли доброволно да разкрият такава информация в съответствие с условията, посочени в ЗЗЛД (както е описано в съображение 193), и със Закона за информацията за местонахождението. Както е пояснено и в бележка под линия 17, информацията за местонахождението не се предава от Съюза към корейски администратори въз основа на настоящото решение, а по-скоро се генерира в самата Корея.

([352]) Вж. приложение II, раздел 3.2.2.2.

([353]) Вж. член 58, параграф 4 от ЗЗЛД, в който се предвижда личните данни да се обработват в минимално необходимата степен за постигане на предвидената цел, и член 3, параграф 6 от ЗЗЛД, в който се предвижда личните данни да се обработват по такъв начин, че да се сведе до минимум възможността за накърняване на неприкосновеността на личния живот на физическото лице. Вж. също член 59, точки 2 и 3 от ЗЗЛД, според който на администраторите се забранява да разкриват лични данни на трети страни без разрешение.

3.3.1.3. Искане за доброволно разкриване на данни на абонат

(194) На основание на ЗТД доставчиците на телекомуникационни услуги могат да разкриват доброволно данни за абонати (вж. съображение 163) по искане на разузнавателна агенция, която възнамерява да събира тези данни за предотвратяване на заплаха за националната сигурност ([354]). По отношение на такива искания от страна на НРС се прилагат същите ограничения (произтичащи от Конституцията, ЗЗЛД и ЗТД), каквито се прилагат в областта на наказателното правоприлагане, съгласно изложеното в съображение 164 ([355]). Доставчиците на телекомуникационни услуги не са задължени да ги изпълняват и могат да направят това само в съответствие с условията, посочени в ЗЗЛД (по-конкретно в съответствие с принципа за свеждане до минимум на данните и чрез ограничаване на въздействието върху неприкосновеността на личния живот на физическото лице, вж. съображение 193). Същите изисквания по отношение на поддържането на архив и уведомяването на засегнатото физическо лице се прилагат в областта на наказателното правоприлагане (вж. съображения 165 и 166).

3.3.2. *По-нататъшно използване на събраната информация*

(195) При обработването на лични данни, събирани от корейските органи за целите на националната сигурност, трябва да се спазват принципите за ограничение на целите (член 3, параграфи 1—2 от ЗЗЛД), законосъобразност и добросъвестност на обработването (член 3, параграф 1 от ЗЗЛД), пропорционалност/свеждане на данните до минимум (член 3, параграфи 1 и 6, член 58 от ЗЗЛД), точност (член 3, параграф 3 от ЗЗЛД), прозрачност (член 3, параграф 5 от ЗЗЛД), сигурност (член 58, параграф 4 от ЗЗЛД) и ограничено съхраняване на данни (член 58, параграф 4 от ЗЗЛД) ([356]). Възможно разкриване на лични данни на трети страни (включително трети държави) може да се извърши само в съответствие с тези принципи (по-конкретно за ограничение на целите и за свеждане на данните до минимум) след оценка на спазването на принципите на необходимостта и пропорционалността (член 37, параграф 2 от Конституцията) и при отчитане на въздействието върху правата на засегнатите физически лица (член 3, параграф 6 от ЗЗЛД).

(196) По отношение на съдържанието на комуникациите и на данните за потвърждаване на комуникациите в ЗЗПК се ограничава допълнително използването на такива данни в рамките на съдебни производства, когато дадена страна, свързана с комуникацията, се позовава на тях в иск за вреди; или разрешеното им използване в съответствие с други закони ([357]).

3.3.3. *Надзор*

(197) Надзорът върху дейностите на корейските национални органи по сигурността се упражнява от различни органи ([358]).

(198) Първо, в Закона за борба с тероризма се предвиждат специални механизми за упражняване на надзор във връзка с антитерористични дейности, включително събирането на данни за заподозрени в тероризъм лица. По-специално на равнището на изпълнителната власт надзорът върху антитерористичните дейности се упражнява от Комисията за борба с тероризма ([359]), на която директорът на НРС трябва да докладва за разследвания и проследяване на заподозрени в тероризъм лица с цел събиране на информация или материали, необходими за антитерористичните дейности ([360]). В допълнение служителят по защита на правата на човека (СЗПЧ) упражнява специален надзор за съответствие на антитерористичните дейности с основните права ([361]). Служителят по защита на правата на човека се назначава от председателя на Комисията за борба с тероризма измежду физически лица, които притежават конкретни квалификации, посочени в Указа за прилагане на Закона за борба с тероризма ([362]), за (подновяем) срок от две години и може да бъде отстранен от длъжност само на конкретни, ограничени основания и по основателна причина ([363]). При упражняване на своята надзорна функция СЗПЧ може да издава общи препоръки за

([354]) Член 83, параграф 3 от ЗТД.
([355]) Вж. също приложение II, раздел 3.2.3.
([356]) Вж. приложение II, раздел 1.2.
([357]) Член 5, параграфи 1—2 и 12 и член 13-5 от ЗЗПК.
([358]) Вж. приложение II, раздел 3.3.
([359]) Член 5, параграф 3 от Закона за борба с тероризма. Комисията се председателства от министър-председателя и се състои от няколко министри и ръководители на държавни агенции — от министерствата на външните работи, на правосъдието, на националната отбрана, на вътрешните работи и безопасността, директора на НРС и главния комисар на корейската национална служба „Полиция“ (член 3, параграф 1 от Указа за прилагане на Закона за борба с тероризма).
([360]) Член 9, параграф 4 от Закона за борба с тероризма.
([361]) Член 7 от Закона за борба с тероризма.
([362]) Тоест всеки, който има квалификация на адвокат с най-малко десет години професионален опит или експертни познания в областта на човешките права и е заемал или заема (поне) длъжността доцент най-малко десет години, или е работил като висш държавен служител в държавни агенции или в органи на местното самоуправление, или има поне десет години професионален опит в областта на човешките права, например в неправителствена организация (член 7, параграф 1 от Указа за прилагане на Закона за борба с тероризма).
([363]) Например, когато е обвинен по наказателно дело, свързано с неговите/нейните задължения, при разкриване на поверителна информация или поради продължителна психическа или физическа неспособност (член 7, параграф 3 от Указа за прилагане на Закона за борба с тероризма).

подобряване на защитата на правата на човека ([364]) и специални препоръки за корективни мерки, ако е установено нарушение на правата на човека ([365]). От публичните органи се изисква да информират СЗПЧ за предприетите действия в отговор на неговите препоръки ([366]).

(199) Второ, КЗЛД упражнява надзор върху спазването от националните органи по сигурността на правилата за защита на данните, което включва както приложимите разпоредби на ЗЗЛД (вж. съображение 149), така и ограниченията и гаранциите, които се прилагат във връзка със събирането на лични данни в съответствие с други закони (ЗЗПК, Закона за борба с тероризма и ЗТД, вж. също съображение 171) ([367]). При упражняването на тази надзорна роля КЗЛД може да използва всички свои правомощия за разследване и коригиране, описани подробно в раздел 2.4.2.

(200) Трето, дейностите на националните органи по сигурността са предмет на независим надзор от страна на НКПЧ в съответствие с процедурите, описани в съображение 172 ([368]).

(201) Четвърто, надзорната функция на СОИ обхваща също така органите за национална сигурност, въпреки че НРС в извънредни обстоятелства може да откаже да предостави определена информация или материали, т.е. когато те представляват държавни тайни и узнаването им от обществеността би имало сериозни последици за националната сигурност ([369]).

(202) Накрая, Националното събрание извършва парламентарен контрол върху дейностите на НРС (чрез специализиран Комитет по разузнаване) ([370]). В ЗЗПК се отрежда специална надзорна роля на Националното събрание по отношение на използването на мерките за ограничаване на комуникациите за целите на националната сигурност ([371]). По-специално Националното събрание може да извършва проверки на място на оборудване за подслушване и може да изисква от НРС и от телекомуникационните оператори, които са разкрили съдържанието на комуникациите, да докладват за това. Националното събрание може да извършва също така общи надзорни функции (в съответствие с процедурите, описани в съображение 174). Съгласно Закона за НРС от директора на НРС се изисква да отговори незабавно, когато Комитетът по разузнаването изиска доклад по определен въпрос ([372]), при спазване на специални правила по отношение на определена особено чувствителна информация. По-конкретно директорът на НРС може да откаже да отговоря или да свидетелства пред Комитета само в извънредни обстоятелства, т.е. ако искането е свързано с държавни тайни, касаещи военни и дипломатически въпроси или въпроси, свързани със Северна Корея, когато узнаването им от обществеността би имало сериозни последици за „националната съдба“ на държавата ([373]). В този случай Комитетът по разузнаването може да поиска обяснение от министър-председателя, и ако в срок от седем дни не бъде дадено обяснение, отговорът или свидетелстването не могат да бъдат отказани.

3.3.4. *Средства за правна защита*

(203) Също в областта на националната сигурност корейската система предоставя различни (съдебни) механизми за получаване на средства за правна защита, включително обезщетение за вреди. Тези механизми осигуряват на субектите на данни ефективни административни и съдебни средства за правна защита, като им дават възможност по-специално да защитят правата си, включително правото на достъп до личните им данни или правото на коригиране или заличаване на такива данни.

(204) Първо, в съответствие с член 3, параграф 5 и член 4, параграфи 1, 3 и 4 от ЗЗЛД физическите лица могат да упражняват правата си на достъп, коригиране, заличаване и спиране на използването спрямо националните органи по сигурността. В раздел 6 от Уведомление № 2021-5 (приложение I към настоящото решение) се пояснява

([364]) Член 8, параграф 1 от Указа за прилагане на Закона за борба с тероризма.
([365]) Член 9, параграф 1 от Указа за прилагане на Закона за борба с тероризма. Служителят по защита на правата на човека взема самостоятелни решения за даване на препоръки, но трябва да докладва за тях на председателя на Комисията за борба с тероризма.
([366]) Член 9, параграф 2 от Указа на прилагане на Закона за борба с тероризма. В съответствие с официалното изявление на корейското правителство всяко неизпълнение на препоръка на СЗПЧ се отнася до Комисията за борба с тероризма, включително до министър-председателя, макар че досега не е имало случаи на неизпълнение на препоръки на СЗПЧ (вж. раздел 3.3.1 от приложение II).
([367]) Приложение II, раздел 3.3.4
([368]) По-специално по отношение на НРС преди това НКПЧ е извършвала служебни разследвания и е разглеждала редица индивидуални жалби. Вж. например годишния доклад на НКПЧ за 2018 г., стр. 128 (достъпен на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) и годишния доклад на НКПЧ за 2019 г., стр. 70 (достъпен на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Член 13, параграф 1 от Закона за НРС.
([370]) Член 36 и член 37, параграф 1, точка 15 от Закона за Националното събрание.
([371]) Член 15 от ЗЗПК.
([372]) Член 15, параграф 2 от Закона за НРС.
([373]) Член 17, параграф 2 от Закона за НРС. Като „държавни тайни“ се определят (класифицирани) факти, стоки или информация, които не трябва да бъдат разгласявани на друга държава или организация, за да не се допусне изпадането в неизгодна позиция за националната сигурност, и до които се разрешава само ограничен достъп. Вж. член 13, параграф 4 от Закона за НРС.

допълнително как се прилагат тези права в контекста на обработването на лични данни за целите на националната сигурност. По-специално даден национален орган по сигурността може да ограничи или да откаже упражняването на правото само до степента и доколкото е необходимо и пропорционално, за да се защити важна цел от обществен интерес (например до степента и доколкото предоставянето на правото би застрашило текущо разследване или би представлявало заплаха за националната сигурност), или когато предоставянето на правото може да доведе до вредни последствия за живота или до телесни увреждания на трета страна. Поради това позоваването на такова ограничение изисква балансиране на правата и интересите на физическото лице спрямо съответния обществен интерес и във всеки случай не може да засегне същността на това право (член 37, параграф 2 от Конституцията). Когато искането е отхвърлено или ограничено, физическото лице трябва да бъде уведомено незабавно за причините.

(205) Второ, физическите лица имат право да получат правна защита съгласно ЗЗЛД, ако техните данни са обработени от национален орган по сигурността в нарушение на ЗЗЛД или в нарушение на ограниченията и гаранциите, уреждащи събирането на лични данни в други закони (например ЗЗПК, вж. съображение 171) ([374]). Това право може да бъде упражнено чрез жалба до КЗЛД (включително чрез Информационния център по въпросите на поверителността, управляван от Корейската агенция за интернет и сигурност) ([375]). Освен това, за да се улесни достъпът до средства за правна защита срещу корейските национални органи по сигурността, физическите лица от ЕС могат да подадат жалба до КЗЛД чрез своя национален орган по защита на данните ([376]). В този случай КЗЛД ще уведоми физическото лице чрез националния орган по защита на данните след приключването на разследването (включително, ако е приложимо, с информация за наложените корективни мерки). Въз основа на Закона за административното съдопроизводство физическите лица могат допълнително да обжалват/оспорват решенията или бездействието на КЗЛД (вж. съображение 132).

(206) Трето, във връзка с нарушаване на тяхното право на неприкосновеност на личния живот/защита на личните им данни в контекста на антитерористични дейности (т.е. съгласно Закона за борба с тероризма) ([377]) физическите лица могат да подадат жалба до СЗПЧ, който може да препоръча корективно действие. Тъй като няма изисквания за допустимост на жалбите пред СЗПЧ, жалбата ще бъде разгледана, дори ако засегнатото физическо лице не може да докаже дали в действителност е понесло вреда (например поради предполагаемото незаконно събиране на личните му/ѝ данни от национален орган по сигурността) ([378]). Съответният орган трябва да информира СЗПЧ за предприетите мерки в изпълнение на неговите препоръки.

(207) Четвърто, физическите лица могат да подадат жалба до НКПЧ относно събирането на техните данни от националните органи по сигурността и да получат правна защита в съответствие с процедурата, описана в съображение 178 ([379]).

(208) Накрая, физическите лица разполагат с различни съдебни средства за правна защита ([380]), които им позволяват да се позоват на ограниченията и гаранциите, описани в раздел 3.3.1, за да получат защита. По-специално физическите лица могат да оспорят законосъобразността на действия на националните органи по сигурността въз основа на Закона за административното съдопроизводство (в съответствие с процедурата, описана в съображение 181 или със Закона за Конституционния съд (вж съображение 182). В допълнение те могат да получат обезщетение за вреди въз основа на Закона за държавните обезщетения (както е описано по-подробно в съображение 183).

4. ЗАКЛЮЧЕНИЕ

(209) Комисията смята, че Република Корея — чрез ЗЗЛД, специалните правила, приложими за определени сектори (както е анализирано в раздел 2), и допълнителните гаранции, предвидени в Уведомление № 2021-5 (приложение I) — осигурява за личните данни, предавани от Европейския съюз, ниво на защита, което по същество е равностойно на нивото, гарантирано от Регламент (ЕС) 2016/679.

(210) Комисията смята освен това, че като цяло механизмите за упражняване на надзор и възможностите за правна защита, предвидени от корейското право, позволяват нарушенията на правилата за защита на личните данни, допуснати от администраторите в Корея, да бъдат установени и реално наказани и предоставят на субекта на данните средства за правна защита за получаване на достъп до отнасящите се за него лични данни и в крайна сметка за поправяне или заличаване на такива данни.

([374]) Член 58, параграф 4 и член 4, параграф 5 от ЗЗЛД. Вж. приложение II, раздел 3.4.2.
([375]) Член 62 и член 63, параграф 2 от ЗЗЛД.
([376]) Уведомление № 2021-5 (раздел 6, приложение I).
([377]) Член 8, параграф 1, точка 2 от Указа за прилагане на закона за борба с тероризма.
([378]) Вж. приложение II, раздел 3.4.1.
([379]) Например НКПЧ редовно получава жалби срещу Националната разузнавателна служба, вж. данните в годишния доклад на НКПЧ за 2019 г. относно броя на получените жалби в периода 2015—2019 г., стр. 70 (достъпен на адрес: https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Вж. приложение II, раздел 3.4.4.

(211) Накрая, въз основа на наличната информация за правния ред на Корея, в това число изявленията, гаранциите и ангажиментите, поети от корейското правителство и посочени в приложение II, Комисията смята, че всяко вмешателство във връзка с основните права на физическите лица, чиито лични данни са предадени от Европейския съюз към Република Корея, от страна на корейските публични органи поради цели от обществен интерес, и по-специално цели в областта на наказателното правоприлагане и националната сигурност, ще бъде ограничено до строго необходимото за постигане на въпросната законосъобразна цел, както и че съществува реална правна защита срещу такова вмешателство.

(212) Поради това, предвид изложените в настоящото решение констатации, следва да се вземе решение, че Република Корея осигурява адекватно ниво на защита по смисъла на член 45 от Регламент (ЕС 2016/679, тълкуван в светлината на Хартата на основните права на Европейския съюз, по отношение на лични данни, предадени от Европейския съюз на Република Корея на администратори на лични данни в Република Корея съгласно ЗЗЛД, с изключение на религиозните организации, доколкото те обработват лични данни за своите мисионерски дейности; политическите партии, доколкото те обработват лични данни в контекста на определянето на кандидати, и на администратори, които подлежат на надзор от Комисията по финансов надзор, по отношение на обработването на лична кредитна информация съгласно Закона за кредитната информация, доколкото те обработват такава информация.

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

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

(214) Следователно решение на Комисията относно адекватното ниво на защита, прието съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679, е обвързващо за всички органи на държавите членки, адресати на решението, включително за независимите им надзорни органи. По-специално предаването на данни от администратор или обработващ лични данни в Европейския съюз на администратори в Република Корея може да се извършва, без да е необходимо допълнително разрешение.

(215) Следва да се припомни, че съгласно член 58, параграф 5 от Регламент (ЕС) 2016/679 и както е обяснено от Съда на ЕС в решението по *делото* Schrems ([381]), когато национален орган за защита на данните поставя под въпрос, включително въз основа на получена жалба, съгласуваността на дадено решение на Комисията относно адекватното ниво на защита с основните права на неприкосновеност на личния живот и на защита на данните на физическото лице, националното законодателство трябва да предвижда правни способи, позволяващи на съответния орган да представи възраженията си пред национална юрисдикция, която може да бъде длъжна да отправи преюдициално запитване до Съда на ЕС ([382]).

6. МОНИТОРИНГ И ПРЕРАЗГЛЕЖДАНЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(216) Според практиката на Съда на ЕС ([383]) и както е предвидено в член 45, параграф 4 от Регламент (ЕС) 2016/679, след като приеме решение относно адекватното ниво на защита, Комисията следва непрекъснато да наблюдава релевантните промени в третата държава, за да прецени дали третата държава продължава да гарантира ниво на защита, което по същество е равностойно на нивото в Европейския съюз. Такава проверка е наложителна във всички случаи, когато Комисията получи информация, която поражда основателни съмнения в това отношение.

(217) Следователно Комисията следва да осъществява постоянно наблюдение на ситуацията, що се отнася до нормативната уредба и реалната практика при обработването на лични данни, както са оценени в настоящото Решение, включително спазването от корейските органи на изявленията, гаранциите и ангажиментите, посочени в приложение II. За да се улесни този процес, от корейските органи се очаква да информират Комисията своевременно за съществени промени, имащи отношение към настоящото решение и свързани с обработването на лични данни от стопанските субекти и публичните органи, както и за ограниченията и гаранциите, приложими към достъпа до лични данни от страна на публичните органи.

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

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

([383]) Решение по дело *Schrems*, т. 76.

(218) На следващо място, за да се даде възможност на Комисията да изпълнява ефективно функцията си по извършване на наблюдение, държавите членки следва да я информират за всички релевантни действия, предприети от националните органи по защита на данните, по-специално във връзка със запитвания или жалби на субекти на данни от ЕС във връзка с предаване на лични данни от Съюза към администратори на лични данни в Република Корея. Комисията следва да бъде информирана и за всякакви признаци, че действията на корейските публични органи, отговарящи за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или за националната сигурност, включително надзорните органи, не гарантират изискваното ниво на защита.

(219) В приложение на член 45, параграф 3 от Регламент (ЕС) 2016/679 ([384]) и с оглед на факта, че нивото на защита, осигурявано от корейския правен ред, може да се промени, след приемането на настоящото решение Комисията следва периодично да проверява дали констатациите във връзка с адекватното ниво на защита, гарантирано от Република Корея, са все още фактически и правно обосновани.

(220) За тази цел първи преглед на настоящото решение следва да бъде извършен в срок от две години след влизането му в сила. След този първи преглед и в зависимост от резултата от него Комисията ще реши, в тесни консултации с комитета, създаден съгласно член 93, параграф 1 от Регламент (ЕС) 2016/679, дали следва да се запази същият тригодишен цикъл. При всички случаи последващите прегледи следва да се извършват най-малко веднъж на четири години ([385]). Прегледът следва да обхваща всички аспекти от функционирането на настоящото решение, и по-специално прилагането на допълнителните гаранции, съдържащи се в приложение I към настоящото решение, като се обръща специално внимание на защитата в случай на последващо предаване; развития в съответната съдебна практика; правилата за обработването на псевдонимизирана информация за статистически цели, за научноизследователски цели или за целите на архивирането в обществен интерес, както и прилагането на изключенията съгласно член 28, параграф 7 от ЗЗЛД; ефективността на упражняването на индивидуалните права, включително пред неотдавна реформираната КЗЛД, и прилагането на изключенията от тези права; прилагането на частичните освобождавания съгласно ЗЗЛД; както и ограниченията и гаранциите във връзка с достъпа на държавните органи (както е посочено в приложение II към настоящото решение), включително сътрудничеството на КЗЛД с органите за защита на личните данни от ЕС относно жалби от физически лица. Той следва да обхваща също ефективността на надзора и правоприлагането, що се отнася до ЗЗЛД и в областта на наказателното правоприлагане и националната сигурност (по-специално от КЗЛД и НКПЧ).

(221) При извършването на прегледа Комисията следва да се срещне с КЗЛД, придружена, ако е целесъобразно, от други корейски органи, отговарящи за достъпа на държавните органи, включително съответните надзорни органи. В тази среща следва да могат да участват представители на членовете на Европейския комитет по защита на данните. В рамките на съвместния преглед Комисията следва да поиска от КЗЛД да предостави изчерпателна информация по всички аспекти, които са от значение за установяването на адекватно ниво на защита, включително относно ограниченията и гаранциите във връзка с достъпа на държавните органи ([386]). Комисията следва също така да потърси обяснения във връзка с всяка получена от нея информация, която е от значение за настоящото решение, включително публични доклади на корейските органи или на други заинтересовани страни в Корея, Европейския комитет по защита на данните, отделни органи за защита на данните, групи на гражданското общество, съобщения в медиите или всякакви други налични източници на информация.

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

7. СПИРАНЕ НА ДЕЙСТВИЕТО, ОТМЯНА ИЛИ ИЗМЕНЕНИЕ НА НАСТОЯЩОТО РЕШЕНИЕ

(223) Когато наличната информация, по-специално информацията, получена в резултат на наблюдението на настоящото решение или предоставена от корейските органи или от органите на държавите членки, показва, че нивото на защита, предлагано от Република Корея, може вече да не е адекватно, Комисията следва да информира своевременно компетентните корейски органи за това и да поиска предприемането на подходящи мерки в определен разумен срок.

(224) Ако при изтичането на посочения срок компетентните корейски органи не предприемат тези мерки или не докажат по друг задоволителен начин, че настоящото решение продължава да се основава на адекватно ниво на защита, Комисията ще започне процедурата, посочена в член 93, параграф 2 от Регламент (ЕС) 2016/679, с оглед частично или пълно спиране или отмяна на настоящото решение.

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

([384]) Съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 „[в] акта за изпълнение се предвижда механизъм за периодичен преглед най-малко веднъж на четири години, при който се отчитат всички имащи отношение промени в третата държава или международната организация.“

([385]) В член 45, параграф 3 от Регламент (ЕС) 2016/679 се предвижда, че периодичният преглед трябва да се извършва „най-малко веднъж на четири години“. Вж. също Референтния документ на Европейския комитет по защита на данните за адекватното ниво на защита, WP 254 rev. 01.

([386]) Вж. приложение II към настоящото решение.

(226) По-специално Комисията следва да започне процедурата за спиране на прилагането или за отмяна на решението, ако има индикации, че допълнителните гаранции, съдържащи се в приложение I, не се спазват от стопанските субекти, получаващи лични данни въз основа на настоящото решение, и/или не се прилагат ефективно, или че корейските органи не спазват изявленията, гаранциите и ангажиментите, посочени в приложение II към настоящото решение.

(227) Комисията следва също така да разгледа необходимостта от започване на процедурата, водеща до изменение, спиране на прилагането или отмяна на настоящото решение, ако при съвместния преглед или по друг повод компетентните корейски органи не предоставят информацията или поясненията, необходими за оценката на нивото на защита на личните данни, предавани от Европейския съюз към Република Корея, или за спазването на настоящото решение. Във връзка с това Комисията следва да взема предвид степента, в която съответната информация може да бъде набавена от други източници.

