II

(Незаконодателни актове)

РЕШЕНИЯ

РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2019/419 НА КОМИСИЯТА

от 23 януари 2019 година

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

(нотифицирано под номер C(2019) 304)

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

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

след консултация с Европейския надзорен орган по защита на данните,

1. ВЪВЕДЕНИЕ

(1) С Регламент (ЕС) 2016/679 се определят правилата за предаването на лични данни от администратори или обработващи лични данни в Европейския съюз на трети държави и международни организации, доколкото това предаване попада в неговото приложното поле. Правилата за международно предаване на лични данни са установени в глава V от посочения регламент, по-конкретно в членове 44—50. Движението на лични данни към и от държави извън Европейския съюз е необходимо за разширяването на международното сътрудничество и международната търговия, като в същото време се гарантира, че нивото на защита на личните данни в Европейския съюз не се излага на риск.

(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 трета държава или дадена международна организация осигуряват адекватно ниво на защита. При това условие предаването на лични данни на тази трета държава, територия или международна организация може да се извършва, без да е необходимо допълнително разрешение, както е предвидено в член 45, параграф 1 и съображение 103 от Регламента.

(3) Както е посочено в член 45, параграф 2 от Регламент (ЕС) 2016/679, приемането на решение относно адекватността трябва да се основава на цялостен анализ на правния ред на третата държава, що се отнася както до правилата, приложими към вносителите на данни, така и до ограниченията и гаранциите по отношение на достъпа до лични данни от страна на публичните органи. Оценката трябва да определи дали въпросната трета държава гарантира ниво на защита, което „по същество е равностойно“ на нивото, гарантирано в рамките на Европейския съюз (съображение 104 от Регламент (ЕС) 2016/679). Както бе изяснено от Съда на Европейския съюз, това не изисква идентично ниво на защита ([2]). По-специално средствата, до които третата въпросна държава прибягва, могат да са различни от тези, прилагани в Европейския съюз, стига те да се окажат на практика ефективни за гарантиране на високо ниво на защита ([3]). Поради това стандартът за адекватно ниво на защита не изисква буквално възпроизвеждане на правилата

([1]) ОВ L 119, 4.5.2016 г., стр. 1.

([2]) Решение по дело C-362/14, *Maximillian Schrems* c/y *Data Protection Commissioner* („*решение по делото Schrems*“), ECLI:EU:C:2015:650, точка 73.

([3]) *Решение по делото Schrems*, точка 74.

на Съюза. Критерият се състои по-скоро в това дали чрез същността на правата на неприкосновеност на личния живот и ефективното им изпълнение, контролиране и прилагане чуждестранната система като цяло осигурява необходимото ниво на защита ([4]).

(4) Комисията анализира внимателно японското право и практиката по него. Въз основа на констатациите, изложени в съображения 6—175, Комисията заключава, че Япония осигурява адекватно ниво на защита на личните данни, предавани на организациите, които попадат в приложното поле на Закона за защита на личната информация ([5]) и спрямо които се прилагат допълнителните условия, посочени в настоящото решение. Тези условия са определени в Допълнителните правила (приложение I), приети от Комисията за защита на личната информация (КЗЛИ) ([6]), и официалните декларации, уверения и ангажименти от японското правителство пред Европейската комисия (приложение II).

(5) Действието на настоящото решение се изразява в това, че предаването на лични данни от администратор или обработващ лични данни в Европейското икономическо пространство (ЕИП) ([7]) на такива организации в Япония може да се извършва, без да е необходимо получаването на допълнително разрешение. Настоящото решение не засяга прякото прилагане на Регламент (ЕС) 2016/679 спрямо такива организации, когато са изпълнени условията, посочени в член 3 от него.

2. ПРАВИЛА, КОИТО СЕ ПРИЛАГАТ ЗА ОБРАБОТВАНЕТО НА ДАННИ ОТ СТРАНА НА СТОПАНСКИ СУБЕКТИ

2.1. Японска нормативна уредба на защита на данните

(6) Нормативната уредба на правото на неприкосновеност на личния живот и защита на данните в Япония има своите корени в Конституцията, обнародвана през 1946 г.

(7) Член 13 от Конституцията гласи:

„Всички хора се зачитат като личности. Правото им на живот, свобода и стремеж към щастие, доколкото то не накърнява общественото благо, е върховно съображение при законодателството и при други държавни дейности.“

(8) Въз основа на този член Върховният съд на Япония е изяснил правата на лицата по отношение на защитата на личната информация. С решение от 1969 г. той е признал правото на неприкосновеност на личния живот и на защита на личните данни за конституционно право ([8]). По-специално Съдът е постановил, че „всеки разполага със свободата да защитава своята лична информация от това тя да бъде разкрита на трета страна или да бъде направена обществено достояние без основателна причина.“ Освен това, в решение от 6 март 2008 г. („Juki-Net“) ([9]), Върховният съд постанови, че „свободата на гражданите в личния им живот трябва да бъде защитена срещу упражняването на публична власт и може да се направи тълкуването, че, наред с другите свободи в личния живот, всеки разполага със свободата да защитава своята лична информация от това тя да бъде разкрита на трета страна или да бъде направена обществено достояние без основателна причина.“ ([10])

(9) На 30 май 2003 г. Япония прие поредица от закони в областта на защитата на данните:

— Закона за защита на личната информация (ЗЗЛИ),

— Закона за защита на личната информация, съхранявана от административни органи (ЗЗЛИСАО),

— Закона за защита на личната информация, съхранявана от независими административни агенции (ЗЗЛИСНАА).

([4]) Вж. Съобщение на Комисията до Европейския парламент и Съвета „Обмен и защита на личните данни в един глобализиран свят“, COM (2017)7 final, 10.1.2017 г., раздел 3.1, стр. 6—7.
([5]) Закон за защита на личните данни (Закон № 57, 2003 г.).
([6]) Повече информация относно КЗЛИ е достъпна посредством следната връзка: https://www.ppc.go.jp/en/ (включително данни за контакт във връзка със запитвания или жалби: https://www.ppc.go.jp/en/contactus/access/).
([7]) 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 трите държави от ЕИП — Исландия, Лихтенщайн и Норвегия. Решението на Съвместния комитет (РСК) за включване на Регламент (ЕС) 2016/679 в приложение XI от 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.
([8]) Върховен съд, Решение на Големия състав от 24 декември 1969 г., Keishu том 23, № 12, стр. 1625.
([9]) Върховен съд, Решение от 6 март 2008 г., Minshu том 62 № 3, стр. 665.
([10]) Върховен съд, Решение от 6 март 2008 г., Minshu том 62 № 3, стр. 665.

(10) Последните два акта (изменени през 2016 г.) съдържат разпоредби, приложими към защитата на личната информация от страна на субекти от публичния сектор. Обработването на данни, попадащо в приложното поле на тези актове, не е предмет на констатацията за адекватност, съдържаща се в настоящото решение, която се ограничава до защитата на лична информация от страна на „стопански субекти, третиращи лична информация“ (ССТЛИ) по смисъла на ЗЗЛИ.

(11) ЗЗЛИ беше реформиран през последните години. Измененият ЗЗЛИ беше обнародван на 9 септември 2015 г. и влезе в сила на 30 май 2017 г. С изменението бяха въведени редица нови гаранции и бяха засилени съществуващите гаранции, посредством което японската система за защита на данните бе сближена с европейската. Това включва например набор от приложими индивидуални права или създаването на независим надзорен орган (Комисията за защита на личната информация, КЗЛИ), отговарящ за прилагането на ЗЗЛИ и за надзора във връзка с него.

(12) В допълнение към ЗЗЛИ обработването на лична информация, попадаща в приложното поле на настоящото решение, се урежда от правилата за прилагане, издадени въз основа на ЗЗЛИ. Те включват изменение на Постановлението на Министерския съвет за прилагане на Закона за защита на личната информация от 5 октомври 2016 г. и т.нар Правила за прилагане на Закона за защита на личната информация, приети от КЗЛИ ([11]). И двата набора от правила са правно обвързващи и приложими и влязоха в сила едновременно с изменения ЗЗЛИ.

(13) Освен това на 28 октомври 2016 г. Министерския съвет на Япония (състоящ се от министър-председателя и министрите, влизащи в състава на неговото правителство) издаде „Основна политика“ за „всеобхватното и цялостното насърчаване на мерки относно защитата на личната информация“. В съответствие с член 7 от ЗЗЛИ „Основната политика“ се издава под формата на решение на Министерския съвет и включва насоки за политиката относно прилагането на ЗЗЛИ, адресирани както до централното правителство, така и до местните органи.

(14) Наскоро с решение на Министерския съвет, прието на 12 юни 2018 г., японското правителство измени „Основната политика“. За да се улесни международното предаване на данни, с това решение на Министерския съвет на КЗЛИ като органа, компетентен за администрирането и прилагането на ЗЗЛИ, се делегира „правомощието да предприема необходимите действия за преодоляване на различията по отношение на системите и операциите между Япония и съответната чужда държава въз основа на член 6 от Закона с оглед на гарантиране на правилното третиране на лична информация, получена от тази държава“. Решението на Министерския съвет предвижда, че това включва правомощието за установяване на засилена защита чрез приемането от КЗЛИ на по-строги правила, които допълват и надхвърлят тези, определени в ЗЗЛИ и Постановлението на Министерския съвет. Съгласно посоченото решение тези по-строги правила са обвързващи и приложими спрямо японските стопански субекти.

(15) Въз основа на член 6 от ЗЗЛИ и това решение на Министерския съвет КЗЛИ прие на 15 юни 2018 г. „Допълнителни правила съгласно Закона за защита на личната информация за третирането на лични данни, предадени от ЕС въз основа на решение относно адекватността“(„Допълнителните правила“) с оглед повишаване на защитата на личната информация, предавана от Европейския съюз към Япония въз основа на настоящото решение относно адекватността. Тези допълнителни правила са правно обвързващи за японските стопански субекти и тяхното спазване може да бъде осигурено както от КЗЛИ, така и от съдилищата, по същия начин като спазването на разпоредбите на ЗЗЛИ, който тези правила допълват с по-строги и/или по-подробни правила ([12]). Тъй като японските стопански субекти, получаващи и/или обработващи допълнително лични данни от Европейския съюз, ще бъдат правно задължени да спазват Допълнителните правила, те ще трябва да гарантират (напр. чрез технически средства („маркиране“) или организационни средства (съхраняване в специална база данни), че могат да идентифицират такива лични данни през целия си „жизнен цикъл“ ([13]). В следващите раздели съдържанието на всяко допълнително правило е предмет на анализ в рамките на оценката на членовете от ЗЗЛИ, които то допълва.

(16) За разлика от времето преди изменението от 2015 г., когато това попадаше в компетентността на различни министерства на Япония в конкретни сектори, ЗЗЛИ оправомощава КЗЛИ да приема „насоки“ „за да гарантира правилното и ефективно изпълнение на действията, които трябва да бъдат предприети от даден стопански субект“ съгласно правилата за защита на данните. Чрез своите насоки КЗЛИ дава официално тълкуване на тези правила, по-специално на ЗЗЛИ. Според информацията, получена от КЗЛИ, тези насоки представляват неразделна част от правната рамка и се четат заедно с текста на ЗЗЛИ, Постановлението на Министерския съвет, Правилата на КЗЛИ

([11]) На разположение на адрес: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Вж. Допълнителните правила (уводен раздел).

([13]) Това задължение не е в противоречие с общото задължение за поддържане на записи (само) за определен период от време. Въпреки че произходът на данните е информация, която придобиващият ССТЛИ трябва да потвърди съгласно член 26, параграф 1 от ЗЗЛИ, задължението съгласно член 26, параграф 4 от ЗЗЛИ във връзка с член 18 от Правилата на КЗЛИ се отнася само до особена форма на запис (вж. член 16 от Правилата на КЗЛИ) и не възпрепятства ССТЛИ да гарантира идентификацията на данните за по-дълги периоди. Това беше потвърдено от КЗЛИ, която заяви, че „ССТЛИ трябва да съхранява информацията за произхода на данните от ЕС толкова дълго, колкото е необходимо, за да може да се съобрази с Допълнителните правила“.

и набор от въпроси и отговори ([14]), изготвен от КЗЛИ. Следователно те са „обвързващи за стопанските субекти“. Когато в Насоките се посочва, че даден стопански оператор „трябва“ или „не следва“ да действа по определен начин, КЗЛИ ще счита, че неспазването на приложимите разпоредби представлява нарушение на закона ([15]).

2.2. **Материално и персонално приложно поле**

(17) Приложното поле на ЗЗЛИ се определя от установените понятия за лична информация, лични данни и стопански субект, третиращ лична информация. В същото време в ЗЗЛИ се предвиждат някои важни изключения от неговото приложно поле, най-вече за анонимно обработените лични данни и за специфични видове обработване на данни от страна на определени субекти. Макар че в ЗЗЛИ не се използва терминът „обработване“, този закон се позовава на равностойното понятие за „обработване“, което, съгласно информацията, получена от КЗЛИ, обхваща „всяко действие, отнасящо се до лични данни“, включително придобиването, въвеждането, натрупването, организирането, съхранението, редактирането/обработването, подновяването, заличаването, извеждането, използването или предоставянето на лична информация.

2.2.1. *Определение за лична информация*

(18) На първо място, що се отнася до неговото материално приложно поле, в ЗЗЛИ се прави разграничение между лична информация и лични данни, като само определени разпоредби на Закона се прилагат за първата категория. Съгласно член 2, параграф 1 от ЗЗЛИ понятието за „лична информация“ включва всяка информация, свързана с живо лице, която дава възможност за идентифициране на това лице. Определението разграничава две категории лична информация: i) индивидуални идентификационни кодове и ii) друга лична информация, чрез която определено лице може да бъде идентифицирано. Последната категория включва също информация, която сама по себе си не позволява извършването на идентифициране, но, когато „може лесно да бъде засечена“ с друга информация, дава възможност за идентифицирането на конкретно физическо лице. В съответствие с Насоките на КЗЛИ ([16]) преценката дали дадена информация може да се разглежда като информация, която „може лесно да бъде засечена“ се извършва за всеки отделен случай, като се взема предвид действителното положение („състояние“) на стопанския субект. Приема се, че информацията може лесно да бъде засечена, ако засичането се извършва (или може да бъде извършено) от средностатистически („нормален“) стопански субект, използващ средствата, намиращи се на неговото разположение. Например, информацията не „може лесно да бъде засечена“ с друга информация, ако даден стопански субект трябва да положи необичайни усилия или да извърши незаконни действия, за да получи информацията, която трябва да бъде засечена от един или повече други стопански субекти.

2.2.2. *Определение за лични данни*

(19) Само определени видове лична информация попадат в обхвата на понятието „лични данни“ съгласно ЗЗЛИ. Всъщност „лични данни“ се определя като „лична информация, представляваща база данни с лична информация, т.е. „общ набор от информация“, съдържащ лична информация, която е „организирана систематично така, че да е възможно търсене на конкретна лична информация с помощта на компютър“ ([17]) или „която съгласно постановление на Министерския съвет трябва да бъде систематично организирана така, че да е възможно лесно търсене на конкретна лична информация“, но „с изключение на тази, за която съгласно постановление на Министерския съвет има малка възможност да накърни правата и интересите на дадено лице, като се има предвид начина за нейното използване“ ([18]).

(20) Това изключение е допълнително уредено в член 3, параграф 1 от Постановлението на Министерския съвет, съгласно което трите посочени по-долу условия трябва да бъдат изпълнени едновременно: i) общият набор от информация трябва да е бил „издаден с цел да бъде продаван на значителен брой неопределени лица и неговото издаване не трябва да е било осъществено в нарушение на законови разпоредби или на основани на тях подзаконови разпоредби“; ii) трябва да е възможно той да бъде „закупен по всяко време от значителен брой неопределени лица“ и iii) личните данни, съдържащи се в него трябва да бъдат „предоставени за свързаната с тях първоначална цел, без да

([14]) КЗЛИ, документ „Въпроси и отговори“, 16 февруари 2017 г. (изменен на 30 май 2017 г.), достъпен посредством следната връзка: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. В документа „Въпроси и отговори“ се обсъждат редица въпроси, които са предмет на насоките, като се дават практически примери, свързани с въпроси като това кои лични данни са чувствителни, тълкуването на индивидуалното съгласие, предаването на данни на трети страни в контекста на изчисления в облак или задължението за водене на регистри, приложимо към трансграничното предаване на данни. Документът „Въпроси и отговори“ е наличен само на японски език.

([15]) В отговор на поставен конкретен въпрос КЗЛИ информира ЕКЗД, че „японските съдилища основават своето тълкуване на Насоките, когато прилагат ЗЗЛИ/Правилата на КЗЛИ по конкретни случаи, с които са сезирани, и в тази връзка пряко са се позовавали на текста на Насоките в решенията си. Следователно, също от тази гледна точка, Насоките са обвързващи за стопанските субекти. КЗЛИ няма информация Съдът някога да се е отклонил от Насоките“. В тази връзка КЗЛИ посочи на Комисията съдебно решение в областта на защитата на данните, в което съдът изрично се позовава на Насоките, за да обоснове своите заключения (вж. Окръжен съд - Осака, решение от 19 май 2006, Hanrei Jiho, том 1948, стр. 122, в което съдът е постановил, че стопанският субект е имал задължение да предприеме действие за контрол на сигурността на основание на тези насоки).

([16]) Насоки на КЗЛИ (General Rule Edition), стр. 6.

([17]) Това обхваща всяка електронна регистрационна система. В насоките на КЗЛИ (General Edition, стр. 17) се предоставят конкретни примери в това отношение, напр. списък с електронни адреси, съхраняван в клиентски софтуер за електронна поща.

([18]) Член 2, параграфи 4 и 6 от ЗЗЛИ.

се добавя друга информация, отнасяща се до живо лице“. Съгласно получените от КЗЛИ обяснения това тясно изключение е било въведено с цел да бъдат изключени телефонни указатели или подобни видове справочници.

(21) За данните, събирани в Япония, това разграничение между „лична информация“ и „лични данни“ е от значение, тъй като е възможно такава информация не винаги да е част от „база данни с лична информация“ (например единен набор от данни, събрани и обработени ръчно) и следователно само тези разпоредби на ЗЗЛИ, които се отнасят единствено до лични данни, няма да се прилагат ([19]).

(22) От друга страна, това разграничение няма да бъде от значение за личните данни, внесени от Европейския съюз в Япония въз основа на решение относно адекватното ниво на защита. Тъй като тези данни обикновено се предават по електронен път (предвид факта, че в цифровата ера това е обичайният начин за обмен на данни, особено на големи разстояния, като например между ЕС и Япония) и по този начин стават част от електронната регистрационна система на вносителя на данни, такива данни от ЕС ще попадат в категорията „лични данни“ съгласно ЗЗЛИ. В изключителни случаи, когато личните данни биха били предавани от ЕС по друг начин (напр. на хартиен носител), те ще продължават да бъдат обхванати от ЗЗЛИ, ако след прехвърлянето им те станат част от „общия набор от информация“, който е систематично организиран така, че да позволява лесно търсене на конкретна информация (член 2, параграф 4, подточка ii) от ЗЗЛИ). Съгласно член 3, параграф 2 от Постановлението на Министерския съвет, такъв е случаят, в който информацията е подредена „според определено правило“ и базата данни включва инструменти като съдържание или индекс, предназначени за улесняване на търсенето на данни. Това съответства на определението за „регистър с лични данни“ по смисъла на член 2, точка 1 от ОРЗД.

2.2.3. *Определение за запазени лични данни*

(23) Някои разпоредби на ЗЗЛИ, по-конкретно членове 27—30, свързани с индивидуални права, се прилагат само за специална категория лични данни, а именно „запазени лични данни“. Тези данни са определени съгласно член 2, параграф 7 от ЗЗЛИ като лични данни, различни от тези, които или i) „съгласно постановление на Министерския съвет е възможно да накърнят обществения интерес или други интереси, ако тяхното наличие или отсъствие бъде оповестено“, или ii) „трябва да се заличат в срок не по-дълъг от една година, определен с постановление на Министерския съвет“.

(24) Що се отнася до първата от тези две категории, тя е обяснена в член 4 от Постановлението на Министерския съвет и обхваща четири вида изключения ([20]). Тези изключения преследват подобни цели като тези, изброени в член 23, параграф 1 от Регламент (ЕС) 2016/679, а именно защитата на субекта на данни („засегнатото лице“ съгласно терминологията на ЗЗЛИ) и свободата на другите, националната сигурност, обществената сигурност, наказателното правоприлагане или други важни цели от широк обществен интерес. Освен това от текста на член 4, параграф 1, подточки i)-iv) от Постановлението на Министерския съвет произтича, че прилагането на тези изключения винаги предполага конкретен риск за един от защитените важни интереси ([21]).

(25) Втората категория е допълнително уточнена в член 5 от Постановлението на Министерския съвет. Съгласно този член, във връзка с член 2, параграф 7 от ЗЗЛИ, от обхвата на понятието за запазени лични данни и по този начин от обхвата на индивидуалните права съгласно ЗЗЛИ са изключени тези лични данни, „които трябва да се заличат“ в срок от шест месеца. КЗЛИ обясни, че това изключение има за цел да насърчи стопанските субекти да запазват и обработват данни за възможно най-кратък срок. Това обаче би означавало, че субектите на данни от ЕС няма да могат да се ползват от важни права единствено поради продължителността на запазването на личните им данни от съответния стопански субект.

(26) За да се коригира това положение, Допълнително правило 2 изисква личните данни, предавани от Европейския съюз „да се третират като запазени лични данни по смисъла на член 2, параграф 7 от Закона, независимо от срока, в който те трябва да бъдат заличени“. Следователно срокът на запазване не оказва въздействие върху правата, предоставени на субектите на данни от ЕС.

([19]) Например член 23 от ЗЗЛИ относно условията за обмена на лични данни с трети страни.

([20]) А именно лични данни i) „във връзка с които съществува риск от увреждане на живота, телесната неприкосновеност или имуществото на дадено засегнато лице или трета страна, ако наличието или отсъствието на въпросните лични данни бъде оповестено“; ii), „във връзка с които съществува риск от насърчаване или предизвикване на незаконно или несправедливо действие, ако наличието или отсъствието на въпросните лични данни бъде оповестено“; iii) „във връзка с които съществува риск от застрашаване на националната сигурност, разрушаване на връзките на доверие с друга държава или международна организация или изпадане в неизгодна позиция при преговори с друга държава или международна организация, ако наличието или отсъствието на въпросните лични данни бъде оповестено“; и iv) „във връзка с които съществува риск от възпрепятстване на поддържането на обществения ред и сигурност, например предотвратяването, противодействието или разследването на престъпления, ако наличието или отсъствието на въпросните лични данни бъде оповестено“.

([21]) При тези условия не се изисква уведомяване на лицето. Това е в съответствие с член 23, параграф 2, буква з) от ОРЗД, в който е предвидено, че субектите на данни не трябва да бъдат информирани за ограничаването, ако това „би било в разрез с целта на ограничаването“.

2.2.4. *Определение за анонимно обработена лична информация*

(27) Изискванията, приложими за анонимно обработена лична информация по смисъла на определението в член 2, параграф 9 от ЗЗЛИ, са предвидени в глава 2, раздел 4 от Закона („Задължения на стопански субект, третиращ анонимно обработена информация“). Обратно, тази информация не се урежда от разпоредбите на глава IV, раздел 1 от ЗЗЛИ, включващ членовете, в които са предвидени гаранциите за защита на данните и правата, които се прилагат за обработването на лични данни съгласно този закон. Следователно, въпреки че „стандартните“ правила за защита на данните (тези, съдържащи се в глава IV, раздел 1 и член 42 от ЗЗЛИ) не се прилагат спрямо „анонимно обработена лична информация“, тя попада в приложното поле на ЗЗЛИ, а именно членове 36—39.

(28) Съгласно член 2, параграф 9 от ЗЗЛИ „анонимно обработена лична информация“ е информация, свързана с дадено лице, която е „получена от обработването на лична информация“ посредством мерки, предписани в ЗЗЛИ (член 36, параграф 1) и подробно уредени в правилата на КЗЛИ (член 19), в резултат на което е невъзможно да се идентифицира конкретно лице или да се възстанови личната информация.

(29) От тези разпоредби следва заключението, което беше потвърдено и от КЗЛИ, че процесът на „анонимизиране“ на лична информация не трябва да бъде технически необратим. Съгласно член 36, параграф 2 от ЗЗЛИ стопанските субекти, третиращи „анонимно обработена лична информация“ трябва единствено да предотвратяват повторна идентификация, като предприемат мерки за гарантиране на сигурността на „описанията и т.н. и индивидуалните идентификационни кодове, заличени от личната информация, използвана за изготвянето на анонимно обработена информация, както и на информацията, свързана с прилагането на даден метод на обработване“.

(30) Като се има предвид, че „анонимно обработена лична информация“ съгласно определението в ЗЗЛИ включва данни, посредством които повторно идентифициране на лицето все още е възможно, това би могло да означава, че лични данни, които се предават от Европейския съюз, е възможно да загубят част от наличната защита в резултат от процес, който съгласно Регламент (ЕС) 2016/679 би се считал за форма на „псевдонимизация“, а не за „анонимизация“ (и който следователно не променя характера им на лични данни).

(31) За се коригира това положение, в Допълнителните правила се предвиждат допълнителни изисквания, приложими само по отношение на личните данни, предавани от Европейския съюз съгласно настоящото решение. Съгласно Правило 5 от Допълнителните правила такава лична информация се счита за анонимно обработена лична информация по смисъла на ЗЗЛИ само „ако стопанският субект, третиращ лична информация, предприеме мерки, посредством които анонимизирането на лицето става необратимо за всеки, включително заличаването на информация, отнасяща се до метода на обработване.“ Последната информация е определена в Допълнителните правила като информация, отнасяща се до индивидуалните идентификационни кодове, които са били заличени от личната информация, използвана за изготвянето на „анонимно обработена лична информация“, както и като информация, отнасяща се до метод на обработване, приложен при заличаването на тези описания и индивидуални идентификационни кодове. С други думи Допълнителните правила изискват стопанският субект, изготвящ анонимно обработена лична информация, да унищожи „ключа“, позволяващ повторно идентифициране на данните. Това означава, че лични данни с произход от Европейския съюз ще попаднат в обхвата на разпоредбите на ЗЗЛИ относно „анонимно обработена лична информация“ само в случаите, когато тези данни също биха били считани за анонимна информация съгласно Регламент (ЕС) 2016/679 ([22]).

2.2.5. *Определение за стопански субект, третиращ лична информация (ССТЛИ)*

(32) Що се отнася до неговото персонално приложно поле, ЗЗЛИ се прилага само по отношение на ССТЛИ. ССТЛИ е определен в член 2, параграф 5 от ЗЗЛИ като „лице, което предоставя база данни с лична информация и т.н. за употреба в рамките на дадена дейност“, с изключение на правителството и административните агенции както на централно, така и на местно равнище.

(33) В съответствие с Насоките на КЗЛИ „дейност“ означава „поведение, което има за цел повтаряемо и трайно осъществяване с определена цел, независимо дали тази цел е стопанска или не, на социално признато начинание“. Организации без правосубектност (като например фактически сдружения) или физически лица се считат за ССТЛИ, ако предоставят (използват) база данни с лични данни и т.н. за своята дейност ([23]). Следователно обхватът на понятието „дейност“ съгласно ЗЗЛИ е много широк, тъй като включва не само дейности със стопанска цел, но и дейности с нестопанска цел на всякакви видове организации и физически лица. Освен това „употреба в рамките на дадена дейност“ обхваща също така лична информация, която не се употребява във търговски отношения на стопанския субект (външни отношения), а вътрешно, например за обработване на данни на служители.

([22]) Вж. Регламент (ЕС) 2016/679, съображение 26.
([23]) Насоки на КЗЛИ (General Rule Edition), стр. 18.

(34) Що се отнася до лицата, ползващи се от защитата, предвидена в ЗЗЛИ, Законът не прави разграничение въз основа на гражданството, местожителството или местонахождението на лицето. Същото се отнася и за възможностите, предоставени на лицата да търсят защита, било то от КЗЛИ, било то от съдилищата.

2.2.6. *Понятията „администратор“ и „обработващ лични данни“*

(35) Съгласно ЗЗЛИ няма конкретно разграничение между задълженията, възложени на администраторите и обработващите лични данни. Липсата на това разграничение не засяга нивото на защита, защото всички разпоредби на Закона се прилагат по отношение на всички ССТЛИ. ССТЛИ, който възлага третирането на лични данни на довереник (еквивалента на обработващ лични данни съгласно ОРЗД), продължава да е обвързан от задълженията съгласно ЗЗЛИ и Допълнителните правила във връзка с данните, чието третиране той е възложил на довереника. Освен това съгласно член 22 от ЗЗЛИ той е длъжен да „упражнява необходим и подходящ надзор“ върху довереника. На свой ред, както КЗЛИ потвърждава, довереникът е обвързан от всички задължения съгласно ЗЗЛИ и Допълнителните правила.

2.2.7. *Секторни изключения*

(36) Съгласно член 76 от ЗЗЛИ определени видове обработване на данни са изключени от прилагането на глава IV на Закона, която съдържа основните разпоредби за защита на данните (основни принципи, задължения на стопанските субекти, индивидуални права, надзор от страна на КЗЛИ). Спрямо обработването, попадащо в приложното поле на секторното изключение в член 76, също така не се прилагат правомощията на КЗЛИ за правоприлагане съгласно, в съответствие с член 43, параграф 2 от ЗЗЛИ ([24]).