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

8. **ЗАКЛЮЧИТЕЛНИ СЪОБРАЖЕНИЯ**

(229) Европейският комитет по защита на данните публикува становището си ([387]), като то бе взето предвид при изготвянето на настоящото решение.

(230) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, създаден по силата на член 93, параграф 1 от Регламент (ЕС) 2016/679,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

1. За целите на член 45 от Регламент (ЕС) 2016/679 Република Корея осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз към образувания в Република Корея, които са подчинени на Закона за защита на личните данни, допълнен с допълнителните гаранции, посочени в приложение I, заедно с официалните изявления, гаранции и ангажименти, съдържащи се в приложение II.

2. Настоящото решение не обхваща личните данни, предавани на получатели от една от следните категории, доколкото всички или част от целите на обработването на личните данни съответстват на една от изброените цели, а именно:

а) религиозните организации, доколкото те обработват лични данни за целите на своите мисионерски дейности;

б) политическите партии, доколкото те обработват лични данни в контекста на определянето на кандидати;

в) образуванията, които подлежат на надзор от Комисията по финансов надзор, по отношение на обработването на лична кредитна информация съгласно Закона за кредитната информация, доколкото те обработват такава информация.

Член 2

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

Член 3

1. Комисията наблюдава непрекъснато прилагането на правната рамка, на която се основава настоящото решение, включително условията, при които се извършват последващите предавания, условията, при които се упражняват индивидуалните права и при които публичните органи на Корея имат достъп до данните, предадени въз основа на настоящото решение, с цел да прецени дали Република Корея продължава да осигурява адекватно ниво на защита по смисъла на член 1.

([387]) Становище 32/2021 относно проекта на решение за изпълнение на Европейската комисия съгласно Регламент (ЕС) 2016/679 относно адекватната защита на личните данни в Република Корея, достъпно на следния адрес: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Държавите членки и Комисията се информират взаимно за случаите, в които Комисията за защита на личните данни или всеки друг компетентен корейски орган не е гарантирал спазването на правната рамка, на която се основава настоящото решение.

3. Държавите членки и Комисията се информират взаимно за всички признаци, че намесата на корейските публични органи в правото на физическите лица на защита на личните им данни надвишава строго необходимото или че няма реална правна защита срещу подобна намеса.

4. В срок от три години от датата на нотифицирането на настоящото решение до държавите членки, а след това поне веднъж на всеки четири години Комисията ще извършва оценка на констатацията, съдържаща се в член 1, параграф 1, въз основа на цялата налична информация, включително получената като част от съвместния преглед, извършен заедно със съответните корейски органи.

5. Ако Комисията открие признаци, че вече не се осигурява адекватно ниво на защита, тя информира компетентните корейски органи. Ако е необходимо, тя може да реши да спре прилагането, да измени или да отмени настоящото решение, или да ограничи приложното му поле в съответствие с член 45, параграф 5 от Регламент (ЕС) 2016/679, по-специално, когато са налице признаци, че:

а) администраторите в Корея, които са получили лични данни от Европейския съюз въз основа на настоящото решение, не прилагат допълнителните гаранции, съдържащи се в приложение I към настоящото решение, или че в това отношение няма достатъчен надзор и правоприлагане;

б) корейските публични органи не спазват изявленията, гаранциите и ангажиментите, съдържащи се в приложение II към настоящото решение, включително във връзка с условията и ограниченията за събиране и достъп до личните данни, предадени въз основа на настоящото решение, от страна на корейските публични органи за целите на наказателното правоприлагане или националната сигурност.

Комисията може да приеме такива мерки и когато липсата на съдействие от страна на корейското правителство не позволява на Комисията да определи дали Република Корея продължава да осигурява адекватно ниво на защита.

Член 4

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 17 декември 2021 година.

За Комисията
Didier REYNDERS
Член на Комисията

ПРИЛОЖЕНИЕ I

ДОПЪЛНИТЕЛНИ ПРАВИЛА ЗА ТЪЛКУВАНЕТО И ПРИЛАГАНЕТО НА ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ (ЗЗЛД) ВЪВ ВРЪЗКА С ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ НА КОРЕЯ

Съдържание

I. Резюме 54

II. Определения на понятията 55

III. Допълнителни правила 55

1. Ограничаване на използването и предоставянето на лични данни извън предвидените цели (членове 3, 15 и 18 от закона) 55

2. Ограничаване на последващото предаване на лични данни (член 17, параграфи 3 и 4, член 18 от закона) 57

3. Уведомление за данните, когато личните данни не са получени от субекта на данни (член 20 от закона) 58

4. Приложно поле на специалното изключение за обработване на псевдонимизирани данни (членове 28-2, 28-3, 28-4, 28-5, 28-6 и 28-7, член 3 и член 58-2 от закона) 60

5. Корективни мерки и др. (член 64, параграфи 1, 2 и 4 от закона) 61

6. Прилагане на ЗЗЛД по отношение на обработването на лични данни за целите на националната сигурност, включително разследване на нарушения и принудително изпълнение в съответствие със ЗЗЛД (член 7-8, член 7-9, член 58, член 3, член 4 и член 62 от ЗЗЛД) 62

I. **Резюме**

Корея и Европейският съюз (наричан по-нататък „ЕС“) проведоха обсъждания относно адекватното ниво на защита, в резултат на което Европейската комисия определи, че Корея гарантира адекватно ниво на защита на личните данни в съответствие с член 45 от Общия регламент относно защитата на данните.

В този контекст Комисията за защита на личните данни прие настоящото уведомление въз основа на член 5 (Задължения на държавата и пр.) и член 14 (Международно сътрудничество) ([1]) от Закона за защита на личните данни, за да изясни тълкуването, прилагането и изпълнението на определени разпоредби на закона, включително по отношение на обработването на лични данни, предадени на Корея въз основа на решението на ЕС относно адекватното ниво на защита.

Тъй като настоящото уведомление има статут на административно правило, което компетентният административен орган установява и обявява, за да разясни стандартите за тълкуване, прилагане и изпълнение на Закона за защита на личните данни в правната система на Корея, то има правнообвързваща сила за администратора на лични данни, в смисъл че всяко нарушение на настоящото уведомление може да се смята за нарушение на съответните разпоредби на ЗЗЛД. Освен това, ако личните права и интереси са нарушени поради нарушение на настоящото уведомление, засегнатите физически лица имат право да получат правна защита от Комисията за защита на личните данни или от съда.

Съответно, ако администраторът на лични данни, който обработва личните данни, предадени на Корея съгласно решението на ЕС относно адекватното ниво на защита, не предприеме мерки, съответстващи на настоящото уведомление, ще се счита, че „има сериозни основания да се смята, че е извършено нарушение по отношение на личните данни и че бездействието може да причини трудно поправими вреди“, съгласно член 64, параграфи 1 и 2 от закона. В тези случаи Комисията за защита на личните данни или свързаните с нея централни административни органи могат да наредят на

([1]) В член 14 от Закона за защита на личните данни се определят правомощията на корейското правителство да установява политики за подобряване на нивото на защита на личните данни в международната среда и да предотвратява нарушаването на правата на субектите на данни поради трансграничното предаване на лични данни.

съответния администратор на лични данни да предприеме корективни мерки и пр. съгласно правомощията, предоставени с тази разпоредба, и в зависимост от конкретните нарушения на закона могат да бъдат наложени и съответни наказания (санкции, административни глоби и др.).

II. **Определение на понятията**

Определенията на понятията, използвани в настоящата разпоредба, са както следва:

i) Закон: Закон за защита на личните данни (Закон № 16930, изменен на 4 февруари 2020 г. и влязъл в сила на 5 август 2020 г.)

ii) Указ на президента: Указ за прилагане на Закона за защита на личните данни (Указ на президента № 30509, 3 март 2020 г., изменя други закони)

iii) Субект на данни: физическо лице, което може да бъде идентифицирано чрез данните, обработвани съгласно настоящото, за да стане субект на тези данни

iv) Администратор на лични данни: държавна институция, юридическо лице, организация, физическо лице и др., които обработват пряко или непряко лични данни като част от своите дейности;

v) ЕС: ЕС (към края на февруари 2020 г. — 27 държави членки ([2]), включително Белгия, Германия, Франция, Италия, Люксембург, Нидерландия, Дания, Ирландия, Гърция, Португалия, Испания, Австрия, Финландия, Швеция, Кипър, Чешка република, Естония, Унгария, Латвия, Литва, Малта, Полша, Словакия, Словения, Румъния, България и Хърватия), както и държави, асоциирани към ЕС чрез Споразумението за ЕИП (Исландия, Лихтенщайн, Норвегия).

vi) Общ регламент относно защитата на данните: общото право на ЕС в областта на защитата на личните данни — Общ регламент относно защитата на данните (Регламент (ЕС) 2016/679).

vii) Решение относно адекватното ниво на защита: Съгласно член 45, параграф 3 от Общия регламент относно защитата на данните Европейската комисия реши, че трета държава, територията на трета държава, една или повече области или международна организация осигуряват адекватно ниво на защита на личните данни.

III. **Допълнителни правила**

1. **Ограничаване на използването и предоставянето на лични данни извън предвидените цели (членове 3, 15 и 18 от закона)**

<Закон за защита на личните данни

(Закон № 16930, частично изменен на 4 февруари 2020 г.)>

Член 3 (Принципи за защита на личните данни) 1) Администраторът на лични данни посочва изрично целите, за които се обработват личните данни; и събира по законосъобразен и добросъвестен начин лични данни в минимално необходимата степен за тези цели.

2) Администраторът на лични данни обработва личните данни по подходящ начин, необходим за целите, за които се обработват личните данни, като не ги използва извън тези цели.

Член 15 (Събиране и използване на лични данни) 1) Администраторът на лични данни може да събира лични данни при всяко от следните обстоятелства и да ги използва в рамките на целта на събирането:

1. когато е получено съгласие от субекта на данни;

2. когато в законите съществуват специални разпоредби или е неизбежно да се спазват правните задължения;

3. когато това е неизбежно за изпълнение на задълженията на държавна институция в рамките на нейната компетентност, както е предвидено в законите и др.;

4. когато това е неизбежно необходимо за сключването и изпълнението на договор със субекта на данни;

([2]) До края на преходния период това включва и Обединеното кралство, както е предвидено в членове 126, 127 и 132 от Споразумението за оттеглянето на Обединеното кралство Великобритания и Северна Ирландия от Европейския съюз и Европейската общност за атомна енергия (2019/C 384 I/01).

5. когато се смята за очевидно необходимо за защита от непосредствена опасност на живота, телесните или имуществените интереси на субекта на данни или на трета страна, когато субектът на данни или неговият законен представител не е в състояние да изрази намерение или не може да бъде получено предварително съгласие поради неизвестни адреси и др.;

6. когато е необходимо да се постигне оправданият интерес на администратор на лични данни, който интерес е очевидно по-висш от правата на субекта на данни. В такива случаи обработването се разрешава само доколкото то е съществено свързано с оправдания интерес на администратора на личните данни и не излиза извън рамките на разумното.

Член 18 (Ограничаване на използването и предоставянето на лични данни извън предвидените цели)
1) Администраторът на лични данни не може да използва лични данни извън обхвата, предвиден в член 15, параграф 1 и член 39-3, параграфи 1 и 2, нито да ги предоставя на трети страни извън обхвата, предвиден в член 17, параграфи 1 и 3.

2) Независимо от параграф 1, когато се прилага някоя от точките по-долу, администраторът на лични данни може да използва лични данни или да ги предоставя на трета страна за други цели, освен ако има вероятност това да наруши несправедливо интересите на субекта на данни или на третата страна: като се има предвид, че доставчиците на информационни и комуникационни услуги [както е посочено в член 2, параграф 1, точка 3 от Закона за насърчаване на използването на информационни и комуникационни мрежи и защита на информацията и пр.; оттук нататък се прилага същото], които обработват лични данни на потребители [както е посочено в член 2, параграф 1, точка 4 от Закона за насърчаване на използването на информационни и комуникационни мрежи и защита на информацията и пр.; оттук нататък се прилага същото], са подчинени единствено на точки 1 и 2, а точки 5—9 се прилагат само за държавните институции:

1. когато е получено допълнително съгласие от субекта на данни;

2. когато съществуват други специални законови разпоредби;

3. когато се смята за очевидно необходимо за защита от непосредствена опасност на живота, телесните или имуществените интереси на субекта на данни или на трета страна, когато субектът на данни или неговият законен представител не е в състояние да изрази намерение или не може да бъде получено предварително съгласие поради неизвестни адреси;

4. заличено;<със Закон № 16930, 4 февруари 2020 г. >

5. когато не е възможно задълженията в рамките на неговата компетентност да се изпълнят както е предвидено в законите, освен ако администраторът на лични данни използва личните данни за цел, различна от предвидената, или ги предоставя на трета страна, и това е предмет на обсъждане и решаване от Комисията;

6. когато е необходимо да се предоставят лични данни на чуждестранно правителство или на международна организация за изпълнение на договор или друга международна конвенция;

7. когато е необходимо за разследване на престъпление, повдигане на обвинение и наказателно преследване;

8. когато е необходимо съдът да пристъпи към изпълнение на свързани с делото задължения;

9. когато е необходимо за изпълнението на наказание, пробация и задържане под стража.

пропуснати параграфи 3) ~ 4)

5) Когато администратор на лични данни предоставя лични данни на трета страна за цел, различна от предвидената, във всеки от случаите по параграф 2, администраторът на лични данни изисква от получателя на личните данни да ограничи целта и начина на използване, както и други необходими обстоятелства, или да подготви необходимите защитни мерки, за да гарантира безопасността на личните данни. В тези случаи лицето, което получава такова искане, предприема необходимите мерки, за да гарантира безопасността на личните данни.

i) В член 3, параграфи 1 и 2 от закона се предвижда принципът, че администраторът на лични данни трябва да събира само минимално необходимите лични данни за целите на законосъобразното обработване на личните данни и не следва да ги използва за цели, различни от предвиденото ([3]).

ii) В съответствие с този принцип в член 15, параграф 1 от закона се предвижда, че когато администратор на лични данни събира лични данни, те могат да се използват в рамките на целите на събирането, а в член 18, параграф 1 се предвижда, че личните данни не следва да се използват извън целите на събирането или да се предоставят на трета страна.

([3]) Тъй като с тези разпоредби се установяват общи принципи, които се прилагат по отношение на всяко обработване на лични данни, включително когато това обработване е изрично уредено в други закони, разясненията в настоящия раздел се прилагат и когато личните данни се обработват въз основа на други закони (вж. напр. член 15, параграф 1 от Закона за кредитната информация, който изрично се позовава на тези разпоредби).

iii) Също така, дори ако личните данни могат да бъдат използвани за цели, различни от предвидените, или да бъдат предоставени на трета страна в изключителните случаи ([4]), описани в точките на член 18, параграф 2 от закона, трябва да се поиска ограничаване на целта или начина на използване, така че личните данни да могат да бъдат обработвани безопасно в съответствие с параграф 5, или следва да се предприемат необходимите мерки за гарантиране на безопасността на личните данни.

iv) Горепосочените разпоредби се прилагат еднакво по отношение на обработването на всички лични данни, получени от трета държава в рамките на правната юрисдикция на Корея, независимо от националността на субекта на данни.

v) Например, ако администратор на лични данни в ЕС предаде лични данни на корейски администратор на лични данни в съответствие с решението на Европейската комисия относно адекватното ниво на защита, целта на администратора на лични данни в ЕС за предаването на личните данни се смята за целта на корейския администратор на лични данни за събирането на лични данни и в тези случаи корейският администратор на лични данни може да използва личните данни или да ги предоставя на трета страна само в рамките на целта на събирането, освен в изключителните случаи, описани в точките на член 18, параграф 2 от закона.

2. **Ограничаване на последващото предаване на лични данни (член 17, параграфи 3 и 4, член 18 от закона)**

<Закон за защита на личните данни

(Закон № 16930, частично изменен на 4 февруари 2020 г.)>

Член 17 (Предоставяне на лични данни) 1) пропуснат параграф

2) Когато получи съгласието съгласно параграф 1, точка 1, администраторът на лични данни предоставя на субекта на данни информацията по-долу. Същото се прилага, когато се променят някои от следните данни:

1. получателят на лични данни;
2. целта, за която получателят на лични данни използва тези данни;
3. подробности за личните данни, които трябва да се предоставят;
4. периодът, през който получателят съхранява и използва личните данни;
5. фактът, че субектът на данни има право да откаже да даде съгласие, както и неблагоприятните последици, ако има такива, произтичащи от отказа за даване на съгласие.

3) Администраторът на лични данни предоставя на субекта на данни информацията, предвидена в параграф 2, и получава съгласието на субекта на данни, за да предостави лични данни на трета страна в чужбина; и не сключва договор за трансгранично предаване на лични данни в нарушение на този закон.

4) Администраторът на лични данни може да предоставя лични данни без съгласието на субект на данни в рамките на обхвата, който е свързан в разумна степен с целите, за които първоначално са били събрани личните данни, в съответствие с предписаното в Указа на президента, като отчита дали има неблагоприятни последствия за субекта на данни, дали са предприети необходимите мерки, за да се гарантира безопасността, като например криптиране и др.

※ Моля, вж. стр. 3, 4 и 5 за член 18

<Указ за прилагане на Закона за защита на личните данни

([Дата на влизане в сила 5 февруари 2021 г.] [Указ на президента № 30892, 4 август 2020 г., изменя други закони])>

Член 14-2 (Стандарти за допълнително използване/предоставяне на лични данни и др.)

1) Ако администраторът на лични данни използва или предоставя лични данни (наричано по-нататък „допълнително използване или предоставяне на лични данни“) без съгласието на субекта на данни в съответствие с член 15, параграф 3 от закона или член 17, параграф 4 от закона, администраторът на лични данни разглежда следните обстоятелства:

1. дали това е разумно свързано с първоначалната цел, за която са събрани личните данни;
2. дали допълнителното използване или предоставяне на лични данни е предвидимо с оглед на обстоятелствата, при които са събрани личните данни, и с оглед на практиките за обработване;
3. дали допълнителното използване или предоставяне на лични данни не нарушава несправедливо интересите на субекта на данни; както и
4. дали са взети необходимите мерки за гарантиране на сигурността, като например псевдонимизация или криптиране.

([4]) Доставчиците на информационни и комуникационни услуги са подчинени единствено на разпоредбите на член 18, параграф 2, точки 1 и 2. Точки 5—9 се прилагат само за държавните институции.

2) Администраторът на лични данни оповестява предварително критериите за оценка на обстоятелствата, посочени в точките на параграф 1, в политиката за поверителност по член 30, параграф 1 от закона, а служителят по въпросите на поверителността по член 31, параграф 1 от закона проверява дали администраторът на лични данни използва или предоставя допълнително лични данни съгласно съответните стандарти.

i) Ако администраторът на лични данни предоставя лични данни на трета страна в чужбина, той трябва предварително да информира субектите на данни относно всички обстоятелства, описани в член 17, параграф 2 от закона, и да получи тяхното съгласие, с изключение на случаите, попадащи в обхвата на параграфи 1 или 2. Не следва да се сключват договори за трансгранично предоставяне на лични данни в нарушение на този закон.

1) Ако личните данни се предоставят в рамките на обхвата, който е свързан в разумна степен с първоначалната цел на събирането съгласно член 17, параграф 4 от Закона. Случаите, за които може да се прилага тази разпоредба, обаче са ограничени до случаите, в които са изпълнени стандартите за допълнително използване и предоставяне на лични данни, предвидени в член 14-2 от Указа за прилагане. Освен това администраторът на лични данни трябва да прецени дали предоставянето на лични данни може да доведе до неблагоприятни последици за субектите на данни и дали са предприети необходимите мерки за гарантиране на безопасността на данните, като например криптиране.

2) Ако личните данни могат да бъдат предоставени на трета страна в изключителните случаи, посочени в член 18, параграф 2 от Закона (вж. страници 3~5). Дори и в такива случаи обаче, ако има вероятност предоставянето на тези лични данни да наруши несправедливо интересите на субекта на данни или на трета страна, личните данни не могат да бъдат предоставени на трета страна. Освен това доставчикът на лични данни трябва да поиска от получателя на лични данни да ограничи целта или начина на използване на личните данни или да предприеме необходимите мерки за осигуряване на тяхната безопасност, така че личните данни да могат да се обработват по сигурен начин.

ii) Ако личните данни се предоставят на трета страна в чужбина, те могат да не получат нивото на защита, гарантирано от Закона за защита на личните данни на Корея, поради разликите в системите за защита на личните данни в различните държави. Съответно такива случаи ще се считат за „случаи, които могат да доведат до неблагоприятни последствия за субекта на данни“, както е упоменато в член 17, параграф 4 от закона, или „случаи, при които интересът на субекта на данни или на трета страна е нарушен несправедливо“, както е упоменато в член 18, параграф 2 от закона и член 14-2 от Указа за прилагане на същия закон ([5]). Следователно, за да изпълнят изискванията на тези разпоредби, администраторът на лични данни и третата страна трябва изрично да осигурят ниво на защита, равностойно на закона, включително гарантиране на упражняването на правата на субекта на данни в правнообвързващи документи, като например договори, дори след като личните данни са предадена в чужбина.

3. **Уведомление за данните, когато личните данни не са получени от субекта на данни (член 20 от закона)**

<Закон за защита на личните данни

(Закон № 16930, частично изменен на 4 февруари 2020 г.)>

Член 20 (Уведомление относно източниците и пр. на лични данни, събрани от трети страни) 1) Когато администраторът на лични данни обработва лични данни, събрани от трети страни, по искане на субекта на данни той незабавно го уведомява за:

1. източника на събраните лични данни;

2. целта на обработването на лични данни;

3. факта, че субектът на данни има право да поиска спиране на обработването на личните данни, както е предвидено в член 37.

2) Независимо от параграф 1, когато администратор на лични данни, който отговаря на критериите, определени с Указ на президента, като взема предвид вида и обема на обработваните лични данни, броя на служителите, размера на продажбите и др., събира лични данни от трети страни и обработва същите съгласно член 17, параграф 1, точка 1, администраторът на лични данни уведомява субекта на данни по въпросите, посочени в параграф 1: като това не се прилага, когато информацията, събрана от администратора на лични данни, не съдържа никакви лични данни, например данни за контакт, посредством които субектът на данни може да бъде уведомен.

([5]) В съответствие с член 18, параграф 2, точка 2 от ЗЗЛД това се прилага и когато личните данни се разкриват на трети страни в чужбина въз основа на разпоредби в други закони (като например Закона за кредитната информация).

3) Необходимите въпроси във връзка с времето, начина и процедурата за уведомяване на субекта на данни съгласно основното изречение на параграф 2 се определят с Указ на президента.

4) Параграф 1 и основната клауза на параграф 2 не се прилагат за нито едно от следните обстоятелства: като това важи само в случаите, когато това е очевидно по-висше от правата на субектите на данни съгласно настоящия закон:

1. когато лични данни, предмет на искане за уведомление, са включени в досиетата с лични данни, посочени в която и да е от точките на член 32, параграф 2;

2. когато това уведомление може да причини вреда върху живота или тялото на което и да е друго лице, или несправедливо да нанесе вреда върху имуществото и да накърни други интереси на което и да е друго лице.

i) Ако администраторът на лични данни получи лични данни, предадени от ЕС въз основа на решението му относно адекватното ниво на защита ([6]), той трябва, без неоправдано забавяне и във всички случаи не по-късно от един месец от предаването, да предостави на субекта на данни следната информация, посочена в точки 1)—5).

1) Имената и данните за контакт на лицата, които предават и получават личните данни.

2) Елементите или категориите на предадените лични данни.

3) Целта на събирането и използването на личните данни (както е определена от износителя на данни съгласно точка 1 от настоящото уведомление).

4) Срока на съхранение на личните данни.

5) Информация относно правата на субекта на данни във връзка с обработването на личните данни, начина и процедурата за упражняване на правата, както и всякакви неблагоприятни последствия, ако упражняването на тези права води до такива.

ii) Също така, ако администраторът на лични данни предоставя личните данни по точка i) на трета страна в Република Корея или в чужбина, той трябва да уведоми субекта на данни относно информацията по подточки 1)—5) преди предоставянето на личните данни.

1) Имената и данните за контакт на лицата, които предоставят и получават личните данни.

2) Елементите или категориите на предоставените лични данни.

3) Държавата, на която се предоставят личните данни, предвидената дата и начинът на тяхното предоставяне (ограничено до случаите, в които личните данни се предоставят на трета страна в чужбина).

4) Целта на доставчика на лични данни и правното основание за предоставянето на личните данни.

5) Информация относно правата на субекта на данни във връзка с обработването на личните данни, начина и процедурата за упражняване на правата, както и всякакви неблагоприятни последици, ако упражняването на тези права води до такива.

iii) Администраторът на лични данни може да не прилага точки i) или ii) в случаите, посочени в следните подточки 1)—4):

1) ако личните данни, за които трябва да бъде изпратено уведомление, са включени в което и да е от досиетата с лични данни, посочени в член 32, параграф 2 от закона, доколкото интересите, защитени от тази разпоредба, са очевидно по-висши от правата на субекта на данни, и само доколкото уведомлението би застрашило преследването на въпросните интереси, например застрашаване на текущи наказателни разследвания или заплаха за националната сигурност;

2) ако и докато има вероятност уведомлението да доведе до вредни последствия за живота или тялото на друго лице или несправедливо да наруши имуществените интереси на друго лице, когато тези права или интереси са очевидно по-висши от правата на субекта на данни;

3) ако субектът на данни вече разполага с информацията, за която администраторът на лични данни трябва да изпрати уведомление съгласно точки i) или ii);

4) ако администраторът на лични данни не разполага с никаква информация за контакт със субекта на данни или е необходимо да положи прекомерни усилия, за да се свърже със субекта на данни, включително в контекста на обработването при условията, посочени в раздел 3 от ЗЗЛД. При определянето на това дали е възможно да се осъществи контакт със субекта на данни, или дали това е свързано с прекомерни усилия, следва да се вземе предвид възможността за сътрудничество с износителя на данни в ЕС.

([6]) Задълженията по точки i), ii) и iii) се прилагат по същия начин и когато администраторът, който получава лични данни от ЕС въз основа на решението относно адекватното ниво на защита, обработва тези данни въз основа на други закони, като например Закона за кредитната информация.

4. **Приложно поле на специалното изключение за обработване на псевдонимизирани данни (членове 28-2, 28-3, 28-4, 28-5, 28-6 и 28-7, член 3 и член 58-2 от закона)**

<Закон за защита на личните данни

(Закон № 16930, частично изменен на 4 февруари 2020 г.)>

Глава III Обработване на лични данни

РАЗДЕЛ 3 Специални случаи, свързани с псевдонимизирани данни

Член 28-2 (Обработване на псевдонимизирани данни) 1) Администраторът на лични данни може да обработва псевдонимизирани данни без съгласието на субектите на данни за статистически цели, за научноизследователски цели, за архивиране в обществен интерес и др.

2) Администраторът на лични данни не включва данни, които могат да се използват за идентифициране на определено физическо лице, когато предоставя псевдонимизирани данни на трета страна в съответствие с параграф 1.

Член 28-3 (Ограничаване на комбинирането на псевдонимизирани данни) 1) Независимо от разпоредбите на член 28-2, комбинирането на псевдонимизирани данни, обработвани от различни администратори на лични данни за статистически цели, за научни изследвания, за съхраняване на документи от обществен интерес и др., се извършва от специализирана институция, определена от Комисията за защита или от ръководителя на съответния централен административен орган.

2) Администратор на лични данни, който възнамерява да предостави комбинираните данни извън организацията, която ги е комбинирала, получава одобрение от ръководителя на специализираната институция след обработване на данните в псевдонимизирани данни или във формата, посочена в член 58-2.

3) Необходимите въпроси, включително процедурите и методите за комбиниране съгласно параграф 1, стандартите и процедурите за определяне или отмяна на определянето на специализирана институция за управление и надзор, както и стандартите и процедурите за износ и одобрение съгласно параграф 2, се определят с Указ на президента.

Член 28-4 (Задължение за предприемане на мерки за безопасност на псевдонимизираните данни) 1) При обработването на псевдонимизирани данни администраторът на лични данни предприема технически, организационни и физически мерки, като отделно съхраняване и управление на допълнителната информация, необходима за възстановяване на първоначалното състояние, каквито са необходими за осигуряване на безопасността, както е предвидено в Указ на президента, така че личните данни да не могат да бъдат изгубени, откраднати, разкрити, подправени, променени или повредени.

2) Администратор на лични данни, който възнамерява да обработва псевдонимизираните данни, изготвя и поддържа регистър, свързан с предвидените в Указа на президента въпроси, включително целта на обработването на псевдонимизираните данни и третата страна получател, когато се предоставят псевдонимизирани данни, с цел управление на обработването на псевдонимизирани данни.

Член 28-5 (Забранени действия при обработването на псевдонимизирани данни) 1) Никой не може да обработва псевдонимизирани данни за целите на идентифицирането на определено физическо лице.

2) Когато по време на обработването на псевдонимизираните данни се генерират данни, идентифициращи определено физическо лице, администраторът на лични данни прекратява обработването на данните и незабавно извлича и унищожава данните.

Член 28-6 (Налагане на допълнителни административни такси за обработването на псевдонимизирани данни) 1) Комисията може да наложи глоба в размер до три стотни от общите продажби на администратор на данни, който е обработил данни за целите на идентифицирането на конкретно физически лице в нарушение на член 28-5, параграф 1: в случай че няма продажби или са налице трудности при изчисляването на приходите от продажби, на администратора на лични данни може да бъде наложена глоба в размер на не повече от 400 милиона вона или три стотни от размера на капитала, в зависимост от това коя от двете суми е по-голяма.

2) Член 34-2, параграфи 3—5 се прилагат mutatis mutandis по отношение на въпросите, необходими за налагането и събирането на допълнителни административни такси.

Член 28-7 (Приложно поле) @Членове 20, 21, 27, член 34, параграф 1, членове 35—37, членове 39-3, 39-4 и 39-6—39-8 не се прилагат по отношение на псевдонимизираните данни.

Глава I Общи разпоредби

Член 3 (Принципи за защита на личните данни) 1) Администраторът на лични данни посочва изрично целите, за които се обработват личните данни; и събира по законосъобразен и добросъвестен начин лични данни в минимално необходимата степен за тези цели.

2) Администраторът на лични данни обработва личните данни по подходящ начин, необходим за целите, за които се обработват личните данни, като не ги използва извън тези цели.

3) Администраторът на лични данни гарантира, че личните данни са точни, пълни и актуални, доколкото това е необходимо във връзка с целите, за които се обработват личните данни.

4) Администраторът на лични данни управлява личните данни по безопасен начин в зависимост от методите на обработване, вида и пр. на личните данни, като отчита възможността за нарушаване на правата на субекта на данни и сериозността на съответните рискове.

5) Администраторът на лични данни оповестява публично своята политика за поверителност и други въпроси, свързани с обработването на лични данни, и гарантира правата на субекта на данни, като например правото на достъп до неговите лични данни.

6) Администраторът на лични данни обработва личните данни по начин, който свежда до минимум възможността за нарушаване на неприкосновеността на личния живот на субекта на данни.

7) Ако е възможно целите на събирането на лични данни да се постигнат и чрез обработване на анонимизирани или псевдонимизирани лични данни, администраторът на лични данни се стреми да обработва лични данни чрез анонимизиране, когато анонимизирането е възможно, или чрез псевдонимизиране, ако е невъзможно да се постигнат целите на събирането на лични данни чрез анонимизиране.

8) Администраторът на лични данни се стреми да получи доверието на субектите на данни, като спазва и изпълнява задълженията и отговорностите, предвидени в настоящия закон и други свързани закони.

Глава IX Допълнителни разпоредби

Член 58-2 (Изключения от прилагането) Настоящият закон не се прилага за данни, които вече не идентифицират определено физическо лице, когато се съчетават с други данни, като се отчитат в разумна степен времето, разходите, технологията и пр. <Посоченият член е новосъздаден със Закон № 16930 от 4 февруари 2020 г. >

i) В глава III, раздел 3 „Специални случаи, свързани с псевдонимизирани данни“ (член 28-2—член 28-7) се позволява обработването на псевдонимизирани данни без съгласието на субекта на данни за целите на изготвянето на статистически данни, за научни изследвания, за съхраняване на публични регистри и пр. (член 28-2), но в тези случаи са задължителни подходящи защитни мерки и забрани, необходими за защита на правата на субектите на данни (членове 28-4 и 28-5), на нарушителите могат да бъдат налагани санкции (член 28-6), а някои защитни мерки, които иначе са налични съгласно ЗЗЛД (член 28-7), не се прилагат.

ii) Тези разпоредби не се прилагат в случаите, когато псевдонимизираните данни се обработват за цели, различни от изготвянето на статистически данни, научни изследвания, съхраняване на публични регистри и пр. Например, ако личните данни на физическо лице от ЕС, които са били предадени на Корея в съответствие с решението на Европейската комисия относно адекватното ниво на защита, са псевдонимизирани за цели, различни от изготвянето на статистически данни, научни изследвания, съхраняване на публични регистри и др., специалните разпоредби в глава III, раздел 3 не се прилагат ([7]).

iii) Когато администратор на лични данни обработва псевдонимизирани данни за целите на изготвянето на статистически данни, за научни изследвания, за съхраняване на публични регистри и пр., и ако псевдонимизираните данни не са били унищожени, след като е постигната конкретната цел на обработването в съответствие с член 37 от Конституцията и член 3 (Принципи за защита на личните данни) от закона, той анонимизира данните с цел да се гарантира, че с тях вече не се идентифицира конкретно физическо лице, самостоятелно или в комбинация с други данни, като отчита в разумна степен времето, разходите, технологията и пр., в съответствие с член 58-2 от ЗЗЛД.

5. **Корективни мерки и др. (член 64, параграфи 1, 2 и 4 от закона)**

<Закон за защита на личните данни

(Закон № 16930, частично изменен на 4 февруари 2020 г.)>

Член 64 (Корективни мерки) 1) Когато Комисията за защита прецени, че са налице сериозни основания да се смята, че е извършено нарушение по отношение на личните данни и че бездействието може да причини трудно поправими вреди, тя може да разпореди на нарушителя на този закон (с изключение на централните административни органи, органите на местното самоуправление, Националното събрание, съда, Конституционния съд и Националната избирателна комисия) да предприеме някоя от следните мерки:

1. да преустанови нарушението по отношение на личните данни;

2. да преустанови временно обработването на лични данни;

([7]) По подобен начин изключението, предвидено в член 40-3 от Закона за кредитната информация, се прилага само за обработването на псевдонимизирани кредитни данни за целите на изготвянето на статистически данни, за научни изследвания и за съхраняване на публични регистри.

3. други мерки, необходими за защита на личните данни и за предотвратяване на нарушения по отношение на личните данни.

2) Когато ръководителят на заинтересован централен административен орган прецени, че са налице сериозни основания да се смята, че е извършено нарушение по отношение на личните данни и че бездействието може да причини трудно поправими вреди, той може да нареди на администратора на лични данни да предприеме някоя от мерките, предвидени в параграф 1, в съответствие със законите и съгласно компетентността на съответния централен административен орган.

4) Когато настоящият закон се нарушава от централен административен орган, орган на местното самоуправление, Националното събрание, съда, Конституционния съд или Националната избирателна комисия, Комисията за защита може да препоръча на ръководителя на съответния орган да предприеме някоя от мерките, предвидени в параграф 1. В такива случаи, след като получи препоръката, органът се съобразява с нея, освен ако няма извънредни обстоятелства.

i) Първо, съгласно съдебната практика ([8]) ([9]) „трудно поправима вреда“ се тълкува като случай, който би могъл да доведе до вредни последствия за личните права или за неприкосновеността на личния живот на физическо лице.

ii) Съответно „сериозни основания да се смята, че е извършено нарушение по отношение на личните данни и че бездействието може да причини трудно поправими вреди“, предвидено в член 64, параграфи 1 и 2, се отнася до случаите, когато се счита, че нарушението на закона има вероятност да наруши правата и свободите на физическите лица по отношение на личните данни. Това се прилага винаги когато се нарушава някой от принципите или някое от правата и задълженията, включени в закона за защита на личните данни ([10]).

iii) Съгласно член 64, параграф 4 от Закона за защита на личните данни има мярка по отношение на „нарушение на настоящия закон“, т.е. действие срещу нарушение на ЗЗЛД.

Централен административен орган и др., като публичен орган, обвързан с върховенството на закона, не може да нарушава нито един закон и е длъжен да предприеме корективна мярка, включително незабавно да преустанови действието, и да предостави обезщетение за вреди в изключителния случай, когато въпреки това е извършено незаконно действие.

Съответно, дори и без намесата на Комисията за защита съгласно член 64, параграф 4 от ЗЗЛД, централен административен орган и пр. трябва да предприеме корективна мярка срещу нарушенията, ако узнае за нарушение на закона.

По-специално, когато Комисията за защита е препоръчала корективна мярка, обикновено за централния административен орган и пр. е обективно ясно, че той е нарушил закона. Затова, за да обоснове защо счита, че дадена препоръка на Комисията за защита не следва да бъде изпълнена, централният административен орган и пр. трябва да представи ясни основания, с които може да се докаже, че не е нарушил закона. Препоръката трябва да бъде изпълнена, освен ако Комисията за защита не установи, че случаят наистина не е такъв.

С оглед на това „извънредните обстоятелства“ по член 64, параграф 4 от Закона за защита на личните данни трябва да бъдат строго ограничени до извънредни обстоятелства, при които има ясни основания централните административни органи и пр. да докажат, че „този закон всъщност не е бил нарушен“, като например „случаи, при които са налице извънредни (фактически или правни) обстоятелства“, за които Комисията за защита не е знаела при първоначалното изготвяне на своята препоръка, и Комисията за защита установява, че наистина не е имало нарушение.

6. **Прилагане на ЗЗЛД по отношение на обработването на лични данни за целите на националната сигурност, включително разследване на нарушения и принудително изпълнение в съответствие със ЗЗЛД (член 7-8, член 7-9, член 58, член 3, член 4 и член 62 от ЗЗЛД)**

<Закон за защита на личните данни

(Закон № 16930, частично изменен на 4 февруари 2020 г.)>

Член 7-8 (Работа на Комисията за защита) 1) Комисията за защита извършва следната дейност: […]

3. разглеждане на въпроси, свързани с разследването на нарушения на правата на субектите на данни и последващите разпореждания;

4. разглеждане на жалби или коригиращи процедури, свързани с обработването на лични данни, и посредничество при спорове относно личните данни;

[…]

([8]) (Решение 97Da10215,10222 на Върховния съд от 26 януари 1999 г.) Ако престъпните деяния на обвиняемия бъдат оповестени чрез медиите, това може да причини непоправими психически и физически вреди не само на жертвата, т.е. на ищеца, но и на хората около него, включително на семействата.

([9]) (Решение 2006Na92006 на Висшия съд на Сеул от 16 януари 2008 г.) Ако бъде публикувана клеветническа статия, има вероятност същата да причини сериозни непоправими вреди на засегнатото лице.

([10]) Същите принципи, изложени в точка ii), се прилагат по отношение на член 45-4 от Закона за кредитната информация.

Член 7-9 (Въпроси, подлежащи на обсъждане и решаване от Комисията за защита) 1) Комисията за защита обсъжда и взима решения по следните въпроси: […]

5. въпроси, свързани с тълкуването и действието на законодателството, свързано със защитата на личните данни;

[…]

Член 58 (Частично изключение по отношение на прилагането) 1) Глави III—VII не се прилагат за следните лични данни:

1. лични данни, събирани съгласно Закона за статистиката, с оглед на обработването им от държавни институции;
2. лични данни, събирани или поискани да бъдат предоставени за анализ на информация, свързана с националната сигурност;
3. лични данни, обработвани временно, когато това е спешно необходимо за обществената безопасност и сигурност, за общественото здраве и др.;
4. лични данни, събирани или използвани за собствени цели, съответно за отразяване от пресата, за мисионерска дейност от религиозни организации и за номиниране на кандидати от политически партии.

[пропуснати параграфи 2) и 3)]

4) В случай на обработване на лични данни съгласно параграф 1 администраторът на лични данни обработва личните данни в минимално необходимата степен за постигане на предвидената цел за минимален срок от време, като също така предприема необходимите мерки, например технически, управленски и физически защитни мерки, разглеждане на индивидуални жалби и други необходими мерки за безопасното управление и подходящото обработване на такива лични данни.

Член 3 (Принципи за защита на личните данни) 1) Администраторът на лични данни посочва изрично целите, за които се обработват личните данни; и събира по законосъобразен и добросъвестен начин лични данни в минимално необходимата степен за тези цели.

2) Администраторът на лични данни обработва личните данни по подходящ начин, необходим за целите, за които се обработват личните данни, като не ги използва извън тези цели.

3) Администраторът на лични данни гарантира, че личните данни са точни, пълни и актуални, доколкото това е необходимо във връзка с целите, за които се обработват личните данни.

4) Администраторът на лични данни управлява личните данни по безопасен начин в зависимост от методите на обработване, вида и пр. на личните данни, като отчита възможността за нарушаване на правата на субекта на данни и сериозността на съответните рискове.

5) Администраторът на лични данни оповестява публично своята политика за поверителност и други въпроси, свързани с обработването на лични данни, и гарантира правата на субекта на данни, като например правото на достъп до неговите лични данни.

6) Администраторът на лични данни обработва личните данни по начин, който свежда до минимум възможността за нарушаване на неприкосновеността на личния живот на субекта на данни.

7) Ако е възможно целите на събирането на лични данни да се постигнат и чрез обработване на анонимизирани или псевдонимизирани лични данни, администраторът на лични данни се стреми да обработва лични данни чрез анонимизиране, когато анонимизирането е възможно, или чрез псевдонимизиране, ако е невъзможно да се постигнат целите на събирането на лични данни чрез анонимизиране.

8) Администраторът на лични данни се стреми да получи доверието на субектите на данни, като спазва и изпълнява задълженията и отговорностите, предвидени в настоящия закон и други свързани закони.

Член 4 (Права на субектите на данни) Субектът на данни има следните права във връзка с обработването на собствените му лични данни:

1. правото да бъде информиран за обработването на такива лични данни;
2. правото да решава дали да даде съгласие, или не, както и за обхвата на съгласието по отношение на обработването на такива лични данни;
3. правото да поиска потвърждение дали се обработват лични данни, или не и да поиска достъп (включително предоставяне на копия; оттук нататък се прилага същото) по отношение на такива лични данни;
4. правото да спре обработването и да поиска коригиране, заличаване и унищожаване на такива лични данни;
5. правото на подходяща защита по отношение на вреди, произтичащи от обработването на такива лични данни, чрез бърза и справедлива процедура.

Член 62 (Докладване на нарушения) 1) Всяко лице, което е претърпяло нарушение на права или интереси, свързани с неговите лични данни, в хода на обработването на личните данни от администратор на лични данни, може да подаде сигнал за такова нарушение до Комисията за защита.

2) Комисията за защита може да определи специализирана институция, която ефикасно да получава и обработва сигнали за претенции съгласно параграф 1, както е предвидено в Указа на президента. В такива случаи тази специализирана институция създава и управлява център за обаждания при нарушения, свързани с личните данни (наричан по-нататък „Център за обаждания по въпросите на поверителността“).

3) Центърът за обаждания по въпросите на поверителността има следните задължения:

1. да получава сигнали за претенции и да предоставя консултации във връзка с обработването на лични данни;

2. да разследва и установява инциденти и да изслушва становищата на съответните страни;

3. задължения, свързани с точки 1 и 2.

4) Комисията за защита може, ако е необходимо, да изпрати свой държавен служител в определената съгласно параграф 2 специализирана институция по силата на член 32-4 от Закона за държавните служители, за целите на ефикасното разследване и установяване на инцидентите по параграф 3, точка 2.

i) Събирането на лични данни за целите на националната сигурност се регулира от специални закони, с които се оправомощават компетентните органи (напр. Националната разузнавателна служба) да прихващат комуникации или да изискват разкриването им при определени условия и защитни мерки (по-нататък: „законодателство в областта на националната сигурност“). Това законодателство в областта на националната сигурност включва например Закона за защита на неприкосновеността на комуникациите, Закона за борба с тероризма за защита на гражданите и обществената сигурност или Закона за телекомуникационните дейности. Освен това събирането и по-нататъшното обработване на лични данни трябва да отговарят на изискванията на ЗЗЛД. В това отношение в член 58, параграф 1, точка 2 от ЗЗЛД се предвижда, че глави III—VII не се прилагат по отношение на личните данни, които се събират или се изисква да бъдат предоставени за анализа на информация, свързана с националната сигурност. Следователно това частично изключение се прилага по отношение на обработването на лични данни за целите на националната сигурност.

Същевременно за обработването на тези лични данни се прилагат глава I (Общи разпоредби), глава II (Установяване на политики за защита на личните данни и др.), глава VIII (Колективен иск при нарушения в областта на данните), глава IX (Допълнителни разпоредби) и глава X (Наказателни разпоредби) от ЗЗЛД. Това включва общите принципи за защита на данните, посочени в член 3 (Принципи за защита на личните данни), и личните права, гарантирани по член 4 от ЗЗЛД (Права на субектите на данни).

Освен това в член 58, параграф 4 от ЗЗЛД се предвижда, че такива данни трябва да се обработват в минимално необходимата степен за постигане на предвидената цел и за минимален период от време. В него се изисква също така администраторът на лични данни да въведе необходимите мерки за осигуряване на безопасно управление и подходящо обработване на данните, като например технически, управленски и физически защитни мерки, както и мерки за разглеждане по подходящ начин на индивидуални жалби.

Накрая, прилагат се разпоредбите, уреждащи задачите и правомощията на Комисията за защита на личните данни (КЗЛД) (включително член 60-65 от ЗЗЛД относно разглеждането на жалби и приемането на препоръки и корективни мерки), както и разпоредбите относно административните и наказателните санкции (член 70 и сл. от ЗЗЛД). Съгласно член 7-8, параграф 1, точки 3 и 4 и член 7-9, параграф 1, точка 5 от ЗЗЛД тези правомощия за разследване и корективни правомощия, включително когато се упражняват в контекста на разглеждането на жалби, обхващат и възможни нарушения на правилата, съдържащи се в специални закони, определящи ограниченията и защитните мерки по отношение на събирането на лични данни, като например законодателството в областта на националната сигурност. Предвид изискванията по член 3, параграф 1 от ЗЗЛД за законосъобразно и справедливо събиране на лични данни, всяко такова нарушение представлява нарушение на „настоящия закон“ по смисъла на членове 63 и 64, което позволява на КЗЛД да провежда разследване и да предприема корективни мерки ([11]). Упражняването на тези правомощия от КЗЛД допълва, но не замества правомощията на Националната комисия по правата на човека съгласно Закона за Комисията по правата на човека.

Прилагането на основните принципи, права и задължения съгласно ЗЗЛД по отношение на обработването на лични данни за целите на националната сигурност отразява залегналите в Конституцията гаранции за защита на правото на физическото лице да контролира собствените си лични данни. Както е признато от Конституционния съд, това включва правото на физическото лице ([12]) „лично да решава кога, на кого или от кого и в каква степен да бъдат разкривани или използвани неговите данни. Това е основно право ([13]), […], съществуващо, за да се защити личната свобода на вземане на решения от риска, причинен от разширяването на държавните функции и информационните и комуникационните технологии“. Всяко ограничаване на това право, например когато е необходимо за защита на националната сигурност, изисква балансиране между правата и интересите на физическото лице и съответния обществен интерес, и не може да засяга същността на това право (член 37, параграф 2 от Конституцията).

([11]) Що се отнася до корективните мерки съгласно член 64, вж. също раздел 5 по-горе.
([12]) Решение 99HunMa513, 2004HunMa190 на Конституционния съд от 26 май 2005 г.
([13]) Решение 2003HunMa282 на Конституционния съд от 21 юли 2005 г.

Ето защо, когато обработва лични данни за целите на националната сигурност, администраторът (напр. Националната разузнавателна служба (НРС) трябва, inter alia:

1) да посочва изрично целите, за които се обработват личните данни, и да събира лични данни по законосъобразен и справедлив начин в минимално необходимата степен за тези цели (член 3, параграф 1 от ЗЗЛД); по-конкретно да събира и обработва по-нататък лични данни само за целите на изпълнение на задълженията по съответните закони, като например Закона за националната разузнавателна служба;

2) да обработва лични данни в минимално необходимата степен и за минимално необходимия период за постигане на предвидената цел (член 58, параграф 4 от ЗЗЛД); след постигане на целта на обработването администраторът необратимо унищожава личните данни, освен ако по-нататъшното съхранение не е изрично предвидено в закона, като в този случай съответните лични данни се съхраняват и управляват отделно от други лични данни, не се използват за цели, различни от посочените в закона, и се унищожават след края на периода на съхранение;

3) да обработва лични данни по подходящ начин, необходим за целите, за които се обработват личните данни, като не ги използва извън тези цели (член 3, параграф 2 от ЗЗЛД);

4) да гарантира, че личните данни са точни, пълни и актуални, доколкото това е необходимо във връзка с целите, за които се обработват личните данни (член 3, параграф 3 от ЗЗЛД);

5) да управлява личните данни по безопасен начин в зависимост от методите на обработване, вида и пр. на личните данни, като отчита възможността за нарушаване на правата на субекта на данни и сериозността на съответните рискове (член 3, параграф 4 от ЗЗЛД);

6) да оповестява публично своята политика за поверителност и други въпроси, свързани с обработването на лични данни (член 3, параграф 5 от ЗЗЛД);

7) да обработва личните данни по начин, който свежда до минимум възможността за нарушаване на неприкосновеността на личния живот на субекта на данни (член 3, параграф 6 от ЗЗЛД).

ii) В съответствие с член 58, параграф 4 от ЗЗЛД администраторът (напр. компетентните органи в областта на националната сигурност, като Националната разузнавателна служба (НРС) предприема необходимите мерки, например въвеждане на технически, управленски и физически защитни мерки, за да гарантира спазването на тези принципи и подходящото обработване на личните данни. Това може да включва например конкретни мерки за гарантиране на безопасността на личните данни, като например ограничения на достъпа до лични данни, контрол на достъпа, регистри, осигуряване на специално обучение на служителите за работа с лични данни и т.н.