(37) Съответните категории за секторното изключение в член 76 от ЗЗЛИ са определени посредством използването на двоен критерий, основаващ се на вида ССТЛИ, обработващ личната информация, и целта на обработването. По-конкретно изключението се прилага за: i) радио- и телевизионни оператори, издатели на вестници, комуникационни агенции или други организации на пресата (включително всички лица, които упражняват дейност, свързана с пресата), доколкото те обработват лична информация за целите на пресата; ii) лица, които по занятие упражняват писателска дейност, доколкото тя засяга лична информация; iii) университети и други организации или групи, които имат за цел извършването на академични проучвания, или лица, принадлежащи към тези организации, доколкото те обработват лична информация за целите на академични проучвания; iv) религиозни организации, доколкото те обработват лична информация за целите на религиозни дейности (включително всички свързани дейности); и v) политически организации, доколкото те обработват лична информация за целите на тяхната политическа дейност (включително всички свързани дейности). Спрямо обработването на лична информация за една от целите, изброени в член 76, от страна на други видове ССТЛИ, както и спрямо обработването на лична информация от страна на един от изброените ССТЛИ за други цели, например в работен контекст, продължават да се прилагат разпоредбите на глава IV.

(38) За да се гарантира адекватно ниво на защита на личните данни, предавани от Европейския съюз на стопански субекти в Япония, само обработването на лична информация, попадаща в приложното поле на глава IV от ЗЗЛИ — т.е. обработване от ССТЛИ, доколкото случаят на обработване не попада в едно от секторните изключения — следва да бъде обхванато от настоящото решение. Следователно обхватът му трябва да бъде приведен в съответствие с този на ЗЗЛИ. Съгласно информацията, получена от КЗЛИ, случаят, в който даден ССТЛИ, попадащ в приложното поле на настоящото решение, впоследствие промени целта на употреба (доколкото това е позволено) и след това спрямо него бъде приложено едно от секторните изключения по член 76 от ЗЗЛИ, ще се счита за международно предаване на данни (като се има предвид, че в такива случаи глава IV от ЗЗЛИ повече няма да се прилага спрямо обработването на лична информация и поради това съответното обработване ще попада извън нейното приложно поле). Същото ще важи и в случая, в който ССТЛИ предоставя лична информация на субект, попадащ в приложното поле на член 76 от ЗЗЛИ, за употреба за една от целите на обработването, посочени в тази разпоредба. По отношение на личните данни, предавани от Европейския съюз, това следователно би представлявало последващо предаване на данни, по отношение на което се прилагат съответните гаранции (по-специално посочените в член 24 от ЗЗЛИ и Допълнително правило 4). Когато ССТЛИ разчита на съгласието на субекта на данните ([25]), той ще трябва да му предостави цялата необходима информация, включително информация за това, че личната информация повече няма да бъде защитена съгласно ЗЗЛИ.

([24]) Що се отнася до другите субекти, КЗЛИ при упражняване на своите правомощия за разследване и правоприлагане не трябва да възпрепятства упражняването на правото им на свобода на изразяване на мнение, на академична свобода, на свобода на религията и на свобода на политическа дейност (член 43, параграф 1 от ЗЗЛИ).

([25]) Както бе обяснено от КЗЛИ, съгласието се тълкува в Насоките на КЗЛИ като „израз на намерението на съответното засегнато лице да приеме, че неговите лични данни могат да бъдат третирани по начина, посочен от стопанския субект, третиращ лична информация“. В Насоките на КЗЛИ (General Rule Edition, стр. 24) са изброени начините за изразяване на съгласие, които се считат за „обичайни стопански практики в Япония“, т.е. устно споразумение, връщане на формуляри или други документи, споразумение по електронна поща, поставяне на отметка в уебстраница, щракване върху начална страница, използване на бутон за съгласие, докосване на сензорен панел и др. Всички тези методи представляват форма на изрично изразяване на съгласие.

2.3. **Гаранции, права и задължения**

2.3.1. *Ограничаване в рамките на целта*

(39) Личните данни следва да се обработват с конкретна цел и впоследствие да се използват само дотолкова, доколкото употребата им не е несъвместима с целта на обработването. Този принцип за защита на данните е гарантиран по силата на членове 15 и 16 от ЗЗЛИ.

(40) ЗЗЛИ се основава на принципа, че стопанските субекти трябва да посочват целта на употребата „по възможно най-ясен начин“ (член 15, параграф 1) и впоследствие са обвързани с тази цел при обработването на данните.

(41) В това отношение член 15, параграф 2 от ЗЗЛИ предвижда, че първоначалната цел не трябва да се променя от ССТЛИ „отвъд степента, за която е признато, че е разумно свързана с целта на употребата преди извършването на промяната“, като тази степен се тълкува в Насоките на КЗЛИ за съответстващата на това, което може да бъде обективно очаквано от субекта на данни въз основа на „нормалните социални конвенции“ ([26]).

(42) Освен това съгласно член 16, параграф 1 от ЗЗЛИ на ССТЛИ е забранено да третират лична информация в „степен, надхвърляща необходимото за постигане целта на употреба“, посочена в член 15, без да получат предварително съгласието на субекта на данни, освен ако е приложимо някое от изключенията по член 16, параграф 3 ([27]).

(43) Когато става въпрос за лична информация, получена от друг стопански субект, ССТЛИ по принцип разполага със свободата да определи нова цел на употреба ([28]). С цел да се гарантира, че в случай на предаване на данни от Европейския съюз получателят на данните е обвързан с целта, за която данните са били предадени, Допълнително правило 3 изисква, че в случаите, „когато [ССТЛИ] получава лични данни от ЕС въз основа на решение относно адекватното ниво на защита“ или такъв стопански субект получава от друг [ССТЛИ] лични данни, които преди това са били предадени от ЕС въз основа на решение относно адекватното ниво на защита“ (последващо споделяне), получателят трябва да „посочи, че въпросните лични данни се употребяват в рамките на целта на употреба, във връзка с която данните първоначално или впоследствие са били получени“. С други думи, правилото гарантира, че в контекста на дадено предаване целта, посочена съгласно Регламент (ЕС) 2016/679, продължава да определя обработването и че една промяна на целта на всеки етап от веригата на обработване в Япония ще изисква съгласието на субекта на данни от ЕС. Получаването на това съгласие изисква обаче ССТЛИ да установи контакт със субекта на данните и в случаите, когато това не е възможно, последицата от това е просто, че първоначалната цел трябва да се запази.

2.3.2. *Законосъобразност и добросъвестност на обработването*

(44) Допълнителната защита, посочена в съображение 43, е от още по-голямо значение, тъй като именно чрез принципа за ограничаване в рамките на целта японските система също гарантира, че личните данни се обработват законосъобразно и добросъвестно.

(45) Съгласно ЗЗЛИ, когато ССТЛИ събира лична информация, той е длъжен да посочи подробно ([29]) целта на употреба на личната информация и своевременно да информира субекта на данни за тази цел на употреба (или да оповести публично тази цел) ([30]). Освен това член 17 от ЗЗЛИ предвижда, че ССТЛИ не може да придобива лична информация чрез измама или други непозволени средства. Що се отнася до определени категории данни, като например лична информация, изискваща специална грижа, за придобиването им е необходимо съгласието на субекта на данни (член 17, параграф 2 от ЗЗЛИ).

([26]) Документът „Въпроси и отговори“, издаден от КЗЛИ, съдържа редица примери, илюстриращи това понятие. Сред примерите за ситуации, в които промяната е извършена в степен, която е разумно свързана с първоначалната цел, е по-специално използването на лична информация, придобита от купувачите на стоки или услуги в контекста на търговска сделка, с цел информиране на тези купувачи за други стоки или услуги (напр. управител на фитнес клуб, който записва електронните адреси на членовете на клуба, за да ги информира за курсове и програми). В същото време документът „Въпроси и отговори“ съдържа също така пример за ситуация, в която промяната на целта на употреба не е позволена, а именно ако дадено дружество изпраща информация за своите стоки и услуги на електронни адреси, които то е събрало с цел отправяне на предупреждение за измама или кражба на членска карта.

([27]) Тези изключения могат да произтичат от други законови и подзаконови актове или да се отнасят до ситуации, при които обработването на лична информация е необходимо i) за „защитата на живота, телесната неприкосновеност или имуществото на дадено лице“; ii) за „подобряването на обществената хигиена или насърчаването на растежа на здрави деца“; или iii) „за сътрудничеството с правителствени агенции или организации или с техни представители“ при изпълнението на техните законоустановени задачи. Освен това категории i) и ii) се прилагат само ако е трудно да се получи съгласието на субекта на данни, а категория iii) — само ако съществува риск получаването на съгласието на субекта на данни да попречи на изпълнението на тези задачи.

([28]) При все това, въз основа на член 23, параграф 1 от ЗЗЛИ, съгласието на съответното лице по принцип е необходимо за разкриването на неговите данни на трета страна. По този начин лицето е в състояние да упражнява известен контрол върху употребата на неговите данни от друг стопански субект.

([29]) Съгласно член 15, параграф 1 от ЗЗЛИ това посочване трябва да бъде направено „по възможно най-ясен начин“.

([30]) Член 18, параграф 1 от ЗЗЛИ.

(46) Поради това, както бе обяснено в съображения 41 и 42, на ССТЛИ е забранено да обработва лични данни за други цели, с изключение на случаите, когато субектът на данните да е дал съгласието си за такова обработване или когато се прилага една от дерогациите съгласно член 16, параграф 3 от ЗЗЛИ.

(47) Накрая, що се отнася до по-нататъшното предоставяне на лична информация на трета страна ([31]), член 23, параграф 1 от ЗЗЛИ ограничава такова разкриване до специфични случаи, в които по правило се изисква предварителното съгласие на субекта на данни ([32]). В член 23, параграфи 2, 3 и 4 от ЗЗЛИ са предвидени изключения от изискването за получаване на съгласие. Тези изключения обаче са приложими само по отношение на нечувствителни данни и изискват стопанският субект да уведоми предварително засегнатите лица за намерението си да разкрие тяхната лична информация на трета страна и за възможността да възразят срещу всякакво по-нататъшно разкриване ([33]).

(48) При предаване на данни от Европейския съюз личните данни по необходимост първо се събират и обработват в ЕС в съответствие с Регламент (ЕС) 2016/679. Това винаги ще включва, от една страна, събиране и обработване на лични данни, включително за предаване от Европейския съюз към Япония, на едно от правните основания, изброени в член 6, параграф 1 от Регламента, и от друга страна, събирането на данни за конкретна, изрично указана и законна цел, както и забраната за по-нататъшно обработване, включително чрез предаване, по начин, който е несъвместим с тази цел, както е предвидено в член 5, параграф 1, буква б) и член 6, параграф 4 от Регламента.

(49) Съгласно Допълнително правило 3 след предаването ССТЛИ, който получава данните, трябва да „потвърди“, конкретната/конкретните цел(и) в основата на предаването (т.е. целта или целите, посочени съгласно Регламент (ЕС) 2016/679) и да извърши по-нататъшно обработване на тези данни в съответствие с тази цел или тези цели ([34]). Това означава че, не само този, който първоначално придобива тези лични данни в Япония, но и всеки бъдещ получател на данните (включително довереник) е обвързан с целта или целите, посочени в Регламента.

(50) Освен това, в случай че ССТЛИ желае да промени целта, посочена предварително съгласно Регламент (ЕС) 2016/679, в съответствие с член 16, параграф 1 от ЗЗЛИ той трябва да получи по принцип съгласието на субекта на данни. Без това съгласие всяко обработване на данни отвъд степента, необходима за постигането на целта на употребата, би представлявало нарушение на член 16, параграф 1, което би могло да бъде предмет на произнасяне от КЗЛИ и съдилищата.

(51) Ето защо, като се има предвид, че съгласно Регламент (ЕС) 2016/679 за предаването се изискват валидно правно основание и конкретна цел, които са отразени в целта на употреба, „потвърдена“ съгласно ЗЗЛИ, комбинацията от съответните разпоредби на ЗЗЛИ и на Допълнително правило 3 гарантира непрекъснатата законосъобразност на обработването на данни от ЕС в Япония.

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

(52) Данните следва да бъдат точни и при необходимост редовно да се актуализират. Данните следва да са подходящи, релевантни и да не превишават по обем необходимото във връзка с целите, за които се обработват.

(53) Тези принципи са гарантирани в японското право от член 16, параграф 1 от ЗЗЛИ, който забранява обработването на лични данни отвъд „степента, необходима за постигане на целта на употреба“. Както беше обяснено от КЗЛИ, това не само изключва използването на данни, които са неподходящи, и прекомерното използване на данни (отвъд степента, необходима за постигане целта на употреба), но също така обхваща забраната за обработване на данни, които не са релевантни за постигането на целта на употреба.

([31]) Въпреки че довереницте са изключени от понятието „трета страна“ за целите на прилагането на член 23 (вж. параграф 5), това изключение се прилага само доколкото довереникът обработва лични данни в рамките на поръчката („в степента, необходима за постигане на целта на употреба“), т.е. действа като обработващ лични данни.

([32]) Другите (изключителни) основания за това са: i) предоставянето на лична информация „въз основа на законови и подзаконови актове“; ii) случаи „в които съществува необходимост от защита на живота, телесната неприкосновеност или имуществото на дадено лице и в които е трудно да се получи съгласието на дадено засегнато лице“; iii) случаи „в които съществува специална необходимост от подобряване на обществената хигиена или насърчаване на отглеждането на здрави деца и в които е трудно да се получи съгласието на дадено засегнато лице“; и iv) случаи „в които съществува необходимост от сътрудничество с организация за централно или местно държавно управление или с лице, на което такава организация е възложила изпълнението на функции, предвидени в закони и подзаконови актове, и в които има риск получаването на съгласието на дадено засегнато лице да попречи на изпълнението на посочените функции“.

([33]) Информацията, която трябва да бъде предоставена включва по-специално категориите лични данни, които трябва да бъдат предадени на дадена трета страна, и метода на предаване. Освен това ССТЛИ трябва да информира субекта на данни за възможността да се противопостави на предаването и за това как да отправи такова искане.

([34]) В съответствие с член 26, параграф 1, подточка ii) от ЗЗЛИ ССТЛИ е задължен, когато получава лични данни от трета страна, да „потвърди“ (провери) „детайлите по придобиването на личните данни от третата страна“, включително целта на въпросното придобиване. Въпреки че в член 26 не се посочва изрично, че ССТЛИ тогава трябва да следва тази цел, това се изисква изрично съгласно Допълнително правило 3.

(54) Що се отнася до задължението за поддържане на точността и актуалността на данните, член 19 от ЗЗЛИ изисква от ССТЛИ да „се стреми да поддържа точността и актуалността на личните данни в степента, необходима за постигане на целта на употреба“. Тази разпоредба следва да се чете заедно с член 16, параграф 1 от ЗЗЛИ: съгласно обясненията, получени от КЗЛИ, ако ССТЛИ не спази предписаните стандарти за точност, обработването на лична информация няма да се счита за постигащо целта на употреба и следователно нейното обработване ще стане незаконно съгласно член 16, параграф 1.

2.3.4. *Ограничение на съхранението*

(55) По принцип данните следва да се съхраняват не повече от необходимото за целите, за които личните данни се обработват.

(56) Съгласно член 19 от ЗЗЛИ ССТЛИ имат задължение да „се стремят […] да заличават личните данни незабавно, когато тази употреба повече не е нужна“. Тази разпоредба е необходимо да се чете във връзка с член 16, параграф 1 от ЗЗЛИ, съдържащ забрана за третирането на лични данни отвъд „степента, необходима за постигане на целта на употреба“. След като бъде постигната целта на употреба, обработването на лична информация не може да се счита за необходимо и следователно не може да продължи (освен ако ССТЛИ получи съгласието на субекта на данни за продължаване на обработването).

2.3.5. *Сигурност на данните*

(57) 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 следва да предприемат подходящи технически и организационни мерки за защита на личните данни от възможни заплахи. Тези мерки следва да се оценяват, като се вземат предвид достиженията на техническия прогрес и съответните разходи.

(58) Този принцип е въведен в японското право с член 20 от ЗЗЛИ, предвиждащ, че ССТЛИ „предприема необходими и подходящи действия за контрола върху сигурността на личните данни, включително за предотвратяването на изтичане, загуба или увреждане на обработените от него данни.“ В Насоките на КЗЛИ се обясняват мерките, които трябва да бъдат взети, включително методите за формулиране на основни политики, правилата за третиране на данни и различните „действия за контрол“ (по отношение на организационната безопасност, както и по отношение на човешката, физическата и технологичната сигурност) ([35]). Освен това Насоките и специално известие (Допълнение 8 относно „съдържанието на мерките за управление на безопасността, които трябва да бъдат взети“), публикувано от КЗЛИ, предоставят по-подробна информация относно мерките по отношение на инциденти във връзка със сигурността, включващи например изтичане на лична информация, като част от мерките за управление на сигурността, които трябва да бъдат взети от ССТЛИ ([36]).

(59) Освен това, когато личната информация се обработва от служители или подизпълнители, съгласно членове 20 и 21 от ЗЗЛИ трябва да се осигури „необходим и подходящ надзор“ за целите на контрола за сигурност. Накрая, съгласно член 83 на ЗЗЛИ, умишлено предизвиканото изтичане на лична информация или кражбата на такава информация се наказва с лишаване от свобода до една година.

2.3.6. *Прозрачност*

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

(61) Член 18, параграф 1 от ЗЗЛИ изисква от ССТЛИ да предоставя на разположение на субекта на данни информация относно целта на употреба на придобитата лична информация, освен в „случаите, в които целта на употреба е била разкрита предварително на обществеността“. Същото задължение важи в случай на разрешена промяна на целта (член 18, параграф 3). Това също гарантира, че субектът на данни е информиран за факта, че негови данни са били събрани. Въпреки че съгласно ЗЗЛИ от ССТЛИ обикновено не се изисква да информира субекта на данни за очакваните получатели на лична информация на етапа на събирането, такава информация е необходима предпоставка за всяко последващо разкриване на информация на трета страна (получател) въз основа на член 23, параграф 2, т.е. когато това се извършва без предварително съгласие на субекта на данни.

([35]) Насоки на КЗЛИ (General Rule Edition), стр. 41 и стр. от 86 до 98.

([36]) Съгласно раздел 3-3-2 от Насоките на КЗЛИ в случай на изтичане, увреждане или загуба на лична информация ССТЛИ е длъжен да извърши необходимите разследвания и по-специално да прецени степента на нарушаване на правата и интересите на лицата, както и естеството и количеството на въпросната лична информация.

(62) По отношение на „запазени лични данни“ член 27 от ЗЗЛИ предвижда, че ССТЛИ предоставя характеризираща го информация на субекта на данни (данни за контакт), а така също и информация относно целта на употреба и процедурите за отговор на искане във връзка с индивидуалните права на субекта на данни съгласно членове 28, 29 и 30 от ЗЗЛИ.

(63) Предвид обстоятелството, че лични данни, предавани от Европейския съюз, ще бъдат считани за „запазени лични данни“ независимо от техния срок на запазване (освен ако не попадат в приложното поле на някое изключение), спрямо тях ще се прилагат изискванията за прозрачност, съдържащи се в двете посочени разпоредби.

(64) Както по отношение на изискванията на член 18, така и по отношение на задължението за предоставяне на информация за целта на употреба съгласно член 27 ЗЗЛИ се прилага същият набор от изключения, основаващи се главно на съображения от обществен интерес и на защитата на правата и интересите на субекта на данни, на трети страни и на администратора ([37]). Съгласно тълкуването, развито в Насоките на КЗЛИ, тези изключения се прилагат в много специфични случаи, например когато има риск информацията за целта на употреба да отслаби действието на законни мерки, взети от стопанския субект за защита на определени интереси (като борба срещу измамите, промишления шпионаж и саботажа).

2.3.7. *Специални категории данни*

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

(66) Определението за „лична информация, изискваща специална грижа“ се съдържа в член 2, параграф 3 от ЗЗЛИ. Тази разпоредба се отнася до „лична информация, която е свързана с расата, убежденията, социалния статус, медицинското досие, съдебното досие, факта, че са претърпени вреди в резултат от престъпление, или други описания на засегнатото лице и която съгласно постановление на Министерския съвет е определена като информация, чието третиране изисква специална грижа с цел засегнатото лице да не бъде подложено на несправедлива дискриминация, предразсъдъци или други неблагоприятни последици“. Тези категории съответстват в голямата си част на списъка на чувствителни данни съгласно членове 9 и 10 от Регламент (ЕС) 2016/679. По-специално „медицинско досие“ съответства на „данни за здравословното състояние“, а „съдебното досие и факта, че са претърпени вреди в резултат от престъпление“ са по същество същите като категориите данни, посочени в член 10 от Регламент (ЕС) 2016/679. На категориите, посочени в член 2, параграф 3 от ЗЗЛИ, е дадено допълнително тълкуване в Постановлението на Министерския съвет и Насоките на КЗЛИ. Съгласно раздел 2.3, точка 8 от Насоките на КЗЛИ., подкатегориите на „медицинско досие“, изложени подробно в член 2, подточки ii) и iii) от Постановлението на Министерския съвет се тълкуват като обхващащи генетични и биометрични данни. Също така, макар че списъкът не включва изрично термините „етнически произход“ и „политически възгледи“, той включва препратки към „раса“ и „убеждения“. Както е обяснено в раздел 2.3, точки 1 и 2 от Насоките на КЗЛИ, препратката към „раса“ обхваща „етнически връзки или връзки с определена част на света“, а „убеждения“ се разбира, че включва както религиозни, така и политически възгледи.

(67) Както е видно от текста на разпоредбата, този списък не е изчерпателен, тъй като може да се добавят допълнителни категории данни, ако тяхното обработване поражда риск от това „засегнатото лице да […] бъде подложено на несправедлива дискриминация, предразсъдъци или други неблагоприятни последици“.

(68) Въпреки че понятието „чувствителни данни“ по своята същност е социална конструкция, тъй като се основава на културните и правни традиции, моралните съображения, избора на политики и т.н. на дадено общество, предвид значението на осигуряването на адекватни гаранции за чувствителните данни при предаването им към стопански субекти в Япония, Комисията постигна разпростирането на специалната защита, предоставена за „лична информация, изискваща специална грижа“ съгласно японското право, върху всички категории данни, признати за „чувствителни данни“ в Регламент (ЕС) 2016/679. За тази цел Допълнително правило 1 предвижда, че данните, предавани от Европейския съюз и отнасящи до сексуалния живот, сексуалната ориентация или членството в синдикална организация на дадено лице, се обработват от ССТЛИ „по същия начин както лична информация, изискваща специална грижа по смисъла на член 2, параграф 3 от [ЗЗЛИ]“.

([37]) Те са i) случаи, в които има риск информирането на субекта на данни за целта на употреба или нейното публично оповестяване да „увреди живота, телесната неприкосновеност, имуществото или други права и интереси на дадено засегнато лице или трета страна“ или „правата или законните интереси на […] ССТЛИ“; ii) случаи, в които „съществува необходимост от сътрудничество с организация за централно или местно държавно управление при изпълнението на нейните законоустановени задачи и в които такава информация или разкриване биха попречили на изпълнението на такива „задачи“; iii) случаи, в които целта на употреба става ясна от ситуацията, в която данните са били придобити.

(69) Що се отнася до допълнителните материалноправни гаранции, приложими към личната информация, изискваща специална грижа, съгласно член 17, параграф 2 от ЗЗЛИ ССТЛИ нямат право да придобиват такъв тип данни без предварителното съгласие на засегнатото лице, като от това правило има само малък брой изключения ([38]). Освен това тази категория лична информация е изключена от възможността за разкриване на лична информация на трети страни въз основа на процедурата, предвидена в член 23, параграф 2 от ЗЗЛИ (позволяваща предаване на данни на трети страни без предварителното съгласие на засегнатото лице).

2.3.8. *Отчетност*

(70) Съгласно принципа на отчетност субектите, които обработват данни, са задължени да въведат подходящи технически и организационни мерки за ефективно спазване на техните задължения за защита на данните и да са в състояние да докажат това спазване, по-специално пред компетентния надзорен орган.

(71) Както бе посочено в забележка под линия 34 (съображение 49), съгласно член 26, параграф 1 от ЗЗЛИ ССТЛИ са задължени да проверят коя е третата страна, която им предоставя лични данни, както и „обстоятелствата“, при които такива данни са били придобити от трета страна (в случая на лични данни, попадащи в приложното поле на настоящото решение, съгласно ЗЗЛИ и Допълнително правило 3 тези обстоятелства включват факта, че данните произхождат от Европейския съюз, както и целта на първоначалното предаване на данни). Наред с другото тази мярка има за цел да гарантира законността на обработването на данните по цялата верига от ССТЛИ, третиращи личните данни. Освен това, съгласно член 26, параграф 3 от ЗЗЛИ, ССТЛИ са задължени да пазят запис на датата на получаване и (задължителната) информация, получена от третата страна в съответствие с параграф 1, както и името на засегнатото лице (субекта на данни), категориите обработвани данни и, доколкото е уместно, обстоятелството, че субекта на данни е дал съгласието си за предаване на негови лични данни. Съгласно член 18 от Правилата на КЗЛИ тези записи трябва да се съхраняват за минимален срок от една до три години в зависимост от обстоятелствата. При изпълнението на своите задачи КЗЛИ може да изисква представянето на такива записи ([39]).

(72) ССТЛИ трябва своевременно и надлежно да разглеждат жалбите от засегнатите лица относно обработването на тяхната лична информация. За да се улесни разглеждането на жалбите, те трябва да установяват „система, необходима за постигането на [тази] цел“, което предполага, че те следва да въведат подходящи процедури в рамките на своята организация (например да възложат отговорности или да определят звено за контакт).

(73) На последно място, ЗЗЛИ създава рамка за участието на секторни браншови организации в осигуряването на високо равнище на съответствие (вж. глава IV, раздел 4). Ролята на такива акредитирани организации за защита на личната информация ([40]) е да насърчават защитата на личната информация, като подпомагат предприятията чрез своя експертен опит, но също така и да допринасят за прилагането на гаранции, по-специално като разглеждат индивидуални жалби и помагат за разрешаването на свързаните с тях спорове. За тази цел те могат да поискат от участващите ССТЛИ, ако е целесъобразно, да приемат необходимите мерки ([41]). Освен това, в случай на нарушения на защитата на данните или други инциденти, свързани със сигурността, ССТЛИ по принцип трябва да информират КЗЛИ, както и субекта на данни (или обществеността), и да предприемат необходимите действия, включително мерки за свеждане до минимум на евентуалните вреди и за предотвратяване на повторното възникване на подобни инциденти ([42]). Въпреки че това са доброволни схеми, към 10 август 2017 г. 44 организации бяха записани в КЗЛИ, като само в най-голямата от тях, Японския център за обработване на информация и

([38]) Изключенията са следните: i) „случаи, основаващи се на законови и подзаконови актове“; ii) „случаи, в които съществува необходимост от защита на живота, телесната неприкосновеност или имуществото на дадено лице и в които е трудно да се получи съгласието на дадено засегнато лице“; iii) „случаи, в които съществува специална необходимост от подобряване на обществената хигиена или насърчаване на отглеждането на здрави деца и в които е трудно да се получи съгласието на дадено засегнато лице“; iv) „случаи, в които съществува необходимост от сътрудничество с организация за централно или местно държавно управление или с лице, на което такава организация е възложила изпълнението на функции, предвидени в закони и подзаконови актове, и в които има риск получаването на съгласието на дадено засегнато лице да попречи на изпълнението на посочените функции“; и v) случаи, в които въпросната лична информация, изискваща специална грижа, е публично оповестена от субект на данни, правителствена организация, орган на местно управление, лице, което попада в една от категориите по член 76, параграф 1, или други лица, определени в правила на КЗЛИ. Още една категория се отнася до „други случаи, които са определени в постановление на Министерския съвет като равностойни на тези случаи, определени във всяка предходна точка“, и съгласно действащото постановление на Министерския съвет обхваща по-специално очевидни личностни характеристики (напр. видимо здравословно състояние), ако чувствителните данни са били придобити (неумишлено) чрез визуално наблюдение, филмиране или фотографиране на субекта на данни, например чрез камери за видеонаблюдение.

([39]) Съгласно член 40, параграф 1 от ЗЗЛИ КЗЛИ може, доколкото това е необходимо за изпълнението на съответните разпоредби от ЗЗЛИ, да изисква от ССТЛИ да представят необходимата информация или материали, свързани с третирането на лична информация.

([40]) В ЗЗЛИ са предвидени, наред с другото, правила за акредитацията на такива организации; вж. членове 47-50 от ЗЗЛИ.

([41]) Член 52 от ЗЗЛИ.

([42]) ЗЗЛИ, Уведомление 1/2017 „Относно действията, които трябва да бъдат предприети при случаи на нарушение на защитата на личните данни или други инциденти“.

информационно развитие (ЯЦОИИР), участват 15 436 стопански субекта ([43]). Акредитираните схеми включват секторни асоциации, като например Японската асоциация на търговците на ценни книжа, Японската асоциация на училищата за водачи на автомобили или Асоциацията на брачните посредници ([44]).