Освен това в съответствие с член 3, параграф 5 и член 4 от ЗЗЛД субектите на данни имат, inter alia, следните права по отношение на личните данни, обработвани за целите на националната сигурност:

1) правото да получават потвърждение дали се обработват техни лични данни, както и информация за обработването и достъп до тези данни, включително предоставяне на копия (член 4, параграфи 1 и 3 от ЗЗЛД);

2) правото да спрат обработването и да поискат коригиране, заличаване и унищожаване на такива лични данни (член 4, параграф 4 от ЗЗЛД).

iii) Субектът на данни може да подаде искане за упражняване на тези права пряко до администратора или непряко — чрез Комисията за защита — и може да упълномощи свой представител да направи това. Когато субектът на данни подаде искане, администраторът предоставя правото незабавно; като може обаче да забави, ограничи или откаже това право, ако е изрично предвидено в други закони или е неизбежно спазването на други закони, доколкото и докато това е необходимо и пропорционално за защитата на важна цел от обществен интерес (например доколкото и докато предоставянето на правото би застрашило текущо разследване или би представлявало заплаха за националната сигурност), или когато предоставянето на правото може да доведе до вредни последствия за живота или до телесно увреждане на трета страна, или до необосновано накърняване на имуществени и други интереси на трета страна. Когато искането е отхвърлено или ограничено, той незабавно уведомява субекта на данни за причините. Администраторът изготвя метода и процедурата, които позволяват на субектите на данни да подават искания, и ги обявява публично, така че субектите на данни да могат да се запознаят с тях.

Освен това, в съответствие с член 58, параграф 4 от ЗЗЛД (изискване за гарантиране на разглеждане на индивидуални жалби по подходящ начин) и член 4, параграф 5 от ЗЗЛД (право на подходяща защита по отношение на вреди, произтичащи от обработването на лични данни, чрез бърза и справедлива процедура), субектите на данни имат право да получат правна защита. Това включва правото да се подаде сигнал за предполагаемо нарушение до Центъра за подаване на сигнали за нарушения, свързани с личните данни (в съответствие с член 62, параграф 3 от ЗЗЛД), да се подаде жалба до КЗЛД в съответствие с член 62 от ЗЗЛД за всяко нарушение на правата или интересите, свързани с личните данни на физическо лице, и да се получи съдебна защита срещу решения или бездействие на КЗЛД съгласно Закона за административното съдопроизводство. Освен това субектите на данни могат да получат съдебна защита по реда на Закона за административното съдопроизводство, ако е налице нарушение на техните права или интереси поради разпореждане или бездействие от страна на администратора (напр. незаконно събиране на лични данни), или да получат обезщетение за вреди в съответствие със Закона за обезщетенията от държавата. Тези средства за правна защита са налични както в случай на евентуални нарушения на правилата, съдържащи се в конкретни закони, определящи ограниченията и защитните мерки по отношение на събирането на лични данни, като например законодателството в областта на националната сигурност, така и в ЗЗЛД.

Физическо лице от ЕС може да подаде жалба до КЗЛД чрез своя национален орган за защита на данните, а КЗЛД ще уведоми физическото лице чрез националния орган за защита на данните след приключването на разследването и на корективни мерки (ако е приложимо).

ПРИЛОЖЕНИЕ II

18 май 2021 г.

Негово Превъзходителство г-н Дидие Рейндерс, комисар по въпросите на правосъдието в Европейската комисия

Ваше Превъзходителство,

Приветствам конструктивните обсъждания между Корея и Европейската комисия, насочени към изграждане на рамка за предаване на лични данни от ЕС към Корея.

По искане от Европейската комисия до правителството на Корея изпращам приложен документ, в който се прави преглед на правната уредба относно достъпа до информация от правителството на Корея.

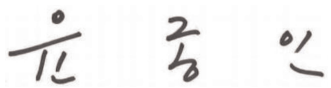
Този документ засяга много министерства и органи на правителството на Корея, а по отношение на съдържанието на документа съответните министерства и органи (Комисията за защита на личните данни, Министерството на правосъдието, Националната разузнавателна служба, Националната комисия на Корея по правата на човека, Националният център за борба с тероризма, корейското звено за финансово разузнаване) отговарят за пасажите в рамките на своите съответни компетенции. По-долу са посочени въпросните министерства и органи, както и съответните подписи.

Комисията за защита на личните данни приема всички запитвания по отношение на този документ и ще координира необходимите отговори между съответните министерства и органи.

Надявам се този документ да бъде от полза при вземането на решения в Европейската комисия.

Високо ценя Вашия голям принос в тази сфера досега.

С уважение,



Yoon Jong In
Председател на Комисията за защита на личните данни

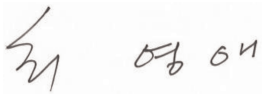
Настоящият документ е изготвен от Комисията за защита на личните данни и от следните заинтересовани министерства и органи.



Park Jie Won
Председател (директор), Национална разузнавателна служба



Lee Jung Soo
Генерален директор, Министерство на правосъдието



Choi Young Ae
Председател, Национална комисия на Корея по правата на човека



Kim Hyuck Soo
Директор, Национален център за борба с тероризма



Kim, Jeong Kag
Комисар, корейско звено за финансово разузнаване

Правна уредба за събирането и използването на лични данни от корейските публични органи за целите на правоприлагането и националната сигурност

Настоящият документ предоставя общ преглед на правната уредба за събирането и използването на лични данни от корейските публични органи за целите на наказателното правоприлагане и националната сигурност (наричан по-нататък „*достъп на държавните органи*“), по-специално по отношение на наличните правни основания, приложимите условия (ограничения) и защитни мерки, както и възможностите за независим надзор и средства за индивидуална правна защита.

1. ОБЩИ ПРАВНИ ПРИНЦИПИ ОТ ЗНАЧЕНИЕ ЗА ДОСТЪПА НА ДЪРЖАВНИТЕ ОРГАНИ

1.1. Конституционна уредба

В Конституцията на Република Корея се установява правото на неприкосновеност на личния живот като цяло (член 17) и правото на неприкосновеност на кореспонденцията в частност (член 18). Държавата има задължението да гарантира тези основни права ([1]). Освен това в Конституцията се постановява, че правата и свободите на гражданите могат да бъдат ограничавани само със закон и когато това е необходимо за националната сигурност или за поддържането на законността и реда за благото на обществото ([2]). Дори когато се налагат такива ограничения, те не могат да засягат същността на свободата или правото ([3]). Корейските съдилища прилагат тези разпоредби в случаи на намеса на държавата в личния живот. Например Върховният съд установява, че наблюдението на граждански лица нарушава основното право на неприкосновеност на личния живот, като подчертава, че гражданите имат „*правото на самоопределяне по отношение на личните данни*“ ([4]). По друго дело Конституционният съд постановява, че неприкосновеността на личния живот е основно право, което предвижда защита от държавна намеса и от наблюдение по отношение на личния живот на гражданите ([5]).

Освен това в Конституцията на Корея се гарантира, че никое лице не може да бъде арестувано, задържано, претърсвано, разпитвано или да бъдат изземвани вещи от него, освен в случаите, предвидени от закона ([6]). Освен това претърсвания и изземвания могат да се извършват само въз основа на заповед, издадена от съдия, по искане на прокурор и при спазване на надлежната процедура ([7]). При извънредни обстоятелства, т.е. когато заподозряно в престъпление лице е задържано по време на извършване на престъпление (*flagrante delicto*) или когато съществува риск лице, заподозряно в извършването на престъпление, наказуемо с лишаване от свобода за срок от три или повече години, да се укрие или да унищожи доказателства, разследващите органи могат да извършат претърсване или изземване без съдебна заповед, като в този случай те трябва да поискат съдебна заповед ex post ([8]). Тези общи принципи са доразвити в специални закони, отнасящи се до наказателното производство и до защитата на комуникациите (вж. по-долу за подробен преглед).

По отношение на чужденците в Конституцията се постановява, че техният статут е гарантиран, както е предвидено в международното право и в договорите ([9]). 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, макар че Конституцията по принцип се позовава на правата на „*гражданите*“, Конституционният съд постановява, че и чужденците имат основни права ([10]). По-специално Съдът постановява, че защитата на достойнството и стойността на човека като човешко същество, както и правото да търси щастие са права на всяко човешко същество, а не само на

([1]) Член 10 от Конституцията на Република Корея, обнародвана на 17 юли 1948 г. (наричана по-нататък „Конституцията“).
([2]) Член 37, параграф 2 от Конституцията.
([3]) Член 37, параграф 2 от Конституцията.
([4]) Решение № 96DA42789 на Върховния съд на Корея, 24 юли 1998 г.
([5]) Решение № 2002Hun-Ma51 на Конституционния съд, 30 октомври 2003 г. По подобен начин в Решение № 99Hun-Ma513 и 2004Hun-Ma190 (консолидирано) от 26 май 2005 г. Конституционният съд пояснява, че „*правото на контрол по отношение на нечии лични данни е право на субекта на данни лично да решава кога, на кого или от кого и в каква степен да бъдат разкривани или използвани неговите данни. Макар и да не е посочено в Конституцията, това е основно право, съществуващо за защита на личната свобода на вземане на решения от риска, предизвикан от разширяването на държавните функции и информационните и комуникационните технологии*“.
([6]) Член 12, параграф 1, първо изречение от Конституцията.
([7]) Член 16 и член 12, параграф 3 от Конституцията.
([8]) Член 12, параграф 3 от Конституцията.
([9]) Член 6, параграф 2 от Конституцията.
([10]) Решение № 93Hun-MA120 на Конституционния съд, 29 декември 1994 г. Вж. също например Решение № 2014Hun-Ma346 на Конституционния съд (31 май 2018 г.), в което съдът установява, че е нарушено конституционното право на получаване на помощ от правен съветник на суданski гражданин, задържан на летището. В друг случай Конституционният съд установява, че свободата на избор на законно работно място е тясно свързана с правото на търсене на щастие, както и с човешкото достойнство и стойност, и следователно не е запазена само за гражданите, а може да бъде гарантирана и на чужденците, които са законно наети на работа в Република Корея (Решение № 2007Hun-Ma1083 на Конституционния съд, 29 септември 2011 г.).

гражданите ([11]). Съдът също така разяснява, че правото на контрол по отношение на собствените данни се смята за основно право, залегнало в правото на достойнство и стремеж към щастие, както и на правото на личен живот ([12]). Въпреки че съдебната практика досега не е разглеждала конкретно правото на неприкосновеност на личния живот на лицата, които не са граждани на Корея, сред учените е широко прието, че в членове 12—22 от Конституцията (които включват правото на неприкосновеност на личния живот, както и на лична свобода) се определят „*правата на човешките същества*“.

И накрая, в Конституцията се предвижда и правото да се иска справедливо обезщетение от публичните органи ([13]). Освен това въз основа на Закона за Конституционния съд всяко лице, чиито основни права, гарантирани от Конституцията, са нарушени от упражняването на публичната власт (с изключение на решенията на съдилищата), може да подаде конституционна жалба до Конституционния съд ([14]).

1.2. **Общи правила за защита на данните**

Общият закон за защита на данните в Република Корея — Законът за защита на личните данни (наричан по-нататък „*ЗЗЛД*“), се прилага както за частния, така и за държавния сектор. По отношение на публичните органи в ЗЗЛД се посочва изрично задължението за формулиране на политики за предотвратяване на „*злоупотреба с лични данни и тяхното неправомерно използване, недискретно наблюдение и проследяване и т.н., както и за укрепване на достойнството на човешките същества и неприкосновеността на личния живот на физическите лица*“ ([15]).

Обработването на лични данни за целите на правоприлагането се подчинява на всички изисквания по ЗЗЛД. Това означава например, че органите за наказателно правоприлагане трябва да спазват задълженията за законосъобразно обработване, т.е. да се позовават на едно от правните основания, изброени в ЗЗЛД за събирането, използването или предоставянето на лични данни (членове 15—18 от ЗЗЛД), както и на принципите на ограничение на целите (член 3, параграфи 1 и 2 от ЗЗЛД), пропорционалност/свеждане на данните до минимум (член 3, параграфи 1 и 6 от ЗЗЛД), ограничено съхраняване на данни (член 21 от ЗЗЛД), сигурност на данните, включително уведомяване за нарушения по отношение на данните (член 3, параграф 4, членове 29 и 34 от ЗЗЛД), и прозрачност (член 3, параграфи 1 и 5, членове 20, 30 и 32 от ЗЗЛД). Специфични предпазни мерки се прилагат по отношение на чувствителната информация (член 23 от ЗЗЛД). Освен това в съответствие с член 3, параграф 5 и член 4 от ЗЗЛД, както и с членове 35—39-2 от ЗЗЛД, физическите лица могат да упражняват правата си на достъп, коригиране, заличаване и спиране на използването vis-à-vis с правоприлагащите органи.

Въпреки че ЗЗЛД се прилага изцяло за обработването на лични данни за целите на наказателното правоприлагане, той съдържа изключение, когато личните данни се обработват за целите на националната сигурност. В съответствие с член 58, параграф 1, точка 2 от ЗЗЛД членове 15—50 от ЗЗЛД не се прилагат по отношение на лични данни, събирани или поискани за анализ на информация, свързана с националната сигурност ([16]). От друга страна, приложими остават глава I (Общи разпоредби), глава II (Установяване на политики за защита на личните данни и др.), глава VIII (Колективен иск при нарушения в областта на данните), глава IX (Допълнителни разпоредби) и глава X (Наказателни разпоредби) от ЗЗЛД. Това включва общите принципи за защита на данните, посочени в член 3 (Принципи за защита на личните данни), и личните права, гарантирани по член 4 от ЗЗЛД (Права на субектите на данни). Това означава, че основните принципи и права са гарантирани и в тази област. Освен това в член 58, параграф 4 от ЗЗЛД се предвижда, че такива данни трябва да се обработват в минимално необходимата степен за постигане на предвидената цел и за минимален период от време. В него се изисква също така администраторът на лични данни да въведе необходимите мерки за осигуряване на безопасно управление и подходящо обработване на данните, като например технически, управленски и физически защитни мерки, както и мерки за разглеждане по подходящ начин на индивидуални жалби.

В Уведомление № 2021-1 относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни Комисията за защита на личните данни (наричана по-нататък „*КЗЛД*“) допълнително разяснява как се прилага ЗЗЛД по отношение на обработването на лични данни за целите на националната сигурност в светлината на това частично изключение ([17]). Това включва по-специално правата на физическите лица (достъп, коригиране, спиране и заличаване), основанията, както и ограниченията за възможното им ограничаване. Според уведомлението прилагането на основните принципи, права и задължения съгласно ЗЗЛД по отношение на обработването на лични данни за целите

([11]) Решение № 99HeonMa494 на Конституционния съд, 29 ноември 2001 г.
([12]) Вж. например Решение № 99HunMa513 на Конституционния съд.
([13]) Член 29, параграф 1 от Конституцията.
([14]) Член 68, параграф 1 от Закона за Конституционния съд.
([15]) Член 5, параграф 1 от ЗЗЛД.
([16]) Член 58, параграф 1, точка 2 от ЗЗЛД.
([17]) Уведомление № 2021-1 на КЗЛД относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни, раздел III, точка 6.

на националната сигурност отразява залегналите в Конституцията гаранции за защита на правото на физическото лице да контролира собствените си лични данни. Всяко ограничаване на това право, например когато е необходимо за защита на националната сигурност, изисква балансиране между правата и интересите на физическото лице и съответния обществен интерес и не може да засяга същността на това право (член 37, параграф 2 от Конституцията).

2. ДОСТЪП НА ДЪРЖАВНИТЕ ОРГАНИ ЗА ЦЕЛИТЕ НА ПРАВОПРИЛАГАНЕТО

2.1. Компетентни публични органи в областта на правоприлагането

Въз основа на Наказателнопроцесуалния закон (наричан по-нататък „*НПЗ*“), Закона за защита на неприкосновеността на комуникациите (наричан по-нататък „*ЗЗНК*“) и Закона за телекомуникационните дейности (наричан по-нататък „*ЗТД*“) полицията, прокуратурата и съдилищата могат да събират лични данни за целите на наказателното правоприлагане. Доколкото в Закона за Националната разузнавателна служба това правомощие се предоставя и на Националната разузнавателна служба (наричана по-нататък „*НРС*“), тя трябва да се съобразява с гореспоменатите закони ([18]). И накрая, в Закона за докладване и използване на конкретна информация за финансови сделки (наричан по-нататък „ЗДИКИФС“) се предоставя правно основание на финансовите институции да разкриват информация на корейското звено за финансово разузнаване (наричано по-нататък „КЗФР“) с цел предотвратяване на изпирането на пари и финансирането на тероризма. Тази специализирана агенция може на свой ред да предоставя такава информация на правоприлагащите органи. Тези задължения за разкриване обаче се отнасят само за администратори на данни, които обработват лична кредитна информация в съответствие със Закона за кредитната информация и са обект на надзор от страна на Комисията по финансови услуги. Тъй като обработването на лична кредитна информация от такива администратори е изключено от обхвата на решението относно адекватното ниво на защита, ограниченията и защитните мерки, които се прилагат съгласно ЗДИКИФС, не са описани по-подробно в настоящия документ.

2.2. Правни основания и ограничения

В НПЗ (вж. 2.2.1), ЗЗНК (вж. 2.2.2) и Закона за телекомуникационните дейности (вж. 2.2.3) се предоставят правни основания за събирането на лични данни за целите на правоприлагането и се определят приложимите ограничения и защитни мерки.

2.2.1. *Претърсвания и изземвания*

2.2.1.1. Правно основание

Прокурорите и висшите служители на съдебната полиция могат да извършват огледи на предмети, да претърсват лица или да изземват предмети само ако 1) дадено лице е заподозряно в извършването на престъпление (заподозряно в извършване на престъпление лице), 2) това е необходимо за разследването и 3) предметите, които трябва да бъдат подложени на оглед, лицата, които трябва да бъдат претърсени, и всички иззети предмети се смятат за свързани с делото ([19]). По подобен начин съдилищата могат да извършват претърсвания и да изземват всякакви предмети, които да бъдат използвани като доказателства или да подлежат на конфискация, стига да се смята, че тези предмети или лица са свързани с конкретно дело ([20]).

2.2.1.2. Ограничения и защитни мерки

Като общо задължение прокурорите и служителите на съдебната полиция трябва да зачитат човешките права на заподозрения в извършване на престъпление, както и на всяко друго засегнато лице ([21]). Освен това принудителни мерки за постигане на целта на разследването могат да се предприемат само когато това е изрично предвидено в НПЗ и във възможно най-малката необходима степен ([22]).

Претърсвания, огледи или изземвания от полицейски служители или прокурори в рамките на наказателно разследване могат да се извършват само въз основа на издадена съдебна заповед ([23]). Органът, който изисква заповедта, трябва да представи материали, доказващи основанията за подозрение, че дадено физическо лице е извършило престъпление, че претърсването, огледът или изземването са необходими и че съответните предмети, които трябва да бъдат иззети, съществуват ([24]). Що се отнася до заповедта, тя трябва да съдържа, наред с други елементи, имената на заподозряното в извършване на престъпление лице и престъплението; мястото, лицето или предметите, които трябва да бъдат претърсени, или предметите, които трябва да бъдат иззети; датата на издаване; както и срока на действие на прилагането ([25]). По подобен начин, когато в рамките на текущо съдебно производство се извършват претърсвания и изземвания, различни от тези в открито съдебно заседание, трябва предварително да се получи издадена от съд заповед ([26]). Съответното физическо лице и неговият съдебен защитник се уведомяват предварително за претърсването или изземването и могат да присъстват по време на изпълнението на заповедта ([27]).

([18]) Вж. член 3 от Закона за НРС (Закон № 12948), който се отнася до наказателни разследвания на определени престъпления, като въстание, бунт и престъпления, свързани с националната сигурност (напр. шпионаж). В такъв контекст ще се прилагат процедурите съгласно НПЗ по отношение на претърсването и изземването, докато ЗЗНК ще урежда събирането на комуникационни данни (вж. част 3 относно разпоредбите, отнасящи се до достъпа до комуникации за целите на националната сигурност).
([19]) Член 215, параграфи 1 и 2 от НПЗ.
([20]) Член 106, параграф 1, членове 107 и 109 от НПЗ.
([21]) Член 198, параграф 2 от НПЗ.
([22]) Член 199, параграф 1 от НПЗ.
([23]) Член 215, параграфи 1 и 2 от НПЗ.
([24]) Член 108, параграф 1 от Наредбата за наказателния процес.
([25]) Член 114,параграф 1 от НПЗ, във връзка с член 219 от НПЗ.
([26]) Член 113 от НПЗ.
([27]) Членове 121 и 122 от НПЗ.

При извършване на претърсвания или изземвания, когато претърсваният предмет е компютърен диск или друг носител за съхранение на данни, по принцип се изземват само самите данни (копирани или разпечатани), а не целият носител ([28]). Самият носител за съхранение на данни може да бъде иззет само когато се смята, че е практически невъзможно необходимите данни да се разпечатат или копират отделно, или когато се смята, че е практически невъзможно по друг начин да се постигне целта на претърсването ([29]). Засегнатото физическо лице трябва да бъде незабавно уведомено за изземването ([30]). В НПЗ не са предвидени изключения от това изискване за уведомяване.

Претърсвания, огледи и изземвания без съдебна заповед могат да се извършват само в ограничени случаи. Първо, такъв е случаят, когато е невъзможно да се получи заповед поради неотложност на мястото на престъплението ([31]). Впоследствие обаче трябва незабавно да бъде получена заповед ([32]). Второ, претърсванията и огледите без съдебна заповед могат да се извършват in loco, когато е арестувано или задържано заподозряно в извършване на престъпление лице ([33]). И накрая, прокурор или висш служител на съдебната полиция може да изземе предмет без заповед, когато предметът е бил изхвърлен от заподозряно в извършване на престъпление лице или от трето лице, или е бил представен доброволно ([34]).

Доказателства, които са получени в нарушение на НПЗ, се смятат за недопустими ([35]). Освен това в Наказателния закон се предвижда, че незаконното претърсване на лица или на жилище на лице, на охранявана сграда, на здание, на автомобил, на кораб, на въздухоплавателно средство или на обитавано помещение се наказва с лишаване от свобода за максимален срок от три години ([36]). Следователно тази разпоредба се прилага и в случаите, когато по време на незаконно претърсване са иззети предмети, като например устройства за съхранение на данни.

2.2.2. *Събиране на комуникационни данни*

2.2.2.1. Правно основание

Събирането на комуникационни данни се урежда от специален закон — ЗЗНК. По-специално, в ЗЗНК се предвижда забрана за когото и да било да цензурира каквато и да е поща, да подслушва каквито и да е телекомуникации, да предоставя данни за потвърждаване на комуникациите, да записва или да слуша разговори между други лица, които не са публично достояние, освен на основание на НПЗ, ЗЗНК или Закона за военните съдилища ([37]). Терминът „*комуникация*“ по смисъла на ЗЗНК обхваща както обикновената поща, така и телекомуникациите ([38]). В това отношение в ЗЗНК се прави разграничение между „*мерки за ограничаване на комуникациите*“ ([39]) и събирането на „*данни за потвърждаване на комуникациите*“.

Понятието „мерки за ограничаване на комуникациите“ обхваща „*цензура*“, т.е. събирането на съдържанието на традиционните пощенски пратки, както и „*подслушване*“, т.е. прякото прихващане (придобиване или записване) на съдържанието на телекомуникации ([40]). Понятието „данни за потвърждаване на комуникациите“ обхваща „*данни относно записите на телекомуникациите*“, които включват датата на телекомуникациите, началния и крайния им час, броя на изходящите и входящите повиквания, както и абонатния номер на другата страна, честотата на използване, регистрационни файлове за използването на телекомуникационни услуги и информация за местоположението (напр. от предавателните кули, в които се приемат сигнали) ([41]).