(74) Акредитираните организации за защита на личната информация представят годишни доклади относно своите дейности. Според „Прегледа на степента на изпълнение [на] ЗЗЛИ през финансовата 2015 г.“, публикуван от КЗЛИ, акредитираните организации за защита на личната информация са получили общо 442 жалби, изискали са 123 обяснения от стопански субекти в своята област на компетентност, изискали са документи от тези субекти в 41 случая, дали са 181 указания и са отправили две препоръки ([45]).

2.3.9. *Ограничения на последващото предаване на данни*

(75) Равнището на защита на личните данни, което се осигурява за данните, предавани от Европейския съюз към стопански субекти в Япония, не трябва да бъде подкопавано от по-нататъшното предаване на тези данни към получатели в трета държава извън Япония. Подобни „последващи предавания“, които от гледна точка на японските стопански субекти представляват международни предавания от Япония, следва да бъдат разрешавани само когато новият получател извън Япония сам по себе си е подчинен на правила, гарантиращи сходно ниво на защита, като това в правния ред на Япония.

(76) Първи тип закрила е заложен в член 24 от ЗЗЛИ, с който по принцип се забранява предаването на лични данни на трети страни извън територията на Япония без предварителното съгласие на съответното лице. Допълнително правило 4 гарантира, че в случай на предаване на данни от Европейския съюз такова съгласие се дава след предоставянето на съществен обем информация, тъй като се изисква на засегнатите лица „да се предоставя информация относно обстоятелствата около предаването, необходими на засегнатото лице, за да вземе решение относно своето съгласие“. На това основание на субекта на данни се предоставя информация, че данните ще бъдат предадени в чужбина (извън приложното поле на ЗЗЛИ), и информация за конкретната държава на местоназначение. Това ще му даде възможност да оцени риска за неприкосновеността на личния му живот, свързан с предаването. Освен това, както може да се заключи от член 23 от ЗЗЛИ (вж. съображение 47), информацията, която се предоставя на засегнатото лице, следва да обхваща задължителните елементи съгласно параграф 2, а именно категориите лични данни, предоставяни на трета страна, и начина на разкриване.

(77) Член 24 от ЗЗЛИ, прилаган във връзка с член 11-2 от правилата на КЗЛИ, предвижда няколко изключения от това правило за предоставяне на съгласие. Освен това, съгласно член 24, същите дерогации като тези, приложими по член 23, параграф 1 от ЗЗЛИ, се прилагат и по отношение на международното предаване на данни ([46]).

(78) С цел да се осигури приемственост в защитата на личните данни, предавани от Европейския съюз на Япония съгласно настоящото решение, допълнително правило 4 увеличава нивото на защита на последващото предаване на такива данни от ССТЛИ към трета държава получател. Това се постига чрез ограничаване и рамкиране на основанията за международно предаване на данни, които могат да се използват от ССТЛИ като алтернатива на получаването на съгласие. По-специално и без да се засягат изключенията, посочени в член 23, параграф 1 от ЗЗЛИ, лични данни, предадени съгласно настоящото решение, могат да бъдат предмет на (по-нататъшно) предаване без предварително съгласие само в два случая: i) когато данните се изпращат в трета държава, която е била призната от КЗЛИ по силата на член 24 от ЗЗЛИ като осигуряваща еквивалентно ниво на защита на това, което се гарантира в Япония ([47]); или ii) когато ССТЛИ и третата страна — получател заедно са въвели мерки, осигуряващи ниво на защита, еквивалентно на предвиденото в ЗЗЛИ, четен във връзка с допълнителните правила, по силата на договор, други форми на обвързващи споразумения или договорености в рамките на дадена корпоративна група. Втората категория съответства на инструментите, използвани съгласно Регламент (ЕС) 2016/679, с цел да се осигурят подходящи гаранции (по-специално, стандартни договорни клаузи и задължителни корпоративни правила). Освен това, както бе потвърдено от КЗЛИ, дори в тези случаи предаването на лични данни остава подчинено на общите правила, приложими към всяко предоставяне на лични данни на трета страна по ЗЗЛИ (т.е. изискването за получаване на съгласие по член 23, параграф 1 или, алтернативно, изискването за предоставяне на информация с възможността за изключение по член 23, параграф 2 от ЗЗЛИ). В случай че със субекта на данни не може да бъде

([43]) Според данните, публикувани на уебсайта PrivacyMark на ЯЦОИИР към 2 октомври 2017 г.

([44]) КЗЛИ, Списък на акредитираните организации за защита на личната информация, достъпен на следния интернет адрес: https://www.ppc.go.jp/personal/nintei/list/ or https://www.ppc.go.jp/files/pdf/nintei_list.pdf

([45]) КЗЛИ, „Преглед на степента на изпълнение на ЗЗЛИ през финансовата 2015 г.“ (октомври 2016 г.), наличен (само на японски език) на интернет адрес: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

([46]) Вж. бележка под линия 32.

([47]) Съгласно член 11 от правилата на КЗЛИ, това изисква не само ефективното наблюдение от независим контролен орган на материалноправните стандарти, равностойни на ЗЗЛИ, но и гарантирането, че съответните правила се прилагат в третата държава.

установен контакт, за да бъде поискано неговото съгласие или за да му се предостави изискваната предварителна информация съгласно член 23, параграф 2 от ЗЗЛИ, предаването не може да се осъществи.

(79) Следователно, извън случаите, в които КЗЛИ е установила, че въпросната трета държава осигурява ниво на защита, което е равностойно на гарантираното от ЗЗЛИ ([48]), изискванията, установени в допълнително правило 4, изключват използването на инструменти за предаване, които не създават обвързващи отношения между японския износител на данни и вносителя на данни на третата държава и които не гарантират изискваното ниво на защита. Такъв е случаят, например, на системата за трансгранични правила за защита на неприкосновеността на личния живот (ТПЗНЛЖ) на държавите от АТИС, в която Япония е участваща икономика ([49]), тъй като в тази система защитата не е резултат от обвързващо споразумение между износителя и вносителя в контекста на двустранните им отношения и тази защита очевидно е на по-ниско ниво от гарантираното от ЗЗЛИ и допълнителните правила ([50]).

(80) И накрая, още една гаранция в случай на (по-нататъшно) предаване произтича от членове 20 и 22 от ЗЗЛИ. Съгласно тези разпоредби, когато оператор на трета държава (вносителят на данни) действа от името на ССТЛИ (износителя на данни), като подизпълнител, последният трябва да гарантира надзор над първия що се отнася до сигурността на обработването на данни.

2.3.10. *Индивидуални права*

(81) Подобно на законодателството на ЕС за защита на данните, ЗЗЛИ предоставя на физическите лица редица права, които подлежат на изпълнение. Това включва правото на достъп („разкриване“), коригиране и заличаване, както и правото на възражение („прекратяване на употребата“).

(82) Първо, съгласно член 28, параграфи 1 и 2 от ЗЗЛИ субектът на данни има право да поиска от ССТЛИ да „разкрие запазени лични данни, които могат да го идентифицират“ и, след получаване на такова искане, ССТЛИ „трябва […] да разкрие запазените лични данни“ на субекта на данните. Член 29 (право на поправяне) и член 30 (право на прекратяване на употребата) имат същата структура като член 28.

(83) В член 9 от Постановлението на Министерски съвет се предвижда, че разкриването на лична информация, както е посочено в член 28, параграф 2 от ЗЗЛИ, се извършва в писмена форма, освен ако ССТЛИ и субектът на данните не са договорили друго.

(84) Тези права са предмет на три типа ограничения, свързани със собствените права на лицето или правата и интересите на трети страни ([51]), сериозно засягане на стопанските операции на ССТЛИ ([52]), както и случаи, в които разкриването на информацията би нарушило други законови или подзаконови разпоредби ([53]). Случаите, в които тези ограничения биха се прилагали, са аналогични на някои от изключенията, приложими съгласно член 23, параграф 1 от Регламент (ЕС) 2016/679, който позволява ограничения на правата на физическите лица по причини, свързани със „защитата на субекта на данните или на правата и свободите на други лица“ или „други важни цели от

([48]) До този момент КЗЛИ все още не е приела никакво решение съгласно член 24 от ЗЗЛИ, с което се признава, че трета държава осигурява ниво на защита, което е равностойно на нивото, гарантирано в Япония. Единственото решение, чието приемане тя предвижда понастоящем, се отнася до ЕИП. Що се отнася до други възможни решения в бъдеще, Комисията ще следи отблизо ситуацията и, ако е необходимо, ще предприеме подходящи мерки за справяне с възможни неблагоприятни последици за непрекъснатостта на защитата (вж. по-долу съображения 176, 177, 184 и член 3, параграф 1).

([49]) Въпреки че само две японски дружества са сертифицирани по тази система на АТИС (вж. https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Извън територията на Япония, единствените други стопански субекти, които са сертифицирани по тази система са малък брой (23) дружества в САЩ (вж. https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Например, няма дефиниция и специални мерки за защита на чувствителните данни, няма задължение за ограничено запазване на данни. Вж. също Работна група по член 29, Становище 02/2014 относно референтен документ за изискванията към задължителните фирмени правила, представени на националните органи по защита на данните в ЕС, и към трансграничните правила за защита на неприкосновеността на личния живот, представени на отговорниците по отчетността на АТИС в сферата на ТПЗНЛЖ, 6 март 2014 г.

([51]) Според КЗЛИ, само такъв тип интереси може да обоснове ограничение, което „следва да бъде правно защитено“. Тази оценка се извършва за всеки отделен случай „като се вземе предвид нарушаването на основното право на неприкосновеност на личния живот, включително защита на личните данни, както са признати от Конституцията и съдебната практика.“ Защитените интереси могат например да включват търговски или други свързани с търговията тайни.

([52]) Понятието „сериозно нарушаване на изпълнението на дейността на субекта“ е пояснено в насоките на КЗЛИ чрез различни примери, например повтарящи се и идентични сложни искания, подадени от едно и също лице, когато тези искания представляват значителна тежест за стопанските субекти, която би навредила на способността им да отговорят на други искания (Насоки на КЗЛИ (General rule edition), стр. 62). В по-общ план КЗЛИ потвърди, че тази категория се ограничава до изключителни случаи, които надхвърлят обикновените неудобства. По-специално, ССТЛИ не може да отказва разкриване само защото се иска достъп до голям обем данни.

([53]) Както бе потвърдено от КЗЛИ, тези закони трябва да зачитат правото на неприкосновеност на личния живот, както е гарантирано от конституцията и следователно „да отразяват необходимо и разумно ограничение.“

широк обществен интерес“. Въпреки че категорията на случаите, в които разкриването на информация би нарушило „други законови или подзаконови разпоредби“ може да изглежда широка, законовите и подзаконовите разпоредби, предвиждащи ограничения в това отношение, трябва да спазват конституционното право на неприкосновеност на личния живот и могат да налагат ограничения само доколкото упражняването на това право би „накърнило общественото благо“ ([54]). Това изисква претегляне на наличните интереси.

(85) Съгласно член 28, параграф 3 от ЗЗЛИ, ако поисканите данни не съществуват или когато съответният ССТЛИ реши да не предостави достъп до запазените данни, той е длъжен да информира засегнатото лице без забавяне.

(86) От друга страна, съгласно член 29, параграфи 1 и 2 от ЗЗЛИ, субектът на данните има право да поиска коригиране, допълване или заличаване на своите запазени лични данни, в случай че данните са неточни. При получаване на такова искане, ССТЛИ „[…] провежда необходимото разследване“ и въз основа на резултатите от това разследване „прави поправка и т.н. на съдържанието на запазените данни“.

(87) Трето, съгласно член 30, параграфи 1 и 2 от ЗЗЛИ субектът на данни има право да поиска от ССТЛИ да преустанови употребата на лична информация или да поиска нейното заличаване, когато тя се третира в нарушение на член 16 (относно принципа на ограничаване до предвидената цел) или е била придобита неправомерно в нарушение на член 17 от ЗЗЛИ (относно придобиването чрез измама, други непозволени средства или, в случай на чувствителни данни — без необходимото съгласие). По подобен начин, съгласно член 30, параграфи 3 и 4 от ЗЗЛИ, лицето има право да изиска от ССТЛИ да преустанови предоставянето на информацията на трета страна, когато това би нарушило разпоредбите на член 23, параграф 1 или член 24 от ЗЗЛИ (относно предоставянето на трета страна, включително международното предаване на данни).

(88) Когато искането е основателно, ССТЛИ незабавно да прекратява употребата на данните или предоставянето им на трета страна, доколкото това е необходимо, за да се отстрани нарушението или, ако случаят е предмет на изключение (по-специално ако използването би довело до особено високи разходи) ([55]) прилага необходимите алтернативни мерки, с които да се защитят правата и интересите на съответното лице.

(89) За разлика от правото на ЕС, в ЗЗЛИ и съответните подзаконови актове не се съдържат правни разпоредби, които конкретно да третират възможността за възражение срещу обработване за целите на директния маркетинг. Това обработване обаче, по силата на настоящото решение, ще се осъществи в контекста на предаването на лични данни, които преди това са били събрани в Европейския съюз. Съгласно член 21, параграф 2 от Регламент (ЕС) 2016/679 субектът на данните следва винаги да има възможността да възрази срещу предаването на данни за обработване за целите на директния маркетинг. Освен това, както е обяснено в съображение 43, съгласно Допълнително правило 3, от ССТЛИ се изисква да обработва данните, получени по силата на решението, за същата цел, за която данните са били предадени от Европейския съюз, освен ако субектът на данните не даде съгласието си за промяна на целта на употреба. Ето защо ако предаването е извършено с каквато и да е друга цел, различна от директния маркетинг, ССТЛИ в Япония, няма да може да обработва данните за целите на директния маркетинг без съгласието на субекта на данните от ЕС.

(90) Във всички случаи, посочени в членове 28 и 29 от ЗЗЛИ, от ССТЛИ се изисква да уведоми незабавно лицето за резултата от неговото искане и освен това да обясни всеки (частичен) отказ въз основа на законовите изключения, предвидени в членове 27—30 (член 31 от ЗЗЛИ).

([54]) Член 13 от Конституцията е тълкуван от Върховния съд като предвиждащ право на неприкосновеност на личния живот (вж. по-горе в съображения 7 и 8). Въпреки че това право може да бъде ограничено в случаите, когато то „накърнява общественото благо“, в решението си от 6 март 2008 г. (вж. съображение 8) Върховният съд поясни, че всяко ограничение (което позволява в случая публичен орган да събира и обработва лични данни), трябва да бъде балансирано спрямо правото на неприкосновеност на личния живот, като се вземат предвид фактори като естеството на данните, за които става въпрос, рисковете, които обработването на тези данни създава за лицата, приложимите гаранции и ползите за обществения интерес в резултат на обработването. Това е подобно на вида на балансиране, изисквано по правото на ЕС, въз основа на принципите на необходимост и пропорционалност, за разрешаване на всякакви ограничения на правата и гаранциите за защита на данните.