([28]) Член 106, параграф 3 от НПЗ.
([29]) Член 106, параграф 3 от НПЗ.
([30]) Член 219 от НПЗ, във връзка с член 106, параграф 4 от НПЗ.
([31]) Член 216, параграф 3 от НПЗ.
([32]) Член 216, параграф 3 от НПЗ.
([33]) Член 216, параграфи 1 и 2 от НПЗ.
([34]) Член 218 от НПЗ. Що се отнася до личните данни, това се отнася само до доброволното им предоставяне от самото засегнато физическо лице, а не от администратор на лични данни, който разполага с такива данни (което би изисквало специално правно основание съгласно Закона за защита на личните данни). Доброволно предоставени предмети се приемат като доказателство в съдебното производство само ако не съществува основателно съмнение относно доброволния характер на разкриването, което трябва да се докаже от прокурора. Вж. Решение № 2013Do11233 на Върховния съд, 10 март 2016 г.
([35]) Член 308-2 от НПЗ.
([36]) Член 321 от Наказателния закон.
([37]) Член 3 от ЗЗНК. В Закона за военните съдилища по принцип се урежда събирането на информация за военнослужещи и може да се прилага по отношение на граждански лица само в ограничен брой случаи (напр. ако военнослужещи и граждански лица извършат престъпление заедно или ако дадено физическо лице извърши престъпление срещу армията, може да бъде образувано производство пред военен съд, вж. член 2 от Закона за военните съдилища). Общите разпоредби, уреждащи претърсването и изземването, са сходни с тези в НПЗ. Вж. напр. членове 146—149 и 153—156 от Закона за военните съдилища. Например пощенски пратки могат да се събират само когато това е необходимо за разследване и въз основа на заповед на Военния съд. Доколкото биха се събирали електронни съобщения, се прилагат ограниченията и защитните мерки съгласно ЗЗНК.
([38]) Член 2, параграф 1 от ЗЗНК, т.е. „*предаване или приемане на всички видове звуци, думи, символи или изображения по жица, безжично, по оптичен кабел или чрез друга електромагнитна система, включително телефон, електронна поща, информационна услуга за членове, по факс и чрез радио пейджинг*“.
([39]) Член 2, параграф 7 и член 3, параграф 2 от ЗЗНК.
([40]) „Цензура“ се определя като „*отваряне на поща без съгласието на засегнатата страна или узнаване, записване или задържане на нейното съдържание по друг начин*“ (член 2, параграф 6 от ЗЗНК). „Подслушване“ означава „*придобиване или записване на съдържанието на телекомуникациите чрез прослушване или кумулативно четене на звуците, думите, символите или изображенията на комуникациите чрез електронни и механични устройства без съгласието на засегнатата страна или намеса в предаването и приемането им*“ (член 2, параграф 7 от ЗЗНК).
([41]) Член 2, параграф 11 от ЗЗНК.

В ЗЗНК се определят ограниченията и защитните мерки за събирането на двата вида данни, а неспазването на някои от тези изисквания подлежи на наказателна отговорност ([42]).

2.2.2.2. Ограничения и защитни мерки, приложими по отношение на събирането на съдържанието на комуникациите (мерки за ограничаване на комуникациите)

Събирането на съдържанието на комуникациите може да се извършва само като допълнително средство за улесняване на наказателно разследване (т.е. като крайна мярка) и трябва да се полагат усилия за свеждане до минимум на намесата в тайната на комуникацията на хората ([43]). В съответствие с този общ принцип мерките за ограничаване на комуникациите могат да се прилагат само когато е трудно по друг начин да се предотврати извършването на престъпление, да се арестува престъпникът или да се съберат доказателства ([44]). Правоприлагащите органи, които събират съдържанието на комуникациите, трябва незабавно да преустановят това, след като продължаването на достъпа до тях вече не се смята за необходимо, като по този начин се гарантира, че нарушаването на неприкосновеността на комуникациите е възможно най-ограничено ([45]).

Освен това мерките за ограничаване на комуникациите могат да се използват само когато има съществени основания да се подозира, че се планират, извършват или са извършени определени тежки престъпления, изрично изброени в ЗЗНК. Те включват престъпления като бунт, престъпления, свързани с наркотици или експлозиви, както и престъпления, свързани с националната сигурност, дипломатическите отношения или военните бази и съоръжения ([46]). Мярката за ограничаване на комуникациите трябва да бъде насочена към конкретни пощенски пратки или телекомуникации, изпратени или получени от заподозрения, или към пощенски пратки или телекомуникации, изпратени или получени от заподозрения по време на определен период от време ([47]).

Дори когато тези изисквания са изпълнени, събирането на данни за съдържанието може да се извършва само въз основа на издадена съдебна заповед. По-специално прокурорът може да поиска от съда да разреши събирането на данни за съдържанието по отношение на заподозряното или разследваното лице ([48]). По подобен начин служител на съдебната полиция може да подаде молба за искане на разрешение до прокурор, който на свой ред може да поиска заповед от съда ([49]). Искането за издаване на заповед трябва да бъде направено в писмена форма и да съдържа конкретни елементи. По-специално в него трябва да се посочат 1) наличието на съществени основания да се подозира, че се планира, извършва или е извършено някое от изброените престъпления, както и всички материали, установяващи вероятна основателност на иска; 2) мерките за ограничаване на комуникациите, както и техните цел, обхват, задачи и срок на действие; и 3) мястото, където ще се изпълняват мерките, и начинът, по който ще се провеждат ([50]).

Когато са изпълнени законовите изисквания, съдът може да даде писмено разрешение за прилагане на мерки за ограничаване на комуникациите по отношение на заподозряното или разследваното лице ([51]). В тази заповед се посочват видовете мерки, както и техните цел, обхват, срок на действие, място и начин на изпълнение ([52]).

Мерките за ограничаване на комуникациите може да се прилагат само за период от два месеца ([53]). Ако целта на мерките бъде постигната по-рано в рамките на този период, мерките трябва да бъдат преустановени незабавно. От друга страна, ако необходимите условия все още са изпълнени, в рамките на двумесечния срок може да бъде подадено искане за удължаване на срока на действие на мерките за ограничаване на комуникациите. Такова искане трябва да включва материали, установяващи вероятна основателност на иска за удължаване на срока на мерките ([54]). Удълженият срок не може да надвишава общо една година или три години за някои особено тежки престъпления (напр. престъпления, свързани с въстание, с външна агресия, с националната сигурност и др.) ([55]).

Правоприлагащите органи могат да задължат операторите на комуникационни услуги да съдействат, като им предоставят писмено разрешение от съда ([56]). От операторите на комуникационни услуги се изисква да съдействат и да съхраняват полученото разрешение в своите досиета ([57]). Те могат да откажат съдействие, когато информацията за засегнатото физическо лице, както е посочено в писменото разрешение от съда (напр. телефонният номер на физическото лице), е невярна. Освен това при всякакви обстоятелства им е забранено да разкриват пароли, използвани за осъществяване на телекомуникации ([58]).

([42]) Членове 16 и 17 от ЗЗНК. Това се отнася например за събирането на данни без съдебна заповед, за липсата на регистър, непреустановяването на събирането на данни при отпадане на извънредната ситуация или неуведомяването на съответното физическо лице.
([43]) Член 3, параграф 2 от ЗЗНК.
([44]) Член 5, параграф 1 от ЗЗНК.
([45]) Член 2 от Указа за прилагане на ЗЗНК.
([46]) Член 5, параграф 1 от ЗЗНК.
([47]) Член 5, параграф 2 от ЗЗНК.
([48]) Член 6, параграф 1 от ЗЗНК.
([49]) Член 6, параграф 2 от ЗЗНК.
([50]) Член 6, параграф 4 от ЗЗНК и член 4, параграф 1 от Указа за прилагане на ЗЗНК.
([51]) Член 6, параграф 5 и член 6, параграф 8 от ЗЗНК.
([52]) Член 6, параграф 6 от ЗЗНК.
([53]) Член 6, параграф 7 от ЗЗНК.
([54]) Член 6, параграф 7 от ЗЗНК.
([55]) Член 6, параграф 8 от ЗЗНК.
([56]) Член 9, параграф 2 от ЗЗНК.
([57]) Член 15-2 от ЗЗНК и член 12 от Указа за прилагане на ЗЗНК.
([58]) Член 9, параграф 4 от ЗЗНК.

Всеки, който изпълнява мерки за ограничаване на комуникациите или от когото е поискано съдействие, трябва да поддържа регистър, в който се посочват целите на мерките, тяхното изпълнение, датата, на която е оказано съдействие, и целта ([59]). Правоприлагащите органи, които прилагат мерки за ограничаване на комуникациите, също трябва да водят регистър, в който се посочват подробностите и получените резултати ([60]). Служителите на съдебната полиция трябва да предоставят тази информация чрез доклад до прокурора, когато приключат с разследването ([61]).

Когато прокурор повдигне обвинение по дело, по което са били използвани мерки за ограничаване на комуникациите, или издаде разпореждане да не се повдига обвинение или да не се арестува съответното физическо лице (т.е. не просто спиране на наказателното преследване), прокурорът трябва да уведоми физическото лице, обект на мерките за ограничаване на комуникациите, за факта, че са били приложени мерки за ограничаване на комуникациите, за изпълняващия орган и за периода на изпълнение. Това уведомление трябва да бъде предоставено в писмен вид в рамките на 30 дни от разпореждането ([62]). Уведомлението може да бъде отсрочено, когато има вероятност с него да се застраши сериозно националната сигурност или да се нарушат обществената сигурност и ред, или когато има вероятност да доведе до вредни последствия за живота и тялото на други хора ([63]). Когато възнамерява да отсрочи уведомяването, прокурорът или служителят на съдебната полиция трябва да получи одобрение от ръководителя на районната прокуратура ([64]). След като основанията за сезиране престанат да съществуват, трябва да бъде предоставено уведомление в рамките на 30 дни от този момент ([65]).

В ЗЗНК се определя и конкретна процедура за събиране на съдържанието на комуникациите при извънредни ситуации. По-специално правоприлагащите органи могат да събират съдържанието на комуникациите, в случай че планирането или извършването на организирано престъпление или друго тежко престъпление, което може пряко да причини смърт или сериозна вреда, е предстоящо и е налице извънредна ситуация, която прави невъзможно преминаването през редовната процедура (както е посочено по-горе) ([66]). При такъв спешен случай полицейският служител или прокурорът може да предприеме мерки за ограничаване на комуникациите без предварително разрешение от съда, но трябва да подаде молба за разрешение от съда веднага след изпълнението. Ако правоприлагащият орган не успее да получи разрешение от съда в рамките на 36 часа от момента, в който са предприети спешните мерки, събирането трябва да бъде преустановено незабавно, обикновено последвано от унищожаване на събраната информация ([67]). Полицейските служители, които извършват спешно наблюдение, извършват това под контрола на прокурор, а в случай че получаването на предварителни указания от прокурора е невъзможно поради необходимостта от спешни действия, полицията трябва да получи одобрението на прокурора незабавно след започване на изпълнението ([68]). Правилата за уведомяване на физическото лице, описани по-горе, се прилагат и за събирането на съдържанието на комуникациите при извънредни ситуации.

Събирането на информация при извънредни ситуации винаги трябва да се извършва в съответствие с „*изявление за извънредна цензура/извънредно подслушване*“, а органът, който извършва събирането, трябва да води регистър за всяка спешна мярка ([69]). Искането до съда за издаване на разрешение за спешни мерки трябва да бъде придружено от писмен документ, в който се посочват необходимите мерки за ограничаване на комуникациите, целта, предметът, обхватът, периодът, мястото и начинът на изпълнение, както и обяснение как съответните мерки за ограничаване на комуникациите отговарят на изискванията по член 5, параграф 1 от ЗЗНК ([70]), заедно с подкрепящи документи.

В случаите, когато спешните мерки са завършени в кратък срок, изключвайки по този начин разрешение на съда (напр. ако заподозреният е арестуван веднага след започване на прихващането, което в резултат на това се прекратява), ръководителят на компетентната прокуратура връчва на компетентния съд официално уведомление за спешна мярка ([71]). В уведомлението трябва да се посочат целта, предметът, обхватът, периодът, мястото на изпълнение и начинът на събиране, както и основанията за неподаване на искане за съдебно разрешение ([72]). С това уведомление се позволява на получаващия съд да провери законосъобразността на събирането, като също трябва да бъде вписано в регистъра на уведомленията за спешни мерки.

([59]) Член 9, параграф 3 от ЗЗНК.
([60]) Член 18, параграф 1 от Указа за прилагане на ЗЗНК.
([61]) Член 18, параграф 2 от Указа за прилагане на ЗЗНК.
([62]) Член 9-2, параграф 1 от ЗЗНК.
([63]) Член 9-2, параграф 4 от ЗЗНК.
([64]) Член 9-2, параграф 5 от ЗЗНК.
([65]) Член 9-2, параграф 6 от ЗЗНК.
([66]) Член 8, параграф 1 от ЗЗНК.
([67]) Член 8, параграф 2 от ЗЗНК.
([68]) Член 8, параграф 3 от ЗЗНК и член 16, параграф 3 от Указа за прилагане на ЗЗНК.
([69]) Член 8, параграф 4 от ЗЗНК.
([70]) Това означава, че има съществени основания да се подозира, че се планират или извършват, или са били извършени определени тежки престъпления и е практически невъзможно по друг начин да се предотврати извършването на престъпление, да се арестува престъпникът или да се съберат доказателства.
([71]) Член 8, параграф 5 от ЗЗНК.
([72]) Член 8, параграфи 6 и 7 от ЗЗНК.

Като общо изискване съдържанието на комуникациите, придобито чрез прилагане на мерки за ограничаване на комуникациите на основание на ЗЗНК, може да се използва само за разследване, наказателно преследване или предотвратяване на конкретните престъпления, изброени по-горе, в дисциплинарно производство за същите престъпления, по иск за вреди, предявен от страна, участваща в комуникациите, или когато това е позволено от други закони ([73]).

При събирането на телекомуникации, предавани по интернет, се прилагат специални защитни мерки ([74]). Тази информация може да се използва само за разследване на тежките престъпления, изброени в член 5, параграф 1 от ЗЗНК. За да се запази информацията, трябва да се получи одобрение от съда, който е разрешил мерките за ограничаване на комуникациите ([75]). Искането за запазване трябва да съдържа информация относно мерките за ограничаване на комуникациите, резюме на резултатите от мерките, причините за запазването (заедно с подкрепящи материали) и телекомуникациите, които трябва да бъдат запазени ([76]). При липса на такова искане придобитите телекомуникации трябва да бъдат заличени в рамките на 14 дни след приключване на мерките за ограничаване на комуникациите ([77]). Ако искането бъде отхвърлено, телекомуникациите трябва да бъдат унищожени в срок от седем дни ([78]). При заличаване на телекомуникации в срок от седем дни трябва да се подаде доклад до съда, разрешил мерките за ограничаване на комуникациите, в който се посочват причините за заличаването, както и подробностите и сроковете за това.

По-общо казано, ако информацията е била незаконно получена чрез мерки за ограничаване на комуникациите, тя няма да бъде приета като доказателство в съдебно или дисциплинарно производство ([79]). Освен това в ЗЗНК се забранява на всяко лице, което предприема мерки за ограничаване на комуникациите, да разкрива поверителна информация, получена в хода на прилагането на тези мерки, както и да използва получената информация за накърняване на репутацията на лицата, спрямо които се прилагат мерките ([80]).

2.2.2.3. Ограничения и защитни мерки, приложими към събирането на данни за потвърждаване на комуникациите

На основание на ЗЗНК правоприлагащите органи могат да поискат от телекомуникационните оператори да предоставят данни за потвърждаване на комуникациите, когато това е необходимо за провеждане на разследване или изпълнение на присъда ([81]). За разлика от събирането на данни за съдържанието, възможността за събиране на данни за потвърждаване на комуникациите не е ограничена до определени конкретни престъпления. Въпреки това, както и в случая с данните за съдържанието, за събирането на данни за потвърждаване на комуникациите се изисква предварително писмено разрешение от съда при същите условия, както е описано по-горе ([82]). Когато поради причини за спешност е невъзможно да се получи съдебно разрешение, данните за потвърждаване на комуникациите могат да бъдат събрани без заповед, като в този случай разрешението трябва да бъде получено незабавно след изискването на данните и трябва да бъде предоставено на доставчика на телекомуникационни услуги ([83]). Ако не бъде получено последващо разрешение, събраната информация трябва да бъде унищожена ([84]).

Прокурорите, служителите на съдебната полиция и съдилищата трябва да поддържат регистър на исканията за предоставяне на данни за потвърждаване на комуникациите ([85]). Освен това доставчиците на телекомуникационни услуги трябва два пъти годишно да докладват на министъра на науката и ИКТ относно разкриването на данни за потвърждаване на комуникациите и да поддържат регистър за това в продължение на седем години, считано от датата, на която данните са били разкрити ([86]).

Физическите лица по принцип се уведомяват за факта, че са събрани данни за потвърждаване на комуникациите ([87]). Сроковете за това уведомление зависят от обстоятелствата по разследването ([88]). След като бъде взето решение за (не) започване на наказателно преследване, уведомлението трябва да бъде предоставено в срок от 30 дни. От друга страна, ако обвинението бъде спряно, уведомлението трябва да бъде предоставено в рамките на 30 дни след изтичането на една година от вземането на това решение. Във всеки случай уведомлението трябва да бъде предоставено в рамките на 30 дни след изтичането на една година от събирането на информацията.

Уведомлението може да бъде отсрочено, ако има вероятност 1) да застраши националната сигурност, обществената сигурност и ред, 2) да причини смърт или телесна повреда, 3) да попречи на справедливото съдебно производство (напр. да доведе до унищожаване на доказателства или заплашване на свидетели) или 4) да оклевети заподозряното

([73]) Член 12 от ЗЗНК.
([74]) Член 12-2 от ЗЗНК.
([75]) Прокурорът или полицейският служител, който изпълнява мерките за ограничаване на комуникациите, трябва да избере телекомуникациите, които трябва да бъдат запазени, в рамките на 14 дни след края на мерките и да поиска одобрение от съда (когато става въпрос за полицейски служител, молбата трябва да бъде подадена до прокурор, който на свой ред подава искането до съда), вж. член 12-2, параграфи 1 и 2 от ЗЗНК.
([76]) Член 12-2, параграф 3 от ЗЗНК.
([77]) Член 12-2, параграф 5 от ЗЗНК.
([78]) Член 12-2, параграф 5 от ЗЗНК.
([79]) Член 4 от ЗЗНК.
([80]) Член 11, параграф 2 от Указа за прилагане на ЗЗНК.
([81]) Член 13, параграф 1 от ЗЗНК.
([82]) Членове 13 и 6 от ЗЗНК.
([83]) Член 13, параграф 2 от ЗЗНК. Както и при спешните мерки за ограничаване на комуникациите, трябва да се изготви документ, в който се излагат подробностите по случая (заподозряното лице, мерките, които трябва да се предприемат, предполагаемото престъпление, както и спешността). Вж. член 37, параграф 5 от Указа за прилагане на ЗЗНК.
([84]) Член 13, параграф 3 от ЗЗНК.
([85]) Член 13, параграфи 5 и 6 от ЗЗНК.
([86]) Член 13, параграф 7 от ЗЗНК.
([87]) Вж. член 13-3, параграф 7 във връзка с член 9-2 от ЗЗНК.
([88]) Член 13-3, параграф 1 от ЗЗНК.

лице, жертвите или други лица, свързани с делото, или да накърни неприкосновеността на личния им живот ([89]). За уведомление въз основа на едно от горепосочените основания се изисква разрешение от директора на компетентната районна прокуратура ([90]). След като основанията за отсрочване престанат да съществуват, трябва да бъде предоставено уведомление в рамките на 30 дни от този момент ([91]).

Уведомените лица могат да отправят писмено запитване до прокурора или служителя на съдебната полиция относно причините за събирането на данните за потвърждаване на комуникациите ([92]). В този случай прокурорът или служителят на съдебната полиция трябва да представи причините в писмен вид в срок от 30 дни след получаване на запитването, освен ако не се прилага някое от горепосочените основания (изключения за отсрочване на уведомлението) ([93]).

2.2.3. *Доброволно разкриване от оператори на телекомуникационни дейности*

В член 83, параграф 3 от ЗТД се позволява на операторите на телекомуникационни дейности доброволно да изпълнят искане (отправено в подкрепа на наказателно производство, разследване или изпълнение на наказание) от съд, прокурор или ръководител на разследващ орган за разкриване на „*комуникационни данни*“. В контекста на ЗТД в понятието „*комуникационни данни*“ се включват името, регистрационният номер на местно лице, адресът и телефонният номер на потребител, датите, на които потребителите се абонират или прекратяват абонамента си, както и идентификационните кодове на потребителите (т.е. кодове, използвани за идентифициране на пълноправния потребител на компютърни системи или комуникационни мрежи) ([94]). За целите на ЗТД за потребители се смятат само лицата, които пряко сключват договори за услуги с корейски доставчик на телекомуникационни услуги ([95]). Вследствие на това ситуациите, в които физически лица от ЕС, чиито данни са били предадени на Република Корея, биха се смятали за потребители по смисъла на ЗТД, вероятно ще бъдат много ограничени, тъй като тези физически лица обикновено не сключват пряк договор с корейски оператор на телекомуникационни услуги.

Исканията за получаване на комуникационни данни въз основа на ЗТД трябва да бъдат направени в писмен вид и в тях да се посочват причините за искането, връзката със съответния потребител и обхвата на исканите данни ([96]). Когато е невъзможно да се предостави писмено искане поради спешност, писменото искане трябва да бъде предоставено веднага щом отпадне причината за спешността ([97]). Операторите на телекомуникационни дейности, които изпълняват искания за разкриване на комуникационни данни, трябва да съхраняват регистри, които съдържат записи, показващи, че комуникационните данни са били предоставени, както и свързаните с тях материали, като например писменото искане ([98]). Освен това операторите на телекомуникационни дейности трябва два пъти годишно да докладват на министъра на науката и ИКТ за предоставянето на комуникационни данни ([99]).

Операторите на телекомуникационни дейности не са задължени да изпълняват искания за разкриване на комуникационни данни въз основа на ЗТД. Поради това за всяко искане трябва да бъде направена оценка от оператора с оглед на приложимите изисквания за защита на данните съгласно ЗЗЛД. По-специално операторът на телекомуникационни дейности трябва да вземе предвид интересите на субекта на данни и може да не разкрива данните, ако има вероятност това да наруши несправедливо интересите на физическото лице или на трета страна ([100]). Освен това, в съответствие с Уведомление № 2021-1 относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни, засегнатото физическо лице трябва да бъде уведомено за разкриването. В изключителни ситуации такова уведомление може да бъде отложено, по-специално ако и доколкото уведомлението би застрашило текущо наказателно разследване или има вероятност да окаже вредни последствия върху живота или тялото на друго лице, когато тези права или интереси са очевидно по-висши от правата на субекта на данни ([101]).

През 2016 г. Върховният съд потвърди, че доброволното предоставяне на комуникационни данни от операторите на телекомуникационни дейности без съдебна заповед въз основа на ЗТД само по себе си не нарушава правото на информационно самоопределение на потребителя на телекомуникационна услуга. Същевременно Съдът уточнява, че такова нарушение ще е налице, ако е очевидно, че запитващият орган е злоупотребил с правомощията си да поиска разкриване на комуникационни данни, като по този начин е нарушил интересите на съответното физическо лице или на трета страна ([102]). В по-общ план всяко искане за доброволно разкриване от страна на правоприлагащ орган трябва да отговаря на принципите за законосъобразност, необходимост и пропорционалност, произтичащи от Конституцията на Корея (член 12, параграф 1 и член 37, параграф 2).

([89]) Член 13-3, параграф 2 от ЗЗНК.
([90]) Член 13-3, параграф 3 от ЗЗНК.
([91]) Член 13-3, параграф 4 от ЗЗНК.
([92]) Член 13-3, параграф 5 от ЗЗНК.
([93]) Член 13-3, параграф 6 от ЗЗНК.
([94]) Член 83, параграф 3 от ЗТД.
([95]) Член 2, параграф 9 от ЗТД.
([96]) Член 83, параграф 4 от ЗТД.
([97]) Член 83, параграф 4 от ЗТД.
([98]) Член 83, параграф 5 от ЗТД.
([99]) Член 83, параграф 6 от ЗТД.
([100]) Член 18, параграф 2 от ЗЗЛД.
([101]) Уведомление № 2021-1 на КЗЛД относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни, раздел III, глава 2, точка iii).
([102]) Решение № 2012Da105482 на Върховния съд, 10 март 2016 г.

2.3. **Надзор**

Надзорът върху органите за наказателно правоприлагане се осъществява чрез различни механизми, както вътрешно, така и от външни органи.

2.3.1. *Вътрешен одит*

В съответствие със Закона за одитите в държавния сектор публичните органи се насърчават да създават орган за вътрешен одит, който има за задача, наред с другото, да осъществява контрол на законосъобразността ([103]). На ръководителите на тези одитни органи трябва да бъде гарантирана независимост във възможно най-голяма степен ([104]). По-конкретно те се назначават измежду външни за съответния орган лица (напр. бивши съдии, преподаватели) за период от две до пет години и могат да бъдат освободени само по основателни причини (напр. когато не са в състояние да изпълняват задълженията си поради психическо или физическо заболяване, когато са обект на дисциплинарно наказание) ([105]). По същия начин одиторите се назначават въз основа на специфични условия, определени в закона ([106]). Одитните доклади могат да включват препоръки или искания за обезщетение за вреди или корекции, както и порицания и препоръки или искания за дисциплинарно наказание ([107]). Те се съобщават на ръководителя на публичния орган, който е обект на одита, както и на Съвета за одити и инспекции (вж. раздел 2.3.2) в рамките на 60 дни от приключването на одита ([108]). Съответният орган трябва да приложи необходимите мерки и да докладва за резултатите на Съвета за одити и инспекции ([109]). Освен това резултатите от одитите обикновено се оповестяват публично ([110]). Отказът от вътрешен одит или неговото възпрепятстване подлежи на административни глоби ([111]). В областта на наказателното правоприлагане, за да се спази гореспоменатото законодателство, в националната служба „Полиция“ функционира система на генералния инспектор, която се занимава с вътрешни одити, включително по отношение на възможни нарушения на правата на човека ([112]).

2.3.2. *Съвет за одити и инспекции*

Съветът за одити и инспекции (наричан по-нататък „*СОИ*“) може да инспектира дейността на публичните органи и въз основа на тези инспекции да издава препоръки, да изисква дисциплинарни наказания или да подава наказателни жалби ([113]). СОИ е създаден под ръководството на президента на Република Корея, но запазва независим статут по отношение на задълженията си ([114]). Освен това в закона за създаване на СОИ се изисква на СОИ да бъде предоставена независимост в максимална степен по отношение на назначаването, освобождаването и организирането на служителите, както и по отношение на съставянето на бюджета на съвета ([115]). Председателят на СОИ се назначава от президента с одобрението на Националното събрание ([116]). Останалите шестима комисари се назначават от президента по препоръка на председателя за срок от четири години ([117]). Комисарите (включително председателят) трябва да отговарят на конкретни критерии за квалификация, предвидени от закона ([118]), и могат да бъдат освобождавани от длъжност само в случай на импийчмънт, на осъждане на лишаване от свобода или на невъзможност да изпълняват задълженията си поради продължителна умствена или физическа слабост ([119]). Освен това на комисарите е забранено да участват в политически дейности, както и да заемат едновременно длъжности в Националното събрание, административни органи, организации, подлежащи на одити и инспекции от СОИ, или други длъжности или позиции, за които се получава възнаграждение ([120]).

СОИ извършва общ одит на годишна база, но може да извършва и конкретни одити по въпроси от особен интерес. СОИ може да поиска представянето на документи в хода на инспекцията и да поиска присъствието на физически лица ([121]). В рамките на одита СОИ проверява приходите и разходите на държавата, но също така следи за общото спазване на

([103]) Членове 3 и 5 от Закона за одитите в държавния сектор.
([104]) Член 7 от Закона за одитите в държавния сектор.
([105]) Членове 8—11 от Закона за одитите в държавния сектор.
([106]) Член 16 и сл. от Закона за одитите в държавния сектор.
([107]) Член 23, параграф 2 от Закона за одитите в държавния сектор.
([108]) Член 23, параграф 1 от Закона за одитите в държавния сектор.
([109]) Член 23, параграф 3 от Закона за одитите в държавния сектор.
([110]) Член 26 от Закона за одитите в държавния сектор.
([111]) Член 41 от Закона за одитите в държавния сектор.
([112]) Вж. по-специално отделите под ръководството на генералния директор за одити и инспекции: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Членове 24 и 31—35 от Закона за Съвета за одити и инспекции (наричан по-нататък „*Закона за СОИ*“).
([114]) Член 2, параграф 1 от Закона за СОИ.
([115]) Член 2, параграф 2 от Закона за СОИ.
([116]) Член 4, параграф 1 от Закона за СОИ.
([117]) Член 5, параграф 1 и член 6 от Закона за СОИ.
([118]) Например да са работили като съдия, прокурор или адвокат в продължение на поне десет години, да са работили като държавен служител, преподавател или на по-висока длъжност в университет в продължение на поне осем години или да са работили в продължение на поне десет години в дружество, чиито акции се търгуват на фондовата борса, или в институция с държавно участие (от които поне пет години като изпълнителен директор), вж. член 7 от Закона за СОИ.
([119]) Член 8 от Закона за СОИ.
([120]) Член 9 от Закона за СОИ.
([121]) Вж. напр. член 27 от Закона за СОИ.

задълженията на публичните органи и длъжностните лица с цел подобряване на работата на публичната администрация ([122]). Следователно надзорът на СОИ надхвърля бюджетните аспекти и включва също така контрол на законосъобразността.

2.3.3. *Националното събрание*

Националното събрание може да разследва и проверява публичните органи ([123]). По време на разследването или инспекцията Националното събрание може да поиска разкриване на документи и задължително явяване на свидетели ([124]). Всеки, който лъжесвидетелства по време на разследване на Националното събрание, подлежи на наказателна санкция (лишаване от свобода до десет години) ([125]). Процесът и резултатите от инспекциите могат да бъдат публично оповестени ([126]). Ако Националното събрание установи незаконосъобразна или неправилна дейност, то може да поиска от съответния публичен орган да предприеме корективни мерки, включително присъждане на обезщетение за вреди, предприемане на дисциплинарно наказание и подобряване на вътрешните си процедури ([127]). След такова искане органът трябва да предприеме незабавни действия и да докладва резултата на Националното събрание ([128]).

2.3.4. *Комисия за защита на личните данни*

Комисията за защита на личните данни (наричана по-нататък „*КЗЛД*“) упражнява надзор върху обработването на лични данни чрез органите за наказателното правоприлагане в съответствие със ЗЗЛД. Освен това съгласно член 7-8, параграфи 3 и 4 и член 7-9, параграф 5 от ЗЗЛД надзорът на КЗЛД обхваща и евентуални нарушения на правилата, определящи ограниченията и защитните мерки по отношение на събирането на лични данни, включително тези, които се съдържат в специалните закони, уреждащи събирането на (електронни) доказателства за целите на наказателното правоприлагане (вж. раздел 2.2). Предвид изискванията по член 3, параграф 1 от ЗЗЛД за законосъобразно и справедливо събиране на лични данни, всяко такова нарушение представлява нарушение на ЗЗЛД, което позволява на КЗЛД да провежда разследване и да предприема корективни мерки ([129]).

При упражняването на надзорната си функция КЗЛД има достъп до цялата необходима информация ([130]). КЗЛД може да дава съвети на правоприлагащите органи за подобряване на нивото на защита на личните данни по време на дейностите по обработването им, да налага корективни мерки (напр. да спира обработването на данни или да предприема необходимите мерки за защита на личните данни) или да предоставя съвети на органа за налагане на дисциплинарни наказания ([131]). Накрая, има предвидени наказателни санкции за някои нарушения на ЗЗЛД, като например незаконно използване или оповестяване на лични данни на трети страни или незаконно обработване на чувствителна информация ([132]). Във връзка с това КЗЛД може да отнесе въпроса до компетентния разследващ орган (включително прокурор) ([133]).

2.3.5. *Национална комисия по правата на човека*

Националната комисия по правата на човека (наричана по-нататък „*НКПЧ*“) — независим орган, натоварен със защитата и насърчаването на основните права ([134]) — има правомощията да разследва и да отстранява нарушения по членове 10—22 от Конституцията, които включват правото на неприкосновеност на личния живот и неприкосновеност на кореспонденцията. НКПЧ се състои от 11 комисари, назначени по предложение на Националното събрание (четирима), президента (четирима) и председателя на Върховния съд (трима) ([135]). За да бъде назначен, комисарят трябва 1) да е работил най-малко десет години в университет или упълномощен научноизследователски институт, поне като доцент; 2) да е работил като съдия, прокурор или адвокат в продължение на поне десет години; 3) да е участвал в дейности, свързани с правата на човека, в продължение на поне десет години (напр. в организация с нестопанска цел, неправителствена организация или международна организация); или 4) да е бил препоръчан от групи на гражданското общество ([136]). Председателят се назначава от президента измежду комисарите и трябва да бъде утвърден от

([122]) Членове 20 и 24 от Закона за СОИ.
([123]) Член 128 от Закона за Националното събрание и членове 2, 3 и 15 от Закона за инспекцията и разследването на държавната администрация. Това включва годишни инспекции на държавните дела като цяло и разследване на конкретни въпроси.
([124]) Член 10, параграф 1 от Закона за инспекцията и разследването на държавната администрация. Вж. също членове 128 и 129 от Закона за Националното събрание.
([125]) Член 14 от Закона за свидетелстване, оценка и др. пред Националното събрание.
([126]) Член 12-2 от Закона за инспекцията и разследването на държавната администрация.
([127]) Член 16, параграф 2 от Закона за инспекцията и разследването на държавната администрация.
([128]) Член 16, параграф 3 от Закона за инспекцията и разследването на държавната администрация.
([129]) Вж. Уведомление № 2021-1 на КЗЛД относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни.
([130]) Член 63 от ЗЗЛД.
([131]) Член 61, параграф 2, член 65, параграфи 1 и 2, и член 64, параграф 4 от ЗЗЛД.
([132]) Членове 70—74 от ЗЗЛД.
([133]) Член 65, параграф 1 от ЗЗЛД.
([134]) Член 1 от Закона за Комисията по правата на човека (наричан по-нататък „*Закон за НКПЧ*“).
([135]) Член 5, параграфи 1 и 2 от Закона за НКПЧ.
([136]) Член 5, параграф 3 от Закона за НКПЧ.

Националното събрание ([137]). Комисарите (включително председателят) се назначават за срок от три години, който може да се подновява, и могат да бъдат освободени от длъжност само в случай че им е наложено наказание лишаване от свобода или вече не са в състояние да изпълняват задълженията си поради продължителна физическа или психическа слабост (в този случай две трети от комисарите трябва да се съгласят с освобождаването от длъжност) ([138]). На комисарите в НКПЧ е забранено да заемат едновременно длъжност в Националното събрание, местните съвети или в който и да е държавен орган или орган на местното самоуправление (като публичен служител) ([139]).

НКПЧ може да започне разследване по своя инициатива или въз основа на петиция от дадено лице. Като част от разследването си НКПЧ може да поиска предоставянето на съответни материали, да извършва инспекции и да призовава физически лица да дават показания ([140]). След провеждане на разследване НКПЧ може да издаде препоръки за подобряване или коригиране на конкретни политики и практики и да ги оповести публично ([141]). Публичните органи трябва да уведомят НКПЧ за план за изпълнение на тези препоръки в срок от 90 дни след получаването им ([142]). Освен това в случай на неизпълнение на препоръките съответният орган трябва да информира Комисията за това ([143]). На свой ред НКПЧ може да оповести този пропуск пред Националното събрание и/или да го направи публично достояние. Публичните органи като цяло изпълняват препоръките на НКПЧ и имат силен стимул да го правят, тъй като тяхното изпълнение се преценява като част от общата оценка, извършвана от Службата за координация на политиката на правителството под ръководството на кабинета на министър-председателя.

2.4. **Средства за индивидуална правна защита**

2.4.1. *Механизми за правна защита, предвидени в ЗЗЛД*

Съгласно ЗЗЛД физическите лица могат да упражняват правото си на достъп, коригиране, заличаване и спиране на използването по отношение на личните данни, обработвани от органите за наказателно правоприлагане. Достъпът може да бъде поискан директно от съответния орган или косвено чрез КЗЛД ([144]). Компетентният орган може да ограничи или да откаже достъп само когато това се предвижда от закона, когато е вероятно да доведе до вредни последствия за живота или до телесно увреждане на трета страна, или до необосновано накърняване на имуществени и други интереси на друго лице (т.е. когато интересите на другото лице биха надделели над интересите на физическото лице, подало искането) ([145]). Ако искането за достъп бъде отхвърлено, физическото лице трябва да бъде информирано за причините за това и за начина на обжалване ([146]). По подобен начин искането за корекция или изтриване може да бъде отхвърлено, когато това е предвидено в други закони, като в този случай физическото лице трябва да бъде информирано за основните причини и за възможността за обжалване ([147]).

Що се отнася до средствата за защита, физическите лица могат да подадат жалба до КЗЛД, включително чрез Центъра за обаждания по въпросите на поверителността, управляван от Корейската агенция за интернет и сигурност ([148]). Освен това дадено физическо лице може да получи посредничество чрез Комитета за посредничество при спорове, свързани с личните данни ([149]). Тези средства за правна защита са налични както в случай на евентуални нарушения на правилата, съдържащи се в конкретни закони, определящи ограниченията и защитните мерки по отношение на събирането на лични данни (раздел 2.2), така и в ЗЗЛД. Освен това физическите лица могат да оспорват решенията или бездействието на КЗЛД по реда на Закона за административното съдопроизводство (вж. раздел 2.4.3).

([137]) Член 5, параграф 5 от Закона за НКПЧ.
([138]) Член 7, параграф 1 и член 8 от Закона за НКПЧ.
([139]) Член 10 от Закона за НКПЧ.
([140]) Член 36 от Закона за НКПЧ. В съответствие с член 36, параграф 7 от закона предоставянето на материали или статии може да бъде отказано, ако това би накърнило държавната тайна, което може да окаже съществено въздействие върху държавната сигурност или дипломатическите отношения, или би представлявало сериозна пречка за наказателно разследване или висящ съдебен процес. В такива случаи Комисията може да поиска допълнителна информация от ръководителя на съответния орган (който трябва да спазва добросъвестно изискванията), когато това е необходимо, за да провери дали отказът за предоставяне на информация е обоснован.
([141]) Член 25, параграф 1 от Закона за НКПЧ.
([142]) Член 25, параграф 3 от Закона за НКПЧ.
([143]) Член 25, параграф 4 от Закона за НКПЧ.
([144]) Член 35, параграф 2 от ЗЗЛД.
([145]) Член 35, параграф 4 от ЗЗЛД.
([146]) Член 42, параграф 2 от Указа за прилагане на ЗЗЛД.
([147]) Член 36, параграфи 1 и 2 от ЗЗЛД и член 43, параграф 3 от Указа за прилагане на ЗЗЛД.
([148]) Член 62 от ЗЗЛД.
([149]) Членове 40—50 от ЗЗЛД и членове 48-2—57 от Указа за прилагане на ЗЗЛД.

2.4.2. *Защита от Националната комисия по правата на човека*

НКПЧ разглежда жалби от физически лица (както корейски граждани, така и чужденци) относно нарушения на правата на човека, извършени от публичните органи ([150]). Физическите лица не са длъжни да подават жалби до НКПЧ ([151]). В резултат на това жалбата ще бъде разгледана от НКПЧ, дори ако засегнатото физическо лице не може да докаже реална вреда на етапа на допустимост. Следователно в контекста на събирането на лични данни за целите на наказателното правоприлагане от физическо лице не се изисква да докаже, че корейските публични органи действително са имали достъп до неговите лични данни, за да бъде жалбата му допустима пред НКПЧ. Физическо лице може също така да поиска жалбата да бъде решена чрез посредничество ([152]).

За да разследва дадена жалба, НКПЧ може да се възползва от правомощията си да провежда разследвания, включително като поиска предоставянето на съответните материали, като извършва проверки и призовава физически лица да дадат показания ([153]). Ако разследването разкрие, че е извършено нарушение на съответните закони, НКПЧ може да препоръча прилагането на средства за правна защита или коригирането или подобряването на съответния закон, политика, практика или организацията на институцията ([154]). Предложените средства за правна защита могат да включват посредничество, прекратяване на нарушаването на правата на човека, обезщетение за вреди и мерки за предотвратяване на повторното извършване на същите или подобни нарушения ([155]). В случай на незаконно събиране на лични данни в рамките на приложимите правила, корективните мерки могат да включват заличаване на събраните лични данни. Ако се прецени, че е много вероятно нарушението да продължава и че е вероятно, ако бъде оставено без внимание, да бъдат причинени трудно поправими вреди, НКПЧ може да приеме спешни мерки за облекчаване ([156]).

Въпреки че НКПЧ няма правомощия да налага задължения, нейните решения (напр. решение да не се продължава разследването на жалба) ([157]) и препоръки могат да бъдат оспорвани пред корейските съдилища съгласно Закона за административното съдопроизводство (вж. раздел 2.4.3 по-долу) ([158]). Освен това, ако констатациите на НКПЧ разкриват, че публичен орган е събрал незаконосъобразно лични данни, физическото лице може да потърси допълнителна правна защита от корейските съдилища срещу този публичен орган, напр. чрез оспорване на събирането съгласно Закона за административното съдопроизводство, подаване на конституционна жалба съгласно Закона за Конституционния съд или подаване на молба за обезщетение за вреди съгласно Закона за обезщетенията от държавата (вж. раздел 2.4.3 по-долу).

2.4.3. *Съдебна защита*

Физическите лица могат да се позоват на ограниченията и защитните мерки, описани в предходните раздели, за да получат правна защита от корейските съдилища по различни начини.

Първо, в съответствие с НПЗ засегнатото физическо лице и неговият/нейният адвокат може да присъства, когато се изпълнява заповед за претърсване или изземване, и съответно може да възрази по време на изпълнението на заповедта ([159]). Освен това в НПЗ е предвиден така наречения механизъм „квазижалба“, който позволява на физическите лица да подадат петиция до компетентния съд с искане за отмяна или промяна на разпореждане на прокурор или полицейски служител относно изземване ([160]). Това позволява на лицата да оспорват мерките, предприети за изпълнение на заповедта за изземване.

([150]) Въпреки че в член 4 от Закона за НКПЧ се говори за граждани и чужденци, пребиваващи в Република Корея, терминът „пребиваващи“ отразява по-скоро понятието за юрисдикция, отколкото за територия. Ето защо, ако основните права на чужденец извън Корея са нарушени от национални институции в Корея, това физическо лице може да подаде жалба до НКПЧ. Вж. например съответния въпрос на страницата на НКПЧ с често задавани въпроси, достъпна на адрес https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Такъв би бил случаят, ако личните данни на чужденец, предадени на Корея, са незаконно достъпни за корейските публични органи.

([151]) По принцип жалбата трябва да бъде подадена в рамките на една година от нарушението, но НКПЧ все пак може да реши да разследва жалба, която е подадена след този срок, стига да не е изтекъл давностният срок по наказателното или гражданското право (член 32, параграф 1, точка 4 от Закона за НКПЧ).

([152]) Член 42 и сл. от Закона за НКПЧ.

([153]) Членове 36 и 37 от Закона за НКПЧ.

([154]) Член 44 от Закона за НКПЧ.

([155]) Член 42, параграф 4 от Закона за НКПЧ.

([156]) Член 48 от Закона за НКПЧ.

([157]) Например, ако НКПЧ по изключение не е в състояние да провери определени материали или съоръжения, тъй като те се отнасят до държавни тайни, които могат да окажат съществено влияние върху държавната сигурност или дипломатическите отношения, или когато инспекцията би представлявала сериозна пречка за наказателно разследване или висящ съдебен процес (вж. бележка под линия 166), и когато това не позволява на НКПЧ да проведе разследването, необходимо за оценка на основателността на получената петиция, тя ще информира физическото лице за причините, поради които жалбата е била отхвърлена, в съответствие с член 39 от Закона за НКПЧ. В този случай физическото лице може да оспори решението на НКПЧ по реда на Закона за административното съдопроизводство.

([158]) Вж. например Решение 2007Nu27259 на Висшия съд на Сеул, 18 април 2008 г., потвърдено с Решение 2008Du7854 на Върховния съд, 9 октомври 2008 г.; Решение 2017Nu69382 на Висшия съд на Сеул, 2 февруари 2018 г.

([159]) Членове 121 и 219 от НПЗ.

([160]) Член 417 от НПЗ във връзка с член 414, параграф 2 от НПЗ. Вж. също Решение № 97Mo66 на Върховния съд, 29 септември 1997 г.

Освен това физическите лица могат да получат обезщетение за вреди пред корейските съдилища. Въз основа на Закона за обезщетенията от държавата физическите лица могат да предявяват иск за обезщетение за вреди, нанесени от длъжностни лица при изпълнение на служебните им задължения в нарушение на закона ([161]). Иск по Закона за обезщетенията от държавата може да бъде подаден до специализиран „Съвет по обезщетенията“ или директно до корейските съдилища ([162]). Ако жертвата е чужденец, Законът за обезщетенията от държавата се прилага, доколкото държавата по произход на лицето гарантира равностойно обезщетение от държавата за корейските граждани ([163]). Според съдебната практика това условие е изпълнено, ако изискванията за искане на обезщетение в другата държава „*не са в значителен дисбаланс между Корея и другата държава*“ и „*не са като цяло по-строги от тези, определени от Корея, без да има значителна и съществена разлика* ([164])." Гражданският закон урежда отговорността на държавата по отношение на обезщетенията и в резултат на това отговорността на държавата обхваща и неимуществени вреди (напр. душевни страдания) ([165]).

При нарушения на правилата за защита на личните данни са предвидени допълнителни средства за правна защита съгласно ЗЗЛД. Съгласно член 39 от ЗЗЛД всяко физическо лице, което е претърпяло вреди в резултат на нарушение на ЗЗЛД или на загуба, кражба, разкриване, фалшифициране, изменение или увреждане на неговите/нейните лични данни, може да получи обезщетение за вреди по съдебен ред. Не съществува подобно изискване за реципрочност, както при Закона за обезщетенията от държавата.

В допълнение към обезщетението за вреди то може да получи защита по административен път срещу действия или бездействия на административни органи съгласно Закона за административното съдопроизводство. Всяко лице може да оспори разпореждане (т.е. упражняването или отказа да се упражни публична власт в конкретен случай) или бездействие (продължителната неспособност на административен орган да се разпореди в противоречие със законовото задължение за това), което може да доведе до отмяна/изменение на незаконно разпореждане, установяване на нищожност (т.е. констатация, че разпореждането няма правно действие или че то не съществува в правния ред) или констатация, че бездействието е незаконно ([166]). За да може да се оспорва административно разпореждане, то трябва да оказва пряко въздействие върху гражданските права и задължения ([167]). Това включва мерки за събиране на лични данни, било то пряко (напр. прихващане на комуникации) или чрез искане за разкриване (напр. към доставчик на услуги).

Гореспоменатите искове могат да бъдат предявени първо пред комисиите за административно обжалване, създадени към някои публични органи (напр. към НРС, НКПЧ), или пред Централната комисия за административно обжалване, създадена към Комисията за борба с корупцията и гражданските права ([168]). Такова административно обжалване предоставя алтернативен, по-неформален начин за оспорване на разпореждане или бездействие на публичен орган. Въпреки това иск може да бъде предявен и директно пред корейските съдилища съгласно Закона за административното съдопроизводство.

Искане за отмяна/изменение на разпореждане съгласно Закона за административното съдопроизводство може да подаде всяко лице, което има правен интерес да иска отмяната/изменението или да му бъдат възстановени правата чрез отмяната/изменението, в случай че разпореждането вече няма действие ([169]). Аналогично, съдебен спор за потвърждаване на нищожност може да бъде заведен от лице, което има правен интерес от такова потвърждаване, докато съдебен спор за потвърждаване на незаконосъобразността на бездействие може да бъде заведен от всяко лице, което е представило искане за разпореждане и има правен интерес да иска потвърждаване на незаконосъобразността на бездействието ([170]). Съгласно съдебната практика на Върховния съд „правен интерес“ се тълкува като „правно защитен интерес“, т.е. пряк и конкретен интерес, защитен от закони и подзаконови актове, на които се основават административните разпореждания (т.е. не общи, косвени и абстрактни интереси на обществото) ([171]). Следователно физическите лица имат правен интерес в случай на нарушение на ограничения и защитни мерки по отношение на събирането на техните лични данни за целите на наказателното правоприлагане (съгласно специални закони или ЗЗЛД). Окончателното съдебно решение по Закона за административното съдопроизводство е задължително за страните ([172]).