([55]) За допълнителни разяснения относно изключенията, вж. проф. Katsuya Uga, коментари член по член на преразгледания Закон за защита на личната информация, 2015 г., стр. 217. Например, пример за искане, водещо до „особено високи разходи“ е случаят, в който някои от имената в дълъг списък (напр. в указател) се обработват в нарушение на принципа за ограничаване в рамките на целта и указателят е вече на пазара, вследствие на което изземването на тези копия и заместването им с нови би било много скъпо. В същия пример, когато копия на указателя са били вече продадени на много хора и не е възможно всички те да бъдат иззети, ще бъде трудно също да се „преустанови употребата“. В тези сценарии „необходимите алтернативни действия“ биха могли да включват, например, публикуване или разпространение на обявление за корекция. Такова действие не изключва други форми на (съдебна) защита във връзка с нарушение на правата, свързани с неприкосновеността на личния живот, увреждане на репутацията (клевета), причинено от публикуването, или накърняване на други интереси.

(91) Що се отнася до условията за отправяне на искане, член 32 от ЗЗЛИ (заедно с постановлението на Министерски съвет) позволява на ССТЛИ да определи разумни процедури, включително по отношение на информацията, необходима за идентифициране на запазените лични данни. Въпреки това, съгласно параграф 4 от този член ССТЛИ не трябва да налагат „прекомерна тежест на субекта на данни“. В определени случаи ССТЛИ може също да налага такси, стига стойността им да остава „в рамките на обхвата, считан за подходящ, с оглед на реалните разходи“ (член 33 от ЗЗЛИ).

(92) На последно място, лицата могат да възразят срещу предоставянето на тяхната лична информация на трета страна по смисъла на член 23, параграф 2 от ЗЗЛИ, или да откажат да дадат съгласието си по член 23, параграф 1 (като по този начин се предотвратява разкриване в случай, че няма друго правно основание). По същия начин лицата могат да прекъснат обработването на данни за различна цел като откажат да дадат съгласие в съответствие с член 16, параграф 1 от ЗЗЛИ.

(93) За разлика от правото на ЕС ЗЗЛИ и съответните подзаконови актове не съдържат общи разпоредби, уреждащи въпроса за решенията, засягащи субекта на данни и основаващи се единствено на автоматизираното обработване на лични данни. Този въпрос обаче се разглежда в някои секторни правила, приложими в Япония, които са особено релевантни за този вид обработване на данни. Това включва секторите, в които е най-вероятно дружествата да прибягват до автоматизирано обработване на личните данни с цел вземане на решения, засягащи физическите лица (напр. финансовия сектор). Така например „Цялостните насоки за надзора над големите банки“, преработени през юни 2017 г., изискват на засегнатото лице да бъдат предоставени специални обяснения относно причините за отхвърляне на молбата за сключване на договора за заем. Следователно с тези правила се предлага защита в по-скоро ограничения брой на случаите, в които автоматизираните решения биха били взети от „внасящия“ японски стопански субект (вместо от „изнасящия“ администратор на данни от ЕС).

(94) Във всеки случай, що се отнася до лични данни, които са били събрани в Европейския съюз, всяко решение, основано 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 ([56]). Това включва сценарии за предаване, в които обработката се извършва от чужд (напр. японски) стопански субект, действащ като представител (обработващ лични данни) на администратора на данни на ЕС (или като подизпълнител, действащ от името на обработващ лични данни от ЕС, който е получил данните от администратора на данни от ЕС, който ги е събрал), който на това основание впоследствие взема решението. Следователно, липсата на конкретни правила относно автоматизираното вземане на решения в ЗЗЛИ е малко вероятно да се отрази върху равнището на защита на личните данни, предавани съгласно настоящото решение.

2.4. **Надзор и изпълнение**

2.4.1. *Независим надзор*

(95) С цел да се гарантира, че адекватното ниво на защита на данните се осигурява и на практика, следва да съществува 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.

(96) В Япония, органът, който отговаря за наблюдението и изпълнението на ЗЗЛИ е КЗЛИ. КЗЛИ се състои от председател и осем комисари, назначени от министър-председателя със съгласието на двете камари на парламента. Мандатът на председателя и на всеки от комисарите е пет години, с възможност за удължаване (член 64 от ЗЗЛИ). Комисарите могат да бъдат освобождавани от длъжност само при наличие на основателна причина при ограничен брой извънредни обстоятелства ([57]) и не трябва да бъдат активно ангажирани с политически дейности. Освен това съгласно ЗЗЛИ членовете на Комисията, работещи на пълно работно време, трябва да се въздържат от всякакви други дейности срещу заплащане или стопански дейности. Всички членове на Комисията също така се подчиняват на вътрешни правила, които възпрепятстват тяхното участие в обсъжданията в случай на възможен конфликт на интереси. КЗЛИ се подпомага от секретариат, ръководен от генерален секретар, който е създаден за целите на изпълняването на задачите, възложени на КЗЛИ (член 70 от ЗЗЛИ). Комисарите и всички служители в секретариата са обвързани от строги правила за конфиденциалност (членове 72, 82 от ЗЗЛИ).

([56]) Обратно, в изключителния случай, в който японският оператор е в пряка връзка със субекта на данни от ЕС, това обикновено ще е резултат от това, че операторът е насочил дейността си към лице в Европейския съюз, предлагайки му стоки или услуги или наблюдавайки неговото поведение. При този сценарий самият японски оператор 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.

([57]) Съгласно член 65 от ЗЗЛИ, освобождаване от длъжност против волята на съответния комисар е възможно единствено на едно от следните основания: i) откриване производство по несъстоятелност; ii) осъждане за нарушение на ЗЗЛИ или Закона за използване на числата; iii) осъждане на лишаване от свобода без задължително полагане на труд или дори още по-тежка присъда; iv) неспособност да изпълнява служебните си задължения поради психично или физическо заболяване или нарушение.

(97) Правомощията на КЗЛИ, които тя упражнява напълно независимо ([58]), са предвидени основно в членове 40, 41 и 42 от ЗЗЛИ. Съгласно член 40 КЗЛИ може да поиска от ССТЛИ да докладват или да представят документи относно операции по обработване и може също така да извършва инспекции, както на място, така и на регистри или други документи. Доколкото е необходимо за изпълнението на ЗЗЛИ, КЗЛИ може също така да дава насоки или съвети на ССТЛИ по отношение на обработването на лична информация. КЗЛИ вече използва това правомощие съгласно член 41 от ЗЗЛИ, като отправи насоки до Facebook след разкритията по случая Facebook Cambridge Analytica.

(98) По-важното е, че в отделни случаи КЗЛИ притежава правомощия — действайки по жалба или по собствена инициатива — да издава препоръки и нареждания в индивидуални случаи с цел изпълнение на ЗЗЛИ и други задължителни правила (включително допълнителните правила). Тези правомощия са предвидени в член 42 от ЗЗЛИ. Параграфи 1 и 2 от посочения член предвиждат двуетапен механизъм, чрез който КЗЛИ може да издаде нареждане (само) след като преди това е издала препоръка, а параграф 3 дава възможност за пряко издаване на нареждания в спешни случаи.

(99) Въпреки че не всички разпоредби на глава IV, раздел 1 от ЗЗЛИ са изброени в член 42, параграф 1, който също определя приложното поле на член 42, параграф 2, това може да се обясни с факта, че някои от тези разпоредби не засягат задълженията на ССТЛИ ([59]) и че всички основни гаранции за защита вече са предоставени чрез други разпоредби, които са включени в този списък. Например, въпреки че член 15 (изискващ от ССТЛИ да определи целта на употреба и да обработва съответната лична информация изключително в обхвата на тази цел) не се споменава, неспазването на това изискване може да даде основание за препоръка, основана на нарушение на член 16, параграф 1 (забрана на ССТЛИ да обработва лична информация извън необходимото за постигане целите на употреба, освен ако не е получил съгласието на субекта на данните) ([60]). Друга разпоредба, която не е посочена в член 42, параграф 1, е член 19 от ЗЗЛИ относно точността и запазването на данните. Неспазването на тази разпоредба може да бъде отчетено или като нарушение на член 16, параграф 1, или като нарушение на член 29, параграф 2, ако съответното лице отправи искане за поправяне или заличаване на неверни или прекомерни по отношение на целите данни и ССТЛИ откаже да удовлетвори това искане. По отношение на правата на субекта на данни съгласно член 28, параграф 1, член 29, параграф 1 и член 30, параграф 1 надзорът от страна на КЗЛИ се осигурява, като ѝ се предоставят изпълнителни правомощия по отношение на съответните задължения на ССТЛИ, предвидени в тези членове.

(100) Съгласно член 42, параграф 1 от ЗЗЛИ, КЗЛИ може, ако смята, че съществува „необходимост за защита на правата и интересите на дадено лице в случаите, когато [ССТЛИ] е нарушил“ конкретни разпоредби от ЗЗЛИ, да издаде препоръка „за спиране на извършването на нарушението или за предприемане на други необходими действия за коригиране на нарушението“. Тази препоръка не е задължителна, но отваря пътя за издаване на задължително нареждане съгласно член 42, параграф 2 от ЗЗЛИ. Въз основа на тази разпоредба, ако препоръката не бъде изпълнена „без да е налице законно основание“ и КЗЛИ „смята, че има непосредствена опасност от извършване на сериозно нарушение на правата и интересите на дадено лице“, тя може да разпореди с нареждане ССТЛИ да предприеме действия за изпълнение на препоръката.

(101) Допълнителните правила доизясняват и укрепват изпълнителните правомощия на КЗЛИ. По-специално, в случаи, отнасящи се до данни, внесени от Европейския съюз, КЗЛИ винаги ще счита, че непредприемането на действия от ССТЛИ за изпълнение на препоръка, издадена на основание член 42, параграф 1 от ЗЗЛИ, без да има законно основание за неизпълнението, представлява тежко нарушение с непосредствено отражение върху правата и интересите на дадено лице по смисъла на член 42, параграф 2 и следователно е нарушение, за което се изисква издаването на правнообвързващо нареждане. Освен това като „законно основание“ за несъобразяване с дадена препоръка КЗЛИ ще приема само „събитие от извънреден характер [пречещо на спазването] извън контрола на [ССТЛИ], което не може да бъде разумно предвидено (например природни бедствия)“ или случаи, в които необходимостта да се предприемат действия във връзка с дадена препоръка „е отпаднала поради предприемането на алтернативни действия [от страна на ССТЛИ], които напълно отстраняват нарушението“.

([58]) Вж. член 62 от ЗЗЛИ.

([59]) Например, някои разпоредби се отнасят до действия на ССТЛИ, които не са задължителни (членове 32 и 33 от ЗЗЛИ), или задължения за полагане на „максимални усилия“, които,като такива, не подлежат на принудително изпълнение (член 31, член 35, член 36, параграф 6 и член 39 от ЗЗЛИ). Някои разпоредби не са адресирани до ССТЛИ, а до други участници. Такъв е случаят, например, с оглед на член 23, параграф 4, член 26, параграф 2 и член 34 от ЗЗЛИ (спазването на член 26, параграф 2 от ЗЗЛИ обаче се осигурява чрез възможността за налагане на наказателноправни санкции съгласно член 88, подточка i) от ЗЗЛИ).

([60]) Освен това, както бе обяснено по-горе в съображение 48, в контекст на предаване на лична информация „целта на употреба“ ще бъде определена от износителя на данни в ЕС, който в това отношение е обвързан от задължението по член 5, параграф 1, буква б) от Регламент (ЕС) 2016/679. Изпълнението на това задължение се следи от компетентния орган за защита на данните в Европейския съюз.

(102) Съгласно член 84 от ЗЗЛИ неспазването на нареждане на КЗЛИ се счита за престъпление и ССТЛИ, който е признат за виновен, може да бъде наказан с лишаване от свобода със задължително полагане на труд за максимален срок от шест месеца или с глоба от максимум 300 000 йени. Освен това, съгласно член 85, буква и) от ЗЗЛИ липсата на сътрудничество с КЗЛИ или възпрепятстване на нейното разследване се наказва с глоба от максимум 300 000 йени. Тези наказателноправни санкции се прилагат в допълнение към тези, които могат да бъдат наложени за нарушения по същество на ЗЗЛИ (вж. съображение 108).

2.4.2. *Защита по съдебен ред*

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

(104) Преди или вместо да се възползва от административни или съдебни средства за защита, дадено лице може да реши да подаде жалба относно обработката на неговите лични данни до самия администратор. Въз основа на член 35 от ЗЗЛИ, ССТЛИ се стремят да разглеждат такива жалби „адекватно и своевременно“ и да въведат вътрешни системи за разглеждане жалби с тази цел. Освен това съгласно член 61, подточка ii) от ЗЗЛИ КЗЛИ отговаря за „необходимата медиация по подадена жалба и сътрудничество, които се предлагат на стопанския оператор, който се занимава с жалбата“, което и в двата случая включва жалби, подадени от чужденци. В това отношение японският законодател е поставил на правителството задачата да предприема „необходимите действия“, за да се осигури възможност за подаване на жалби и да се улесни вземането на решения по тях от ССТЛИ (член 9), докато местните власти в такива случаи се стремят да осигурят медиация (член 13). В това отношение физическите лица могат да подадат жалба до един от над 1 700 потребителски центрове, създадени от местните власти, въз основа на Закона за безопасност на потребителите ([61]), в допълнение към възможността за подаване на жалба до Националния център за потребителите на Япония. Такива жалби могат да се подават и във връзка с нарушение на ЗЗЛИ. По силата на член 19 от Основния закон за потребителите ([62]) местните власти се стремят да започнат медиация във връзка с жалбите и да предоставят на страните необходимия експертен опит. Тези механизми за разрешаване на спорове изглеждат доста ефективни, като процентът на разрешените случаи е 91,2 % за над 75 000 жалби през 2015 г.

(105) Нарушаването на разпоредбите на ЗЗЛИ от ССТЛИ може да доведе до граждански искове, както и до наказателни производства и и наказателноправни санкции. На първо място, ако дадено лице смята, че правата му по силата на членове 28, 29 и 30 от ЗЗЛИ са били нарушени, то може да потърси правна защита под формата на съдебна заповед, като поиска от съда да разпореди ССТЛИ да удовлетвори искането му по един от тези членове, тоест да разкрие запазени лични данни (член 28), да коригира запазени лични данни, които са грешни (член 29), или да преустанови незаконната обработка или предоставянето на данни на трети страни (член 30). Такъв иск може да бъде заведен без да е необходимо да се основава на член 709 от Гражданския кодекс ([63]) или на друго деликтно основание ([64]). По-специално това означава, че лицето не трябва да доказва причинена вреда.

(106) На второ място, когато предполагаемо нарушение не се отнася до индивидуални права по членове 28, 29 и 30, а до общите принципи на защита на данните или до задълженията на ССТЛИ, засегнатото лице може да заведе граждански иск срещу стопанския оператор въз основа на разпоредбите за непозволено увреждане на японския Граждански кодекс, по-специално член 709. При съдебно дело по член 709 се изисква доказване не само на наличието на вина (умисъл или небрежност), но и на настъпилата вреда, а съгласно член 710 от Гражданския кодекс тази вреда може да бъде както материална, така и нематериална. Не е наложено ограничение за размера на обезщетението.

(107) Що се отнася до достъпните видове защита, член 709 от японския Граждански кодекс предвижда парично обезщетение. Според тълкуването в японската съдебна практика обаче този член предоставя също така право на разпореждане за преустановяване на нарушение ([65]). „Следователно, ако субектът на данни предяви иск по член 709 от Гражданския кодекс и твърди, че неговите права или интереси са увредени вследствие на нарушение на разпоредба от ЗЗЛИ, извършено от ответника, претенцията може да включва, освен обезщетение за вреди, иск за преустановяване на нарушение, по-специално с цел спиране на всяко неправомерно обработване.

([61]) Закон № 50 от 5 юни 2009 г.
([62]) Закон № 60 от 22 август 2012 г.
([63]) Член 709 от Гражданския кодекс е основното правно основание за завеждане на граждански искове за обезщетение за вреди. Според тази разпоредба „лице, което умишлено или поради небрежност е нарушило права или законово защитени интереси на други лица, е длъжно да обезщети всички последвали вреди“.
([64]) Висш съд на Токио, решение от 20 май 2015 г. (непубликувано); Окръжен съд на Токио, решение от 8 септември 2014 г., Westlaw Japan 2014WLJPCA09088002. Вж. също член 34, параграфи 1 и 3 от ЗЗЛИ.
([65]) Вж. Върховен съд, решение от 24 септември 2002 г. (Hanrei Times, т. 1106, стр. 72).

(108) На трето място, в допълнение към средствата за защита по гражданското (деликтното) право, субектът на данните може да подаде жалба до прокурор или служител от съдебната полиция във връзка с нарушения на ЗЗЛИ, които могат да доведат до наказателноправни санкции. Глава VII от ЗЗЛИ съдържа редица наказателни разпоредби. Най-важната от тях (член 84) се отнася до неспазването от страна на ССТЛИ на нареждания на КЗЛИ съгласно член 42, параграфи 2 и 3. Ако стопански оператор не се подчини на нареждане на КЗЛИ, председателят на КЗЛИ (както и друго правителствено длъжностно лице) ([66]) може да препрати случая на прокурора или на служител от съдебната полиция и по този начин да задейства образуването на наказателно производство. Санкцията за нарушение на нареждането на КЗЛИ е лишаване от свобода със задължително полагане на труд за срок до шест месеца или глоба до 300 000 йени. Други разпоредби на ЗЗЛИ, предвиждащи санкции в случай на нарушения на ЗЗЛИ, засягащи правата и интересите на субектите на данни, са член 83 от ЗЗЛИ (относно „предоставянето или използването скришом“ на база данни с лична информация „с цел извличане на […] незаконни печалби“) и член 88, подточка i) от ЗЗЛИ (относно невъзможността на трета страна да предостави точна информация на ССТЛИ, когато той получава лични данни в съответствие с член 26, параграф 1 от ЗЗЛИ, по-специално относно подробностите около придобиването от третата страна на тези данни). Приложимите санкции за тези нарушения на ЗЗЛИ са съответно лишаване от свобода със задължително полагане на труд до една година или глоба в размер до 500 000 йени (за нарушение по член 83) или административна глоба в размер до 100 000 йени (за нарушение по член 88, подточка i)). Въпреки че самата заплаха от наказателноправна санкция вероятно оказва силно възпиращо въздействие върху управителните органи, ръководещи операциите за обработка на ССТЛИ, както и върху лицата, третиращи данните, член 87 от ЗЗЛИ уточнява, че когато представител, работник или друг служител на юридически субект е извършил нарушение по членове 83—85 от ЗЗЛИ, „това лице се наказва и на въпросния юридически субект се налага глобата, предвидена в съответните членове“. В този случай както на служителя, така и на дружеството може да бъдат наложени санкции до пълния максимален размер.

(109) И накрая, физическите лица могат да търсят правна защита срещу действия или бездействия на КЗЛИ. В това отношение японският закон предвижда няколко възможности за административна и съдебна защита.

(110) Ако дадено лице не е удовлетворено от действията, предприети от КЗЛИ, то може да подаде жалба по административен ред по реда, предвиден в Закона за административното обжалване ([67]). И обратно, когато дадено лице смята, че КЗЛИ е трябвало да предприеме действия, но не го е направила, то може, съгласно член 36-3 от посочения закон, да поиска от КЗЛИ да се разпореди или да предостави административни насоки, ако лицето смята, че „не е било дадено разпореждане или не са били предоставени необходимите административни насоки за коригирането на нарушението“.

(111) Що се отнася до съдебната правна защита, съгласно Закона за административното съдопроизводство лице, което не е удовлетворено от административно разпореждане на КЗЛИ, може да подаде *mandamus* иск ([68]), с който да поиска от съда да нареди на КЗЛИ да предприеме по-нататъшни действия ([69]). В някои случаи съдът може да издаде временно постановление за *mandamus*, така че да се предотврати настъпването на необратими вреди ([70]). Освен това съгласно същия закон физическо лице може да поиска отмяна на решение на КЗЛИ ([71]).

(112) Накрая, дадено лице може да подаде иск за държавно обезщетение срещу КЗЛИ по силата на член 1, параграф 1 от Закона за обезщетенията, дължими от държавата, в случай че е претърпяло вреди вследствие на незаконосъобразно нареждане на КЗЛИ, адресирано до стопански оператор, или защото КЗЛИ не е упражнила правомощията си.

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

(113) Комисията извърши също така оценка на ограниченията и гаранциите, включително на предвидените от японското законодателство механизми за надзор и индивидуална правна защита във връзка със събирането и последващото използване на лични данни, предадени на стопански субекти в Япония от публичните органи за цели от обществен интерес, и по-специално за целите на наказателното правоприлагане и националната сигурност („достъп на държавните органи“). В това отношение японското 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.

([66]) Член 239, параграф 2 от Наказателнопроцесуалния кодекс.
([67]) Закон № 160 от 2014 г.
([68]) Член 37-2 от Закона за административното съдопроизводство.
([69]) Съгласно член 3, параграф 6 от Закона за административното съдопроизводство понятието „mandamus иск“ означава иск, с който от съда се иска да разпореди на административен орган да извърши изначално административно действие или да даде административно разпореждане, което е трябвало да извърши или даде, но не го е направил.
([70]) Член 37-5 от Закона за административното съдопроизводство.
([71]) Глава II, раздел 1 от Закона за административното съдопроизводство.

3.1. **Обща правна уредба**

(114) Тъй като представлява израз на упражняване на публична власт, достъпът на държавните органи в Япония трябва да се осъществява при пълно зачитане на закона (принцип за законност). Във връзка с това Конституцията на Япония съдържа разпоредби, ограничаващи и регулиращи събирането на лични данни от публичните органи. Както вече бе посочено по отношение на обработката от стопански субекти, като се основава на член 13 от Конституцията, който наред с другото защитава правото на свобода, Върховният съд на Япония признава правото на неприкосновеност на личния живот и защита на данните ([72]). Един от важните аспекти на това право е свободата личната информация на лицата да не се разкрива на трети страни без разрешение ([73]). Това предполага право на ефективна защита на личните данни срещу злоупотреби и (по-специално) срещу неправомерен достъп. Допълнителна защита се гарантира от член 35 от Конституцията, отнасящ се до правото на всички лица да бъдат сигурни в домовете си и по отношение на вещите и документите си, което налага на публичните органи да получат съдебна заповед, издадена въз основа на „достатъчен повод“ ([74]) във всички случаи на „претърсване и изземване“. В решението си от 15 март 2017 г. по делото GPS Върховният съд е пояснил, че това изискване за получаване на съдебна заповед се прилага във всички случаи, когато държавните органи посягат на („навлизат в“) сферата на личния живот по начин, който потиска волята на индивида, и съответно чрез способи за „задължително разследване“. Съдия може да издаде такава заповед единствено въз основа на конкретни подозрения за престъпления, т.е. когато са му предоставени писмени доказателства, въз основа на които лицето, засегнато от разследването, може да се разглежда като извършило престъпление ([75]). Следователно японските органи нямат законово право да събират лична информация чрез задължителни средства в ситуации, когато все още няма нарушение на закона ([76]), например за да се предотврати престъпление или друга заплаха за сигурността (какъвто е случаят за разследвания по съображения, свързани с националната сигурност).

(115) Според принципа за законност всяко събиране на данни като част от принудително разследване трябва да бъде изрично разрешено от закона (както е отразено например в член 197, параграф 1 от Наказателнопроцесуалния кодекс (НПК) относно задължителното събиране на информация за целите на наказателни разследвания). Това изискване се прилага и за достъпа до информация в електронна форма.

(116) Важно е, че член 21, параграф 2 от Конституцията гарантира поверителността на съобщенията чрез всички средства за комуникация, като ограничения в това отношение се допускат единствено в предвидените от закона случаи по съображения от обществен интерес. Член 4 от Закона за далекосъобщенията, според който поверителността на съобщенията, третирани от телекомуникационна компания, не може да се нарушава, въвежда изискването за поверителност на законодателно равнище. Това се тълкува в смисъл, че се забранява разкриването на информацията, съдържаща се в съобщенията, освен при наличие на съгласието на ползвателите или ако се основава на едно от изричните изключения от наказателна отговорност, предвидени в Наказателния кодекс ([77]).

(117) Освен това Конституцията гарантира правото на достъп до съд (член 32) и правото да се иска обезщетение от държавата за вреди, претърпени от физическо лице вследствие на незаконосъобразен акт на публично длъжностно лице (член 17).

(118) Що се отнася по-специално до правото на защита на данните, глава III, раздели 1, 2 и 3 на ЗЗЛИ установяват общи принципи, които се отнасят за всички сектори — включително и публичния сектор. По-специално, член 3 от ЗЗЛИ предвижда, че личната информация трябва да се обработва в съответствие с принципа на зачитане на личността на лицата. След като лична информация, включително като част от електронни записи, е била събрана („получена“) от публични органи ([78]), нейната обработка се урежда от Закона за защита на лична информация, съхранявана от

([72]) Вж. например решение на Върховния съд от 12 септември 2003 г. по дело № 1656 (2002 (Ju). По-специално Върховният съд е постановил, че „всеки разполага със свободата да защитава своята лична информация от това тя да бъде разкрита на трета страна или да бъде направена обществено достояние без основателна причина.“

([73]) Решение от 6 март 2008 г. на Върховния съд (Juki-net).

([74]) „Достатъчен повод“ съществува само когато се счита, че съответното лице (заподозряно, обвиняемо) е извършило престъпление и претърсването и изземването са необходими за целите на наказателното разследване. Вж. решение на Върховния съд от 18 март 1969 г. по дело № 100, (1968 (Shi).

([75]) Вж. член 156, параграф 1 от Наказателнопроцесуалния кодекс.

([76]) Следва обаче да се отбележи, че Законът за наказване на организираната престъпна дейност и контрол на облагите от престъпна дейност от 15 юни 2017 г. създава ново престъпление, криминализиращо подготовката на терористични актове и някои други форми на организирана престъпност. Разследвания могат да бъдат започнати само при наличие на конкретни подозрения, основани на доказателства, че трите необходими условия, съставляващи престъплението (участие в организирана престъпна група, „действия по планиране“ и „действия по подготовка за изпълнение“ на престъплението), са изпълнени. Вж. също например членове 38—40 от Закона за предотвратяване на подривни дейности (Закон № 240 от 21 юли 1952 г.).

([77]) Член 15, параграф 8 от Насоките относно защитата на личната информация в телекомуникационния сектор.

([78]) Административни органи, както са определени в член 2, параграф 1 от ЗЗЛИСАО. Според информацията, получена от японското правителство, всички публични органи, с изключение на полицията на префектурите, попадат в обхвата на определението за „административни органи“. В същото време, полицията на префектурата функционира съгласно правната уредба, очертана от наредбите на префектурите за защита на личните данни (вж. член 11 от ЗЗЛИ и основната политика), които предвиждат разпоредби за защита на личната информация, еквивалентни на ЗЗЛИСАО. Вж. приложение II, раздел I, буква Б. Както беше обяснено от КЗЛИ, според „Основната политика“ тези наредби трябва да бъдат приети въз основа на съдържанието на ЗЗЛИСАО и МВРС издава обявления за предоставяне на местните власти на необходимите насоки в това отношение. Както беше подчертано от КЗЛИ, „[в] тези рамки се създава наредбата за защита на личната информация във всяка префектура […] въз основа на основната политика и съдържанието на обявленията.“

административни органи („ЗЗЛИСАО“) ([79]). Това включва по принцип ([80]) и обработването на лична информация за целите на наказателното правоприлагане или националната сигурност. Наред с другото, ЗЗЛИСАО предвижда, че публичните органи: i) могат да задържат лична информация само доколкото това е необходимо за изпълнението на задълженията им; ii) не могат да използват такава информация за „несправедливи“ цели или не могат да я разкриват пред трета страна без основателна причина; iii) посочват целта на обработката и не променят тази цел извън това, което разумно може да се счита за свързано с първоначалната цел (ограничаване на целта); iv) по принцип не използват или не предоставят на трета страна задържаните лични данни за други цели и, ако счетат за необходимо, налагат ограничения на целта или метода на употреба на трети страни; v) стремят се да гарантират достоверността на информацията (качество на данните); vi) предприемат необходимите мерки за правилното управление на информацията и за предотвратяване на изтичане на информация, загуби или щети (сигурност на данните); и vii) полагат усилия за правилното и експедитивното обработване на жалби във връзка с обработката на информацията ([81]).

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

(119) Японското законодателство съдържа редица ограничения по отношение на достъпа и използването на лични данни за целите на наказателното правоприлагане, както и механизми за надзор и правна защита, които осигуряват достатъчно гаранции за данните, които трябва да бъдат ефективно защитени срещу незаконна намеса и риск от злоупотреби.

3.2.1. *Правно основание и приложими ограничения/гаранции*

(120) Според японската правна уредба събирането на информация в електронна форма за целите на наказателното правоприлагане е допустимо въз основа на заповед (принудително събиране) или искане за доброволно разкриване.