Искането за отмяна/изменение на разпореждане и искането за потвърждаване на незаконосъобразността на бездействие трябва да бъдат подадени в срок от 90 дни от датата, на която физическото лице е узнало за разпореждането/бездействието, и по принцип не по-късно от една година от датата на издаване на разпореждането/настъпването на

([161]) Вж. член 2, параграф 1 от Закона за обезщетенията от държавата.

([162]) Членове 9 и 12 от Закона за обезщетенията от държавата. В закона се предвижда създаването на районни съвети (които се председателстват от заместник-прокурора на съответната прокуратура), Централен съвет (който се председателства от заместник-министъра на правосъдието) и Специален съвет (който се председателства от заместник-министъра на националната отбрана и отговаря за исковете за обезщетение за вреди, нанесени на военнослужещи или на цивилни служители на армията). Исканията за обезщетение за вреди по принцип се разглеждат от районните съвети, които при определени обстоятелства трябва да препратят случаите към Централния/Специалния съвет, например ако обезщетението надхвърля определена сума или в случай че дадено физическо лице иска повторно разглеждане. Всички съвети се състоят от членове, назначени от министъра на правосъдието (напр. държавни служители от Министерството на правосъдието, съдебни изпълнители, адвокати и лица с опит по въпросите на обезщетенията от държавата), които са длъжни да спазват конкретни правила във връзка с конфликтите на интереси (вж. член 7 от Указа за прилагане на Закона за обезщетенията от държавата).

([163]) Член 7 от Закона за обезщетенията от държавата.

([164]) Решение № 2013Da208388 на Върховния съд, 11 юни 2015 г.

([165]) Вж. член 8 от Закона за обезщетенията от държавата, както и член 751 от Гражданския закон.

([166]) Членове 2 и 4 от Закона за административното съдопроизводство.

([167]) Решение 98Du18435 на Върховния съд, 22 октомври 1999 г., Решение 99Du1113 на Върховния съд, 8 септември 2000 г., и Решение 2010Du3541 на Върховния съд, 27 септември 2012 г.

([168]) Член 6 от Закона за административните обжалвания и член 18, параграф 1 от Закона за административното съдопроизводство.

([169]) Член 12 от Закона за административното съдопроизводство.

([170]) Членове 35 и 36 от Закона за административното съдопроизводство.

([171]) Решение № 2006Du330 на Върховния съд, 26 март 2006 г.

([172]) Член 30, параграф 1 от Закона за административното съдопроизводство.

бездействието, освен ако няма основателни причини ([173]). Съгласно практиката на Върховния съд понятието „основателни причини“ трябва да се тълкува широко и изисква да се прецени дали е социално приемливо да се допусне закъсняла жалба с оглед на всички обстоятелства по делото ([174]). Това включва например (но не се ограничава до) причини за забавяне, за които съответната страна не може да бъде държана отговорна (т.е. ситуации, които са извън контрола на жалбоподателя, например когато той не е бил уведомен за събирането на неговите лични данни), или форсмажорни обстоятелства (напр. природно бедствие, война).

Накрая, физическите лица могат също така да подадат конституционна жалба до Конституционния съд ([175]). Въз основа на Закона за Конституционния съд всяко лице, чиито основни права, гарантирани от Конституцията, са нарушени поради упражняването или неупражняването на публична власт (с изключение на решенията на съдилищата), може да поиска разглеждане на конституционна жалба. Ако са налични други средства за правна защита, първо те трябва да бъдат изчерпани. Съгласно съдебната практика на Конституционния съд чужденците могат да подадат конституционна жалба, доколкото техните основни права са признати от Конституцията на Корея (вж. обясненията в раздел 1.1) ([176]). Конституционните жалби трябва да бъдат подавани в срок от 90 дни, след като физическото лице е узнало за нарушението, и в срок от една година след извършването му. Като се има предвид, че процедурата от Закона за административното съдопроизводство се прилага за съдебни спорове по Закона за Конституционния съд ([177]), жалбата все пак ще бъде допустима, ако са налице „основателни причини“, както се тълкуват в съответствие с описаната по-горе съдебна практика на Върховния съд.

Ако първо трябва да бъдат изчерпани други средства за правна защита, конституционната жалба трябва да бъде подадена в срок от 30 дни след окончателното решение по такова средство за правна защита ([178]). Конституционният съд може да обезсили упражняването на публична власт, което е довело до нарушението, или да потвърди, че определено бездействие е противоконституционно ([179]). В този случай съответният орган е длъжен да предприеме мерки за изпълнение на решението на Съда.

3. ДОСТЪП НА ДЪРЖАВНИТЕ ОРГАНИ ЗА ЦЕЛИТЕ НА НАЦИОНАЛНАТА СИГУРНОСТ

3.1. Компетентни публични органи в областта на националната сигурност

Република Корея разполага с две специализирани разузнавателни агенции: НРС и Командването за поддържане на сигурността в областта на отбраната. Освен това полицията и прокуратурата могат да събират лични данни и за целите на националната сигурност.

НРС е създадена със Закона за Националната разузнавателна служба (наричан по-нататък „*Закон за НРС*“) и работи пряко под юрисдикцията и надзора на президента ([180]). По-специално НРС събира, обобщава и разпространява данни за чужди държави (и Северна Корея) ([181]), разузнавателни сведения, свързани с противодействието на шпионажа (включително военния и промишления шпионаж), тероризма и дейността на международните престъпни синдикати, разузнавателни сведения за някои видове престъпления, насочени срещу обществената и националната сигурност (напр. вътрешни бунтове, чуждестранна агресия), и разузнавателни сведения, свързани с осигуряването на киберсигурността и предотвратяването или противодействието на кибератаки и заплахи ([182]). В Закона за НРС, с който се създава НРС и се определят нейните задачи, се съдържат също така общи принципи, които предоставят рамка за всички нейни дейности. Като общ принцип НРС трябва да поддържа политически неутралитет и да защитава свободата и правата на физическите лица ([183]). Председателят на НРС е натоварен с разработването на общи насоки, които определят принципите, обхвата и процедурите за изпълнение на задълженията на НРС във връзка със събирането и използването на информация, и трябва да ги докладва на Националното събрание ([184]). Националното събрание (чрез своя Комитет по разузнаването) може да поиска коригиране или допълване на насоките, ако прецени, че те са незаконни или несправедливи. В по-общ план, когато изпълняват задълженията си, директорът и служителите на НРС не могат да принуждават никоя институция, организация или физическо лице да направят нещо, което не са задължени да направят, нито да възпрепятстват упражняването на правата на което и да е лице, като злоупотребяват със служебното си положение ([185]). Освен това всяко цензуриране на поща, прихващане на телекомуникации, събиране на информация за местоположението, събиране на данни за потвърждаване на комуникациите или записване или подслушване на частни комуникации от страна на НРС

([173]) Член 20 от Закона за административното съдопроизводство. Този срок се прилага и за иск за потвърждаване на незаконосъобразността на бездействие, вж. член 38, параграф 2 от Закона за административното съдопроизводство.
([174]) Решение 90Nu6521 на Върховния съд, 28 юни 1991 г.
([175]) Член 68, параграф 1 от Закона за Конституционния съд.
([176]) Решение № 99HeonMa194 на Конституционния съд от 29 ноември 2001 г.
([177]) Член 40 от Закона за Конституционния съд.
([178]) Член 69 от Закона за Конституционния съд.
([179]) Член 75, параграф 3 от Закона за Конституционния съд.
([180]) Член 2 и член 4, параграф 2 от Закона за НРС.
([181]) Това понятие не обхваща информация за физическите лица, а обща информация за чуждите държави (тенденции, развития) и за дейността на държавните участници от трети държави.
([182]) Член 3, параграф 1 от Закона за НРС.
([183]) Член 3, параграф 1, член 6, параграф 2 и членове 11 и 21. Вж. също правилата за конфликт на интереси, по-специално членове 10 и 12.
([184]) Член 4, параграф 2 от Закона за НРС.
([185]) Член 13 от Закона за НРС.

трябва да е в съответствие със ЗЗНК, Закона за информацията за местоположението или НПЗ ([186]). Всяка злоупотреба с власт или събиране на информация в нарушение на тези закони подлежи на наказателни санкции ([187]).

Командването за поддържане на сигурността в областта на отбраната е военна разузнавателна агенция, създадена към Министерството на отбраната. Тя отговаря за въпросите на сигурността в рамките на армията, военните наказателни разследвания (съгласно Закона за военните съдилища) и военното разузнаване. По принцип Командването за поддържане на сигурността в областта на отбраната не извършва наблюдение на граждански лица, освен ако това е необходимо за изпълнение на военните му функции. Лицата, които могат да бъдат разследвани, са военнослужещи, граждански лица — служители в армията, лица, преминаващи военно обучение, лица от запаса или на наборна военна служба и военнопленници ([188]). Когато събира комуникационни данни за целите на националната сигурност, Командването за поддържане на сигурността в областта на отбраната се подчинява на ограниченията и защитните мерки, предвидени в ЗЗНК и в указа за неговото прилагане.

3.2. **Правни основания и ограничения**

В ЗЗНК, в Закона за борба с тероризма за защита на гражданите и обществената сигурност (наричан по-нататък „*Закон за борба с тероризма*“) и в ЗТД се предвиждат правни основания за събирането на лични данни за целите на националната сигурност и се определят приложимите ограничения и защитни мерки ([189]). Тези ограничения и защитни мерки, описани в следващите раздели, гарантират, че събирането и обработването на данни се ограничава до строго необходимото за постигане на законосъобразна цел. Това изключва масовото и безразборното събиране на лични данни за целите на националната сигурност.

3.2.1. *Събиране на комуникационни данни*

3.2.1.1. Събиране на комуникационни данни от разузнавателните агенции

3.2.1.1.1. Правно основание

В ЗЗНК се предоставят правомощия на разузнавателните агенции да събират комуникационни данни и се изисква от доставчиците на комуникационни услуги да съдействат по отношение на исканията от тези агенции ([190]). Както е описано в раздел 2.2.2.1, в ЗЗНК се прави разграничение между събирането на съдържанието на комуникациите (т.е. „*мерки за ограничаване на комуникациите*“, като например мерките „*подслушване*“ или „*цензура*“ ([191])) и събирането на „*данни за потвърждаване на комуникациите*“ ([192]).

Прагът за събиране на тези два вида информация е различен, но приложимите процедури и предпазни мерки са до голяма степен идентични ([193]). Събирането на данни за потвърждаване на комуникациите (или метаданни) може да се извършва с цел предотвратяване на заплахи за националната сигурност ([194]). По-висок праг се прилага за изпълнението на мерки за ограничаване на комуникациите (т.е. за събиране на съдържанието на комуникациите), които могат да бъдат предприети само когато се очаква националната сигурност да бъде изложена на сериозна опасност и събирането на разузнавателни сведения е необходимо за предотвратяването на такава опасност (т.е. ако съществува сериозен риск за националната сигурност и събирането на сведения е необходимо за предотвратяването му) ([195]). Освен това достъпът до съдържанието на комуникациите може да се осъществява само като крайна мярка за гарантиране на националната сигурност и трябва да се полагат усилия за свеждане до минимум на нарушенията в областта на неприкосновеността на комуникациите ([196]). Дори когато е получено съответното одобрение/разрешение, тези мерки трябва да бъдат преустановени незабавно, след като вече не са необходими, като по този начин се гарантира, че всяко нарушение на тайната на комуникацията на физическо лице е ограничено до минимум ([197]).

3.2.1.1.2. Ограничения и защитни мерки, приложими към събирането на комуникационни данни, свързани с поне един корейски гражданин

Събиране на комуникационни данни (както съдържание, така и метаданни), при което едното или двете лица, участващи в комуникацията, са корейски граждани, може да се извършва само с разрешение на старши

([186]) Член 14 от Закона за НРС.
([187]) Членове 22 и 23 от Закона за НРС.
([188]) Член 1 от Закона за военните съдилища.
([189]) При разследването на престъпления, свързани с националната сигурност, полицията и НРС действат въз основа на НПЗ, докато Командването за поддържане на сигурността в областта на отбраната се подчинява на Закона за военните съдилища.
([190]) Член 15-2 от ЗЗНК.
([191]) Член 2, параграфи 6 и 7 от ЗЗНК.
([192]) Член 2, параграф 11 от ЗЗНК.
([193]) Вж. също член 13-4, параграф 2 от ЗЗНК и член 37, параграф 4 от Указа за прилагане на ЗЗНК, в които се посочва, че процедурите, приложими към събирането на съдържанието на комуникациите, се прилагат mutatis mutandis към събирането на данни за потвърждаване на комуникациите.
([194]) Член 13-4 от ЗЗНК.
([195]) Член 7, параграф 1 от ЗЗНК.
([196]) Член 3, параграф 2 от ЗЗНК.
([197]) Член 2 от Указа за прилагане на ЗЗНК.

съдия от Висшия съд ([198]). Искането от разузнавателната агенция трябва да бъде отправено в писмен вид до прокурор или до Върховна прокуратура ([199]). В него трябва да се посочат причините за събирането (т.е. че се очаква националната сигурност да бъде изложена на сериозна опасност или че събирането е необходимо за предотвратяване на заплахи за националната сигурност), заедно с материалите, подкрепящи тези причини и установяващи вероятната основателност на иска, както и подробностите по искането (т.е. целите, засегнатото(ите) физическо(и) лице(а), обхватът, срокът на действие на събирането, както и как и къде ще се извършва събирането) ([200]). Прокурорът/Висшата прокуратура на свой ред иска разрешение от старши съдия на Висшия съд ([201]). Председателят на Върховния съд може да даде писмено разрешение само когато смята молбата за основателна, и ще отхвърли искането, когато го смята за неоснователно ([202]). В заповедта се посочват видът, целта, предметът, обхватът и срокът на действие на събирането, както и мястото и начинът на провеждането му ([203]).

Специални правила се прилагат, в случай че мярката е насочена към разследване на заговор, който застрашава националната сигурност, и е налице извънредна ситуация, която прави невъзможно провеждането на гореспоменатите процедури ([204]). Когато са изпълнени тези условия, разузнавателните агенции могат да осъществяват мерки по наблюдение без предварителното одобрение на съда ([205]). Веднага след изпълнението на спешните мерки обаче разузнавателната агенция трябва да поиска разрешение от съда. Ако разрешението не бъде получено в рамките на 36 часа от предприемането на мерките, те трябва да бъдат преустановени незабавно ([206]). Събирането на информация при извънредни ситуации винаги трябва да се извършва в съответствие с „изявление за извънредна цензура/извънредно подслушване“, а разузнавателната агенция, която извършва събирането, трябва да води регистър за всяка спешна мярка ([207]).

В случаите, когато наблюдението приключва в кратък срок, при отсъствие на разрешение от съда, ръководителят на компетентната Върховна прокуратура трябва да изпрати уведомление за извънредна мярка, изготвено от разузнавателната агенция, до ръководителя на компетентния съд, който съхранява регистъра на извънредните мерки ([208]). Това позволява на съда да проучва законосъобразността на събирането.

3.2.1.1.3. Ограничения и защитни мерки, приложими към събирането на комуникационни данни, свързани само с лица, които не са корейски граждани

За да събират информация за комуникации, водени изключително между лица, които не са корейски граждани, разузнавателните агенции трябва да получат предварително писмено одобрение от президента ([209]). Такива комуникации ще бъдат събирани за целите на националната сигурност само ако попадат в една от няколкото изброени категории, т.е. комуникации между висши държавни служители или други физически лица от враждебни на Република Корея държави, чуждестранни агенции, групи или граждани, заподозрени в участие в дейности срещу Корея ([210]), или членове на групи в рамките на Корейския полуостров, които ефективно са извън суверенитета на Република Корея, и групи под тяхната „шапка“, базирани в чужди държави ([211]). Обратно, ако едната страна в комуникацията е корейски гражданин, а другата — лице, което не е корейски гражданин, се изисква съдебно разрешение в съответствие с процедурата, описана в раздел 3.2.1.1.2.

Ръководителят на разузнавателна агенция трябва да представи на директора на НРС план за мерките, които се предвижда да бъдат предприети ([212]). Директорът на НРС проверява дали планът е подходящ, и ако това е така, го представя за одобрение на президента ([213]). Информацията, която трябва да бъде включена в плана, е същата като информацията, която се изисква за молба за съдебно разрешение за събиране на информация за корейски граждани (както е описано по-горе) ([214]). По конкретно в него трябва да се посочат причините за събирането (т.е. че се очаква националната сигурност да бъде изложена на сериозна опасност или че събирането е необходимо за предотвратяване на заплахи за

([198]) Член 7, параграф 1, точка 1 от ЗЗНК. Компетентният съд е висшият съд, който има юрисдикция по местожителството или седалището на едната или двете страни, подлежащи на наблюдение.
([199]) Член 7, параграф 3 от Указа за прилагане на ЗЗНК.
([200]) Член 7, параграф 3 и член 6, параграф 4 от ЗЗНК.
([201]) Член 7, параграф 4 от Указа за прилагане на ЗЗНК. В искането на прокурора до съда трябва да се посочат основните основания за подозрение, и доколкото се искат няколко разрешения едновременно — обосновката за това (вж. член 4 от Указа за прилагане на ЗЗНК).
([202]) Член 7, параграф 3 и член 6, параграфи 5 и 9 от ЗЗНК.
([203]) Член 7, параграф 3 и член 6, параграф 6 от ЗЗНК.
([204]) Член 8 от ЗЗНК.
([205]) Член 8, параграф 1 от ЗЗНК.
([206]) Член 8, параграф 2 от ЗЗНК.
([207]) Член 8, параграф 4 от ЗЗНК. Вж. по-горе раздел 2.2.2.2. за спешни мерки в контекста на правоприлагането.
([208]) Член 8, параграфи 5 и 7 от ЗЗНК. В уведомлението трябва да се посочат целта, предметът, обхватът, периодът, мястото на изпълнение и начинът на наблюдение, както и основанията за неподаване на искане за разрешение от съда преди предприемането на мярката (член 8, параграф 6 от ЗЗНК).
([209]) Член 7, параграф 1, точка 2 от ЗЗНК.
([210]) Става дума за дейности, които застрашават съществуването и сигурността на нацията, демократичния ред или оцеляването и свободата на хората.
([211]) Освен това, ако едната страна е лице, описано в член 7, параграф 1, точка 2 от ЗЗНК, а другата е неизвестна или не може да бъде посочена, се прилага процедурата, предвидена в член 7, параграф 1, точка 2.
([212]) Член 8, параграф 1 от Указа за прилагане на ЗЗНК. Директорът на НРС се назначава от президента след утвърждаване от парламента (член 7 от Закона за НРС).
([213]) Член 8, параграф 2 от Указа за прилагане на ЗЗНК.
([214]) Член 8, параграф 3 от Указа за прилагане на ЗЗНК, във връзка с член 6, параграф 4 от ЗЗНК.

националната сигурност), съществените основания за подозрението, както и материалите, подкрепящи тези основания и установяващи вероятната основателност на иска, както и подробностите по искането (т.е. целите, засегнатото(ите) физическо(и) лице(а), обхватът, срокът на действие на събирането, както и как и къде ще се извърши събирането). Когато са поискани няколко разрешения едновременно — целта и основанията за тях ([215]).

При извънредни ситуации ([216]) трябва да се получи предварително одобрение от министъра, към когото спада съответната разузнавателна агенция. В този случай обаче разузнавателната агенция трябва да поиска одобрението на президента незабавно след предприемането на спешните мерки. Ако разузнавателната агенция не успее да получи одобрение в рамките на 36 часа от подаването на молбата, събирането трябва да бъде преустановено незабавно ([217]). В тези случаи събраната информация винаги се унищожава.

3.2.1.1.4. Общи ограничения и защитни мерки

Когато искат съдействие от частни субекти, разузнавателните агенции трябва да им представят съдебната заповед/разрешението на президента или копие от заглавната страница на изявление за спешна цензура, което принуденият да съдейства субект трябва да съхранява в досието си ([218]). Субектите, от които е поискано да разкрият информация на разузнавателните агенции въз основа на ЗЗНК, могат да откажат да го направят, когато разрешението или изявлението за извънредна цензура се отнасят до грешен идентификатор (напр. телефонен номер, принадлежащ на лице, различно от идентифицираното). Освен това във всички случаи паролите, използвани за комуникация, не могат да бъдат разкривани ([219]).

Разузнавателните служби могат да възложат прилагането на мерки за ограничаване на комуникациите или за събиране на данни за потвърждаване на комуникациите на пощенска служба или на доставчик на телекомуникационни услуги (съгласно определението в Закона за телекомуникационните дейности) ([220]). Съответната разузнавателна агенция и доставчикът, който получава искане за сътрудничество, трябва да съхраняват в продължение на три години регистри, в които се посочват целта на искането на мерки, датата на изпълнение или сътрудничество и обектът на мерките (напр. поща, телефон, електронна поща) ([221]). Доставчиците на телекомуникационни услуги, които предоставят данни за потвърждаване на комуникациите, трябва да съхраняват в своите досиета в продължение на седем години информация за честотата на събиране и да докладват два пъти годишно на министъра на науката и ИКТ ([222]).

Разузнавателните агенции трябва да докладват на директора на НРС за събраната от тях информация и за резултатите от наблюдението ([223]). По отношение на събирането на данни за потвърждаване на комуникациите трябва да се поддържа регистър относно факта, че е отправено искане за тези данни, както и самото писмено искане и институцията, която се е позовала на него ([224]).

Събирането на съдържанието на комуникациите и на данните за потвърждаване на комуникациите може да продължи за максимален период от четири месеца и трябва да бъде преустановено веднага, ако преследваната цел бъде постигната по-рано ([225]). Ако условията за издаване на разрешение продължават да съществуват, срокът може да бъде удължен с не повече от четири месеца с разрешение на съда или с одобрението на президента. Заявлението за получаване на одобрение за удължаване на срока на действие на мерките за наблюдение трябва да бъде подадено в писмен вид, като се посочват причините, поради които се иска удължаване, и се предоставят подкрепящи материали ([226]).

В зависимост от правното основание за събирането, физическите лица обикновено се уведомяват, когато се събират техните комуникации. По-специално, независимо от това дали събраната информация се отнася до съдържанието на комуникациите, или до данните за потвърждаване на комуникациите и независимо от това дали информацията е получена чрез обикновената процедура или при извънредна ситуация, ръководителят на разузнавателната агенция трябва да уведоми писмено засегнатото физическо лице за мярката за наблюдение в срок от 30 дни от датата, на която е приключило наблюдението ([227]). Уведомлението трябва да включва 1) факта, че информацията е събрана,

([215]) Член 8, параграфи 3 и 4 от Указа за прилагане на ЗЗНК.
([216]) Това означава, че в случаите, когато мярката е насочена към конспиративен акт, който застрашава националната сигурност, няма достатъчно време за получаване на одобрение от президента и неприемането на спешни мерки може да навреди на националната сигурност (член 8, параграф 8 от ЗЗНК).
([217]) Член 8, параграф 9 от ЗЗНК.
([218]) Член 9, параграф 2 от ЗЗНК и член 12 от Указа за прилагане на ЗЗНК.
([219]) Член 9, параграф 4 от ЗЗНК.
([220]) Член 13 от Указа за прилагане на ЗЗНК.
([221]) Член 9, параграф 3 от ЗЗНК и член 17, параграф 2 от Указа за прилагане на ЗЗНК. Този срок не се прилага за данните за потвърждаване на комуникациите (вж. член 39 от Указа за прилагане на ЗЗНК).
([222]) Член 13, параграф 7 от ЗЗНК и член 39 от Указа за прилагане на ЗЗНК.
([223]) Член 18, параграф 3 от Указа за прилагане на ЗЗНК.
([224]) Член 13, параграф 5 и член 13-4, параграф 3 от ЗЗНК.
([225]) Член 7, параграф 2 от ЗЗНК.
([226]) Член 7, параграф 2 от ЗЗНК и член 5 от Указа за прилагане на ЗЗНК.
([227]) Член 9-2, параграф 3 от ЗЗНК. В съответствие с член 13-4 от ЗЗНК това се отнася както за събирането на съдържанието на комуникациите, така и за събирането на данни за потвърждаване на комуникациите.

2) изпълнителния орган и 3) периода на изпълнение. Ако обаче има вероятност официалното уведомление да застраши националната сигурност или би имало вредни последствия за живота и физическата безопасност на хората, официалното уведомление може да бъде отсрочено ([228]). Уведомлението трябва да бъде изпратено в срок от 30 дни, след като основанията за отсрочване престанат да съществуват ([229]).

Това изискване за уведомление обаче се отнася само за събирането на информация, когато поне една от страните е корейски гражданин. В резултат на това лицата, които не са корейски граждани ще бъдат уведомявани само когато се събират техни комуникации с корейски граждани. Следователно няма изискване за уведомление, когато се събират комуникации изключително между лица, които не са корейски граждани.

Съдържанието на всички комуникации, както и данните за потвърждаване на комуникациите, придобити чрез наблюдение въз основа на ЗЗНК, могат да се използват само 1) за разследване, наказателно преследване или предотвратяване на определени престъпления, 2) за дисциплинарни производства, 3) за съдебни производства, при които страна, свързана с комуникацията, се позовава на тях по граждански иск за вреди или 4) въз основа на други закони ([230]).

3.2.1.2. Събиране на комуникационни данни от полицията/прокуратурата за целите на националната сигурност

Полицията/прокурор могат да събират комуникационни данни (както съдържанието на комуникациите, така и данни за потвърждаване на комуникациите) за целите на националната сигурност при същите условия, както са описани в раздел 3.2.1.1. Когато се действа в извънредни ситуации ([231]), приложимата процедура е тази, която беше описана по-рано по отношение на събирането на съдържанието на комуникациите за целите на правоприлагането в извънредни ситуации (т.е. член 8 от ЗЗНК).

3.2.2. *Събиране на информация за заподозрени в тероризъм лица*

3.2.2.1. Правно основание

В Закона за борба с тероризма се оправомощава директорът на НРС да събира информация за заподозрени в тероризъм лица ([232]). „*Заподозряно в тероризъм лице*“ се определя като член на терористична група ([233]), лице, което насърчава терористична група (чрез популяризиране и разпространение на идеи или тактики на терористична група), събира или предоставя средства за тероризъм ([234]) или участва в други дейности по подготовка, заговор, пропагандиране или подстрекаване към тероризъм, или лице, за което има основателни причини да бъде подозирано, че е извършвало такива дейности ([235]). По принцип всеки публичен служител, който прилага Закона за борба с тероризма, трябва да спазва основните права, залегнали в корейската конституция ([236]).

В самия Закон за борба с тероризма не се определят конкретни правомощия, ограничения и защитни мерки за събирането на информация за заподозрени в тероризъм лица, а по-скоро се препраща към процедурите в други закони. Първо, въз основа на Закона за борба с тероризма директорът на НРС може да събира 1) информация за влизането в Република Корея и излизането от нея, 2) информация за операции с финансови средства и 3) информация за комуникациите. В зависимост от вида на търсената информация съответните процедурни правила са предвидени съответно в Закона за имиграцията и Закона за митниците, ЗДИКИФС или ЗЗНК ([237]). За събирането на информация за влизането в Република Корея и за излизането от нея в Закона за борба с тероризма се прави препратка към процедурите, предвидени в Закона за

([228]) Член 9-2, параграф 4 от ЗЗНК.
([229]) Член 13-4, параграф 2 и член 9-2, параграф 6 от ЗЗНК.
([230]) Член 5, параграфи 1 и 2, член 12 и член 13-5 от ЗЗНК.
([231]) Тоест, когато мярката е насочена към конспиративен акт, който застрашава националната сигурност, и съществува извънредна ситуация, която прави невъзможно преминаването през обикновената процедура за одобрение (член 8, параграф 1 от ЗЗНК).
([232]) Член 9 от Закона за борба с тероризма.
([233]) „*Терористична група*“ се определя като група от терористи, посочена от Организацията на обединените нации (член 2, параграф 2 от Закона за борба с тероризма).
([234]) „*Тероризъм*“ се определя в член 2, параграф 1 от Закона за борба с тероризма като действие, извършено с цел да се попречи на упражняването на властта на държавата, на орган на местното самоуправление или на чуждо правителство (включително на органите на местното самоуправление и на международните организации) или с цел да ги принуди да предприемат действия, които не са задължителни за тях или са заплаха за обществото. Това включва а) убийство на човек или създаване на опасност за живота на човек чрез причиняване на телесна повреда или арестуване, задържане, отвличане или вземане на човек за заложник; б) определени видове действия, насочени към въздухоплавателно средство (напр. разбиване, отвличане или повреждане на въздухоплавателно средство по време на полет); в) определени видове действия, свързани с кораб (напр. завземане на кораб или морска конструкция в експлоатация, разрушаване на кораб или морска конструкция в експлоатация или нанасяне на вреди по тях до степен, която застрашава тяхната безопасност, включително повреждане на товара, натоварен на кораб или на морска конструкция в експлоатация); г) поставяне, детониране или използване по какъвто и да е друг начин на биохимично, взривно или запалително оръжие или устройство с цел причиняване на смърт, тежки наранявания или сериозни материални вреди или с такова въздействие върху определени типове превозни средства или съоръжения (напр. влакове, трамваи, моторни превозни средства, обществени паркове и гари, съоръжения за доставка на електроенергия, газ и телекомуникации и др.); д) определени видове действия, свързани с ядрени материали, радиоактивни материали или ядрени съоръжения (напр. вредни последствия за човешкия живот, телесни увреждания или увреждане на имущество или нарушаване на обществената безопасност по друг начин чрез разрушаване на ядрен реактор или неправомерно манипулиране с радиоактивни материали и др.).
([235]) Член 2, параграф 3 от Закона за борба с тероризма.
([236]) Член 3, параграф 3 от Закона за борба с тероризма.
([237]) Член 9, параграф 1 от Закона за борба с тероризма.

имиграцията и Закона за митниците. Понастоящем обаче в тези закони не се предвиждат такива правомощия. Що се отнася до събирането на комуникационни данни и информация за финансови сделки, в Закона за борба с тероризма се прави препратка към ограниченията и защитните мерки в ЗЗНК (които са описани по-подробно по-долу) и ЗДИКИФС (който, както е обяснено в раздел 2.1, не е от значение за целите на оценката на решението относно адекватното ниво на защита).

Освен това в член 9, параграф 3 от Закона за борба с тероризма се посочва, че директорът на НРС може да поиска лични данни или информация за местонахождението на заподозряно в тероризъм лице от администратор на лични данни ([238]) или от доставчик на информация за местоположението ([239]). Тази възможност е ограничена до искания за доброволно разкриване, на които администраторите на лични данни и доставчиците на информация за местоположението не са длъжни да отговарят, и във всеки случай могат да го правят само в съответствие със ЗЗЛД и Закона за информацията за местоположението (вж. раздел 3.2.2.2 по-долу).

3.2.2.2. Ограничения и защитни мерки, приложими към доброволното разкриване съгласно ЗЗЛД и Закона за информацията за местоположението

Исканията за доброволно сътрудничество съгласно Закона за борба с тероризма трябва да бъдат ограничени до информация за заподозрени в тероризъм лица (вж. по-горе раздел 3.2.2.1). Всяко такова искане от страна на НРС трябва да отговаря на принципите на законност, необходимост и пропорционалност, произтичащи от Конституцията на Корея (член 12, параграф 1 и член 37, параграф 2) ([240]), както и на изискванията на ЗЗЛД за събиране на лични данни (член 3, параграф 1 от ЗЗЛД, вж. по-горе раздел 1.2). Освен това в Закона за НРС се прави уточнение, че НРС не може да принуждава никоя институция, организация или физическо лице да прави нещо, което не е длъжно да прави, нито да възпрепятства упражняването на правата на което и да е лице, като злоупотребява с официалните си правомощия ([241]). Нарушаването на тази забрана може да подлежи на наказателна санкция ([242]).

Администраторите на лични данни и доставчиците на информация за местоположението, които получават искания от НРС въз основа на Закона за борба с тероризма, не са длъжни да ги изпълняват. Те могат да ги изпълняват доброволно, но им е позволено да го правят само в съответствие със ЗЗЛД и Закона за информацията за местоположението. Що се отнася до спазването на ЗЗЛД, администраторът трябва по-специално да вземе предвид интересите на субекта на данни и може да не разкрива данните, ако има вероятност това да наруши несправедливо интересите на физическото лице или на трета страна ([243]). Освен това, в съответствие с Уведомление № 2021-1 относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни, засегнатото физическо лице трябва да бъде уведомено за разкриването. В изключителни ситуации такова уведомление може да бъде отложено, по-специално ако и доколкото уведомлението би застрашило текущо наказателно разследване или има вероятност да окаже вредни последствия върху живота или тялото на друго лице, когато тези права или интереси са очевидно по-висши от правата на субекта на данни ([244]).

3.2.2.3. Ограничения и защитни мерки съгласно ЗЗНК

Въз основа на Закона за борба с тероризма разузнавателните агенции могат да събират комуникационни данни (както съдържанието на комуникациите, така и данни за потвърждаване на комуникациите) само когато това е необходимо за антитерористични дейности, т.е. дейности, свързани с предотвратяването и противодействието на тероризма. Процедурите по ЗЗНК, описани в раздел 3.2.1, се прилагат по отношение на събирането на комуникационни данни за целите на борбата с тероризма.

3.2.3. *Доброволно разкриване от оператори на телекомуникационни дейности*

Въз основа на ЗТД операторите на телекомуникационни дейности могат да изпълнят искане за разкриване на „комуникационни данни“, отправено от разузнавателна агенция, която възнамерява да събере информацията, за да предотврати заплаха за националната сигурност ([245]). Всяко такова искане трябва да отговаря на принципите на законност, необходимост и пропорционалност, произтичащи от Конституцията на Корея (член 12, параграф 1 и член 37, параграф 2) ([246]), както и на изискванията на ЗЗЛД за събиране на лични данни (член 3, параграф 1 от ЗЗЛД, вж. по-горе раздел 1.2). Освен това се прилагат същите ограничения и защитни мерки, както по отношение на доброволното разкриване за целите на правоприлагането (вж. раздел 2.2.3) ([247]).

([238]) Съгласно определението в член 2 от Закона за защита на личните данни, т.е. публична институция, юридическо лице, организация, физическо лице и др., които обработват пряко или непряко лични данни, за да използват файловете с лични данни за официални или бизнес цели.

([239]) Съгласно определението в член 5 от Закона за защита, използване и пр. на информация за местоположението (наричан по-нататък „Закон за информацията за местоположението“), т.е. всеки, който е получил разрешение от Корейската комисия по комуникациите да участва в бизнес с информация за местоположението.

([240]) Вж. също член 3, параграфи 2 и 3 от Закона за борба с тероризма.

([241]) Член 11, параграф 1 от Закона за НРС.

([242]) Член 19 от Закона за НРС.

([243]) Член 18, параграф 2 от ЗЗЛД.

([244]) Уведомление № 2021-1 на КЗЛД относно допълнителните правила за тълкуването и прилагането на Закона за защита на личните данни, раздел III, глава 2, точка iii).

([245]) Член 83, параграф 3 от ЗТД.

([246]) Вж. също член 3, параграфи 2 и 3 от Закона за борба с тероризма.

([247]) По-специално искането трябва да бъде в писмена форма и да съдържа информация за причините за искането, както и за връзката със съответния потребител и обхвата на исканата информация, а доставчикът на телекомуникационни услуги трябва да поддържа регистър и да докладва на министъра на науката и ИКТ два пъти годишно.

Операторите на телекомуникационни дейности не са задължени да спазват изискванията, но могат да го направят доброволно и само в съответствие с ЗЗЛД. В това отношение за операторите на телекомуникационни дейности важат същите задължения, включително по отношение на уведомяването на физическото лице, като при получаването на искания от органи за наказателно правоприлагане, както е обяснено по-подробно в раздел 2.2.3.

3.3. **Надзор**

Различни органи упражняват надзор върху дейността на корейските разузнавателни агенции. Надзорът върху Командването за поддържане на сигурността в областта на отбраната се осъществява от Министерство на националната отбрана в съответствие с Директивата на министерството за въвеждане на вътрешен одит. НРС подлежи на надзор от страна на изпълнителната власт, Националното събрание и други независими органи, както е обяснено по-подробно по-долу.

3.3.1. *Служител по защита на правата на човека*

Когато разузнавателните агенции събират информация за заподозрени в тероризъм лица, в Закона за борба с тероризма се предвижда надзор от страна на Комисията за борба с тероризма и от служителя по защита на правата на човека (наричан по-нататък „СЗПЧ“) ([248]).

Комисията за борба с тероризма, inter alia, разработва политики относно дейностите за борба с тероризма и наблюдава изпълнението на антитерористичните дейности, както и дейностите на различните компетентни органи в областта на борбата с тероризма ([249]). Комисията се председателства от министър-председателя и включва няколко министри и ръководители на правителствени агенции, включително министъра на външните работи, министъра на правосъдието, министъра на националната отбрана, министъра на вътрешните работи и сигурността, директора на НРС, генералния комисар на национална служба „Полиция“ и председателя на Комисията по финансови услуги ([250]). При провеждане на антитерористични разследвания и проследяване на заподозрени в тероризъм лица с цел събиране на информация или материали, необходими за антитерористични дейности, директорът на НРС трябва да докладва на председателя на Комисията за борба с тероризма (т.е. на министър-председателя) ([251]).

Освен това със Закона за борбата с тероризма се определя служител за защита на правата на човека (СЗПЧ), за да се защитят основните права на физическите лица срещу нарушения, причинени от дейности за борба с тероризма ([252]). Служителят по защита на правата на човека се назначава от председателя на Комисията за борба с тероризма измежду физически лица, които притежават квалификациите, посочени в Указа за прилагане на Закона за борба с тероризма (т.е. всеки, който има квалификация на адвокат с най-малко десет години професионален опит или експертни познания в областта на човешките права и който е заемал или заема (поне) длъжността доцент за най-малко десет години или е работил като висш държавен служител в държавни агенции или в органи на местното самоуправление, или който има поне десет години професионален опит в областта на човешките права, например в неправителствена организация) ([253]). СЗПЧ се назначава за две години (с възможност за подновяване на мандата) и може да бъде отстранен от длъжност само на конкретни, ограничени основания и при наличие на основателна причина, например при повдигане на обвинение по наказателно дело, свързано със задълженията му, при разкриване на поверителна информация или поради продължителна умствена или физическа неспособност ([254]).

Що се отнася до правомощията, СПЧО може да издава препоръки за подобряване на защитата на правата на човека от страна на агенциите, участващи в антитерористични дейности, и да разглежда граждански петиции (вж. раздел 3.4.3) ([255]). Когато може основателно да се установи наличието на нарушение на правата на човека при изпълнение на служебните задължения, СЗПЧ може да препоръча на ръководителя на отговорната агенция да отстрани това нарушение ([256]). На свой ред отговорната агенция трябва да уведоми СЗПЧ за предприетите действия за изпълнение на тази препоръка ([257]). Ако дадена агенция не изпълни препоръка на СЗПЧ, въпросът се отнася до Комисията, включително до нейния председател — министър-председателя. Досега не е имало случаи, в които препоръките на СЗПЧ да не са били изпълнени.

3.3.2. *Националното събрание:*

Както е описано в раздел 2.3.2, Националното събрание може да разследва и инспектира публични органи и в този контекст да изисква разкриването на документи и задължителното явяване на свидетели. По отношение на въпросите, попадащи в компетентността на НРС, този парламентарен надзор се осъществява от Комитета по разузнаване към Националното събрание ([258]). Директорът на НРС, който следи за изпълнението на задълженията на агенцията, се

([248]) Член 7 от Закона за борба с тероризма.
([249]) Член 5, параграф 3 от Закона за борба с тероризма.
([250]) Член 3, параграф 1 от Указа на прилагане на Закона за борба с тероризма.
([251]) Член 9, параграф 4 от Закона за борба с тероризма.
([252]) Член 7 от Закона за борба с тероризма.
([253]) Член 7, параграф 1 от Указа за прилагане на Закона за борба с тероризма.
([254]) Член 7, параграф 3 от Указа за прилагане на Закона за борба с тероризма.
([255]) Член 8, параграф 1 от Указа за прилагане на Закона за борба с тероризма.
([256]) Член 9, параграф 1 от Указа за прилагане на Закона за борба с тероризма. Служителят по защита на правата на човека взема самостоятелни решения за даване на препоръки, но трябва да докладва за тях на председателя на Комисията за борба с тероризма.
([257]) Член 9, параграф 2 от Указа за прилагане на Закона за борба с тероризма.
([258]) Член 36 и член 37, параграф 1, точка 16 от Закона за Националното събрание.

отчита пред Комитета по разузнаване (както и пред президента) ([259]). Самият Комитет по разузнаване също може да поиска доклад по конкретен въпрос, на който директорът на НРС е длъжен да отговори незабавно ([260]). Директорът може да откаже да отговори или да даде показания пред Комитета по разузнаване само по отношение на държавни тайни, касаещи военни, дипломатически или севернокорейски въпроси, когато публичното им оповестяване може да има сериозно въздействие върху съдбата на нацията ([261]). В този случай Комитетът по разузнаването може да поиска обяснение от министър-председателя. Ако такова обяснение не бъде представено в срок от седем дни от подаване на искането, отговорът или показанията вече не могат да бъдат отказани.

Ако Националното събрание установи незаконосъобразна или неправилна дейност, то може да поиска от съответния публичен орган да предприеме корективни мерки, включително присъждане на обезщетение за вреди, предприемане на дисциплинарно наказание и подобряване на вътрешните процедури ([262]). След такова искане органът трябва да предприеме незабавни действия и да докладва резултата на Националното събрание. Съществуват специални правила относно парламентарния надзор по отношение на използването на мерки за ограничаване на комуникациите (т.е. събиране на съдържанието на комуникациите) съгласно ЗЗНК ([263]). Що се отнася до последното, Националното събрание може да поиска от ръководителите на разузнавателните агенции да докладват за всяка конкретна мярка за ограничаване на комуникациите. Освен това то може да извършва проверки на място на оборудването за подслушване. Накрая, разузнавателните агенции, които са събрали, и операторите, които са разкрили информация за съдържанието за целите на националната сигурност, трябва да докладват за това разкриване при поискване от Националното събрание.

3.3.3. *Съвет за одити и инспекции*

По отношение на разузнавателните агенции СОИ изпълнява същите надзорни функции, както в областта на наказателното правоприлагане (вж. раздел 2.3.2) ([264]).

3.3.4. *Комисия за защита на личните данни*

Що се отнася до обработването на данни за целите на националната сигурност, включително на етапа на събиране, допълнителният надзор се осъществява от Комисията по защита на личните данни. Както е обяснено по-подробно в раздел 1.2, това включва общите принципи и задължения, изложени в член 3 и член 58, параграф 4 от ЗЗЛД, както и упражняването на индивидуалните права, гарантирани в член 4 от ЗЗЛД. Освен това съгласно член 7-8, параграфи 3 и 4 и член 7-9, параграф 5 от ЗЗЛД надзорът на КЗЛД обхваща и евентуални нарушения на правилата, съдържащи се в специалните закони, определящи ограниченията и защитните мерки по отношение на събирането на лични данни, като например ЗЗЛД, Закона за борба с тероризма и ЗТД. Като се имат предвид изискванията по член 3, параграф 1 от ЗЗЛД за законосъобразно и справедливо събиране на лични данни, всяко нарушение на тези закони представлява нарушение на ЗЗЛД. По този начин КЗЛД има правомощията да разследва ([265]) нарушения на законите, уреждащи достъпа до данни за целите на националната сигурност, както и на правилата за обработване съгласно ЗЗЛД, и да дава съвети за подобрение, да налага корективни мерки, да препоръчва дисциплинарно наказание и да предава потенциални престъпления на съответните разследващи органи ([266]).

3.3.5. *Национална комисия по правата на човека*

Надзорът от страна на НКПЧ се прилага по същия начин за разузнавателните агенции, както и за другите държавни органи (вж. раздел 2.3.2).

3.4. **Средства за индивидуална правна защита**

3.4.1. *Правна защита от служителя по защита на правата на човека*

Що се отнася до събирането на лични данни в контекста на дейностите за борба с тероризма, специална възможност за правна защита се предоставя от служителя по защита на правата на човека, назначен от Комисията за борба с тероризма. Служителят за защита на правата на човека се занимава с граждански петиции, свързани с нарушаване на правата на човека вследствие на дейности за борба с тероризма ([267]). Той/тя може да препоръча корективни действия и съответната агенция трябва да докладва на служителя за всички мерки, предприети за изпълнение на тази препоръка. Физическите лица не са длъжни да подават жалби до СЗПЧ. В резултат на това жалбата ще бъде разгледана от СЗПЧ, дори ако засегнатото физическо лице не може да докаже фактическа вреда на етапа на допустимост.

([259]) Член 18 от Закона за НРС.
([260]) Член 15, параграф 2 от Закона за НРС.
([261]) Член 17, параграф 2 от Закона за НРС. „Държавна тайна“ се определя като *„факти, стоки или знания, класифицирани като държавна тайна, достъпът до които е разрешен на ограничен кръг лица, и които не могат да бъдат разкривани на никоя друга държава или организация, за да се избегнат сериозни неблагоприятни последствия за националната сигурност“*, вж. член 13, параграф 4 от Закона за НРС.
([262]) Член 16, параграф 2 от Закона за инспекцията и разследването на държавната администрация.
([263]) Член 15 от ЗЗНК.
([264]) Както и в случая с Комитета по разузнаване към Националното събрание, директорът на НРС може да откаже да отговори на СОИ само на въпроси, които представляват държавна тайна, и ако публичното им оповестяване би имало сериозно въздействие върху националната сигурност (член 13, параграф 1 от Закона за НРС).
([265]) Член 63 от ЗЗЛД.
([266]) Член 61, параграф 2, член 65, параграфи 1 и 2, и член 64, параграф 4 от ЗЗЛД.
([267]) Член 8, параграф 1, точка 2 от Указа за прилагане на Закона за борба с тероризма.

3.4.2. *Механизми за правна защита, предвидени в ЗЗЛД*

Съгласно ЗЗЛД физическите лица могат да упражняват правото си на достъп, коригиране, заличаване и спиране на използването по отношение на личните данни, обработвани за целите на националната сигурност ([268]). Искания за упражняване на тези права могат да се подават директно до разузнавателната агенция или косвено чрез КЗЛД. Разузнавателната агенция може да забави, ограничи или откаже упражняването на правото само доколкото и докато е необходимо и пропорционално, за да се защити важна цел от обществен интерес (например доколкото и докато предоставянето на правото би застрашило текущо разследване или би представлявало заплаха за националната сигурност), или когато предоставянето на правото може да доведе до вредни последствия за живота или телесно увреждане на трета страна. Когато искането е отхвърлено или ограничено, физическото лице трябва да бъде уведомено незабавно за причините.

Освен това, в съответствие с член 58, параграф 4 от ЗЗЛД (изискване за гарантиране на разглеждане на индивидуални жалби по подходящ начин) и член 4, параграф 5 от ЗЗЛД (право на подходяща защита по отношение на вреди, произтичащо от обработването на лични данни, чрез бърза и справедлива процедура), физическите лица имат право да получат правна защита. Това включва правото да се докладва за предполагаемо нарушение на Центъра за обаждания по въпросите на поверителността, управляван от Корейската агенция за интернет и сигурност, и да се подаде жалба до КЗЛД ([269]). Тези средства за правна защита са налични както в случай на евентуални нарушения на правилата, съдържащи се в конкретни закони, определящи ограниченията и защитните мерки по отношение на събирането на лични данни за целите на националната сигурност, така и в ЗЗЛД. Както е обяснено в Уведомление № 2021-1, физическо лице от ЕС може да подаде жалба до КЗЛД чрез своя национален орган за защита на данните. В този случай КЗЛД ще уведоми физическото лице чрез националния орган за защита на данните след приключването на разследването (включително, ако е приложимо, с информация за наложените корективни мерки). Решенията или бездействието от страна на КЗЛД могат да бъдат допълнително обжалвани пред корейските съдилища съгласно Закона за административното съдопроизводство.

3.4.3. *Защита от Националната комисия по правата на човека*

Възможността да се получи индивидуална правна защита от НКПЧ се прилага по същия начин за разузнавателните агенции, както и за други държавни органи (вж. раздел 2.4.2).

3.4.4. *Съдебна защита*

Както е в случая с дейността на органите за наказателно правоприлагане, физическите лица могат да получат съдебна защита по различни начини по отношение на разузнавателните агенции във връзка с нарушения на горепосочените ограничения и защитни мерки.

Първо, физическите лица могат да получат обезщетение за вреди по силата на Закона за обезщетенията от държавата. Например по едно от делата е присъдено обезщетение за вреди във връзка с незаконно наблюдение от страна на Командването за поддържане на отбраната (предшественик на Командването за поддържане на сигурността в областта на отбраната) ([270]).

Второ, в Закона за административното съдопроизводство се позволява на физическите лица да оспорват разпореждания и бездействия на административните органи, включително на разузнавателните агенции ([271]).

Накрая, въз основа на Закона за Конституционния съд физическите лица могат да подадат до Конституционния съд конституционна жалба срещу мерки, предприети от разузнавателните агенции.

([268]) Член 3, параграф 5 и член 4, параграфи 1, 3 и 4 от ЗЗЛД.
([269]) Член 62 и член 63, параграф 2 от ЗЗЛД.
([270]) Решение № 96Da42789 на Върховния съд, 24 юли 1998 г.
([271]) Членове 3 и 4 от Закона за административното съдопроизводство.