3.2.1.1. Задължително разследване въз основа на съдебна заповед

(121) Както е посочено в съображение 115, всяко събиране на данни като част от принудително разследване трябва да бъде изрично разрешено от закона и може да се извършва само въз основа на съдебна заповед, издадена въз основа на „достатъчен повод“ (член 35 от Конституцията). По отношение на разследването на престъпления, това изискване е отразено в разпоредбите на Наказателнопроцесуалния кодекс (НПК). Съгласно член 197, параграф 1 от НПК, принудителните мерки „не се прилагат, освен ако в настоящия кодекс не са предвидени специални разпоредби“. По отношение на събирането на информация в електронна форма единствените подходящи ([82]) правни основания са член 218 от НПК (претърсване и изземване) и член 222-2 от НПК, съгласно който принудителни мерки за прихващане на електронни съобщения без съгласието на всяка от страните се прилагат въз основа на други актове, а именно Закона за подслушване за целите на наказателното разследване („Законът за подслушването“). И в двата случая се прилага изискването за съдебна заповед.

(122) По-конкретно, съгласно член 218, параграф 1 от НПК прокурор, помощник прокурор или служител на съдебната полиция може, ако това е необходимо за разследването на престъплението, да извърши претърсване или изземване (включително на записи) въз основа на заповед, издадена предварително от съдия ([83]). Наред с другото, в такава заповед се посочват името на заподозрения или обвиняемия, разследваното престъпление, за което е обвинен ([84]), електромагнитната документация, която трябва да бъде иззета, и „мястото или вещите“, които трябва да бъдат проверени (член 219, параграф 1 от НПК).

([79]) Личната информация, събрана от служители на административен орган при упражняването на техните функции и съхранявана от споменатия административен орган за организационна употреба, попада в определението за „задържана лична информация“ по смисъла на член 2, параграф 3 от ЗЗЛИСАО, стига това да е отразено в „административни документи“. Това включва информация в електронна форма, събирана и след това допълнително обработвана от такива органи, като се има предвид, че определението за „административни документи“ в член 2, параграф 2 от Закона за защита на личната информация, съхранявана от административни органи (Закон № 42 от 1999 г.) обхваща и електромагнитните записи.

([80]) Въпреки това, съгласно член 53-2 от Наказателнопроцесуалния кодекс глава IV от ЗЗЛИСАО не се прилага за „документи, свързани със съдебни дела“, като според получената информация това понятие включва информацията в електронна форма, получена въз основа на съдебна заповед или искане за доброволно съдействие като част от наказателно разследване. Също така, що се отнася до информацията, събирана в областта на националната сигурност, лицата няма да могат успешно да се позовават на правата си по ЗЗЛИСАО, ако ръководителят на публичния орган има „основателни причини“ да счита, че разкриването на информацията „има вероятност да навреди на националната сигурност“ (вж. член 14, точка iv)). При все това, от публичните органи се изисква да разрешават поне частично разкриване, когато е възможно (член 15).

([81]) Вж. конкретните позовавания на ЗЗЛИСАО в приложение II, раздел II, буква A, точка 1, буква б, подточка (2).

([82]) Макар че член 220 от НПК разрешава извършването на претърсвания и изземвания на място без съдебна заповед, ако прокурор, помощник прокурор или служител на съдебната полиция арестува заподозрян/хванат на местопрестъплението нарушител, същото не се прилага за случаите на предадени данни и следователно не е релевантно за целите на настоящото решение.

([83]) Съгласно член 222, параграф 1 във връзка с член 110 от НПК, заповедта за претърсване/изземване на записите трябва да бъде представена на лицето, срещу което е наложена мярката.

([84]) Вж. също член 189, параграф 2 от НПК, според който служителят на съдебната полиция разследва нарушителя и доказателствата „когато смята, че е било извършено престъпление“. По подобен начин член 155, параграф 1 от правилата за наказателното производство изисква в писменото искане за издаване на съдебна заповед да се посочва, наред с другото, „разследваното престъпление“ и „резюме на фактите по престъплението“.

(123) По отношение на прихващането на съобщения член 3 от Закона за подслушването разрешава такива мерки само при спазване на строги изисквания. По-специално, публичните органи трябва предварително да получат съдебна заповед, която може да бъде издадена само за разследването на конкретни тежки престъпления (изброени в приложението към Закона) ([85]) и когато е „изключително трудно да се идентифицира престъпника или да се изясни ситуацията/подробностите по извършването по какъвто и да е друг начин“ ([86]). Съгласно член 5 от Закона за подслушването съдебната заповед се издава за ограничен период от време като съдията може да налага допълнителни условия. Освен това Законът за подслушването предвижда редица допълнителни гаранции, като например задължителното присъствие на свидетели (членове 12 и 20), забраната за подслушване на съобщенията на някои привилегировани групи (напр. лекари, адвокати) (член 15), задължението за преустановяване на подслушването, ако то повече не е оправдано, дори посоченият в съдебната заповед срок да не е изтекъл (член 18), или общото изискване за уведомяване и предоставяне на достъп на засегнатото лице до направените записи в срок до тридесет дни след приключване на подслушването (членове 23 и 24).

(124) По отношение на всички принудителни мерки, основаващи се на съдебна заповед, може да се извършва само такава проверка, „каквато е необходима за постигането на нейната цел“ — тоест когато целите, преследвани с разследването, не могат да бъдат постигнати по друг начин (член 197, параграф 1 от НПК). Въпреки че критериите за определяне на необходимостта не са допълнително уточнени в закона, Върховният съд на Япония е постановил, че съдията, издаващ заповедта, следва да извърши цялостна оценка, като вземе предвид по-специално i) сериозността на престъплението и начина на извършването му; ii) стойността и значението на материалите, които трябва да бъдат иззети като доказателства; iii) вероятността (рискът) доказателствата могат да бъдат скрити или унищожени; и iv) степента, до която изземването може да навреди на засегнатото лице ([87]).

3.2.1.2. Искане за доброволно разкриване въз основа на „въпросник“

(125) В рамките на своята компетентност, публичните органи могат да събират и информация в електронна форма въз основа на исканията за доброволно разкриване. Това се отнася до незадължителна форма на сътрудничество, при която изпълнението на искането не може да бъде наложено принудително ([88]), с което публичните органи се освобождават от задължението за получаване на съдебна заповед.

(126) Доколкото това искане е насочено към стопански оператор и се отнася до лична информация, стопанският оператор трябва да спазва изискванията на ЗЗЛИ. Съгласно член 23, параграф 1 от ЗЗЛИ стопанските субекти могат да разкрият лична информация на трети страни без съгласието на съответното лице само в определени случаи, включително когато разкриването е „въз основа на законови и подзаконови актове“ ([89]). В областта на наказателното правоприлагане правното основание за такива искания е предвидено в член 197, параграф 2 от НПК, според който „от частни организации може да бъде поискано да предоставят информация по въпроси, свързани с разследването“. Тъй като подобен „въпросник“ е разрешен само като част от наказателно разследване, той винаги предполага наличието на конкретно подозрение за вече извършено престъпление ([90]). Освен това, тъй като такива разследвания обикновено се извършват от полицията на префектурата, се прилагат ограниченията съгласно член 2, параграф 2 от Закона за полицията ([91]). В съответствие с тази разпоредба, действията на полицията са „строго ограничени“ до изпълнението на техните отговорности и задължения (т.е. предотвратяването, противодействието и разследването на престъпления). Освен това при изпълнението на задълженията си полицията действа безпристрастно, непредубедено и справедливо и не трябва никога да злоупотребява със своите правомощия „по начин, който накърнява индивидуалните права и свободи, гарантирани в Конституцията на Япония“ (които включват, както бе посочено, правото на неприкосновеност на личния живот и защита на данните) ([92]).

(127) Специално по отношение на член 197, параграф 2 от НПК, Национална служба „Полиция“ (НСП) — като федерален орган, отговарящ наред с другото по всички въпроси, които засягат криминалната полиция — е издала инструкции

([85]) Приложението се отнася до 9 вида престъпления, например престъпления, свързани с наркотици и огнестрелни оръжия, трафик на хора и поръчкови убийства. Следва да се отбележи, че нововъведеното престъпление „подготовка на терористични актове и други организирани престъпления“ (вж. бележка под линия 76) не се включва в този ограничителен списък.

([86]) Още повече, че съгласно член 23 от Закона за подслушването разследващият орган трябва да уведоми писмено физическите лица, чиито комуникации са били прихванати (и съответно включени в записа от прихващането) за извършеното прихващане.

([87]) Вж. приложение II, раздел II, буква A, точка 1, буква б), подточка (1).

([88]) Според получената информация никой закон не предвижда отрицателни последици (включително и санкции) за стопанските субекти, които не оказват съдействие. Вж. приложение II, раздел II, буква A, точка 2, буква а).

([89]) Член 23, параграф 1, буква и) от Насоките на КЗЛИ (Общо издание) предвижда основата за разкриването на лична информация както в отговор на заповед (член 218 от НПК), така и на „въпросник“ (член 197, параграф 2 от ГПК).

([90]) Това означава, че „въпросникът“ може да се използва само за събиране на информация по отделните случаи, но не и за широкомащабно събиране на лични данни. Вж. също приложение II, раздел I, буква A, точка 2, буква б), подточка (1).

([91]) Както и разпоредбите, приемани от Комисията по въпросите на обществения ред към префектурата, вж. член 189, параграф 1 от НПК.

([92]) Вж. също така член 3 от Закона за полицията, съгласно който всички полицейски служители полагат клетва „да спазват задължението да защитават и спазват Конституцията и законите на Япония и да изпълняват задълженията си безпристрастно, справедливо и без предубеждения.“

към полицията на префектурите ([93]) относно „правилното използване на писмените запитвания в областта на разследванията“. Съгласно това уведомление, исканията трябва да се подават като се използва предварително установен формуляр („формуляр № 49“ или т.нар. „въпросник“) ([94]), трябва да се отнасят до записи „засягащи конкретно разследване“ и исканата информация трябва да е „необходима за [това] разследване“. Във всеки отделен случай, главният разследващ служител трябва да „разгледа внимателно необходимостта, съдържанието и т.н. на всяко индивидуално разследване“ и трябва да получи вътрешно одобрение от високопоставен служител.

(128) Освен това в две съдебни решения от 1969 г. и 2008 г. ([95]) Върховният съд на Япония е определил ограничения по отношение на незадължителните мерки, които оказват отрицателно въздействие върху правото на неприкосновеност на личния живот ([96]). По-специално съдът е счел, че такива мерки трябва да са „разумни“ и да не надвишават „общоприетите граници“, което означава, че трябва да са необходими за разследването на заподозряно лице (събиране на доказателства) и да са извършени с „подходящи методи за постигане на целта на разследването“ ([97]). Решенията показват, че това включва тест за пропорционалност, който взема предвид всички обстоятелства по случая (например равнище на отрицателно въздействие върху правото на неприкосновеност на личния живот, включително очакването за неприкосновеност на личния живот, сериозността на престъплението, вероятността за придобиване на полезни доказателства, значението на тези доказателства, възможни алтернативни методи на разследване и т.н.) ([98]).

(129) Независимо от тези ограничения за упражняване на публична власт, от самите стопански субекти се очаква да проверят („потвърдят“) необходимостта и „рационалността“ на предоставянето на трета страна ([99]). Това включва въпроса дали са възпрепятствани от закона да сътрудничат. Такива конфликтни правни задължения могат, в частност, да произтичат от задължения за поверителност, като например тези член 134 от Наказателния кодекс (относно връзката между адвокат, лекар, свещеник и т.н. и неговия/нейния клиент). Също така, „всяко лице, работещо в телекомуникациите, запазва, докато е на длъжност, тайни на други лица, които са станали му известни от комуникациите, третирани от телекомуникационната компания“ (член 4, параграф 2 от Закона за далекосъобщенията). Това задължение е подкрепено със санкцията, предвидена в член 179 от Закона за далекосъобщенията, който предвижда, че всяко лице, което е нарушило с тайната на комуникациите, третирани от телекомуникационната компания е виновно в извършването на престъпление и се наказва с лишаване от свобода със задължително полагане на труд до две години или глоба до 1 милион йени ([100]). Въпреки че това изискване не е абсолютно и допуска по-специално мерки, нарушаващи тайната на комуникациите, които представляват „действия, които могат да бъдат оправдани“ по смисъла на член 35 от Наказателния кодекс, това изключение не обхваща отговора на незадължителни искания от страна на публичните органи за разкриване на информация в електронна форма съгласно член 197, параграф 2 от НПК ([101]).

3.2.1.3. По-нататъшно използване на събраната информация

(130) След като бъде събрана от японските публични органи, личната информация попада в обхвата на прилагане на ЗЗЛИСАО. Този закон урежда третирането (обработката) на „задържана лична информация“ и налага редица

([93]) Съгласно член 30, параграф 1 и член 31, параграф 2 от Закона за полицията генералните директори на съответните областни служби на полицията (местните клонове на НСП) „ръководят и упражняват надзор“ върху полицията на префектурата.

([94]) Въпросникът трябва да посочва и информация за контакт с „отговорното лице“ („наименование на отдела [длъжност], име на лицето, служебен телефонен номер и др.“).

([95]) Решение от 24 декември 1969 г. на Върховния съд (1965(A) 1187); решение от 15 април 2008 г. (2007(A) 839).

([96]) Въпреки че тези решения не се отнасят до събирането на информация в електронна форма, японското правителство е пояснило, че прилагането на критериите, разработени от Върховния съд, се отнася за всяка намеса на публичните органи в правото на неприкосновеност на личния живот, включително и за всички „доброволни разследвания“, и по този начин тези критерии обвързват японските органи и при отправянето на искания за доброволно разкриване на информация. Вж. приложение II, раздел II, буква A, точка 2, буква б), подточка (1).

([97]) Според получената информация тези фактори трябва да бъдат считани за „разумни в съответствие със социално приетите стандарти“. Вж. приложение II, раздел II, буква A, точка 2, буква б), подточка (1).

([98]) За сходни съображения в контекста на задължителните разследвания (подслушване) вж. също решение 1997 (A) 636 на Върховния съд от 16 декември 1999 г.

([99]) В тази връзка, японските органи изтъкнаха насоките на КЗЛИ (General Rule Edition) и точка 5/14 от Въпросите и отговорите, изготвени от КЗЛИ за прилагането на ЗЗЛИ. Според японските органи, „като се има предвид нарастващото познаване от страна на лицата на техните права, свързани с неприкосновеността на личния им живот, както и обемът работа, създаван от такива искания, стопанските субекти стават все по-предпазливи при отговора на такива искания“. Вж. приложение II, раздел II, буква A, точка 2, с позоваване и на Нотификацията от страна на НСП от 1999 г. Според получената информация, наистина има случаи, в които стопанските субекти са отказали да сътрудничат. Например, в доклада си за прозрачността от 2017 г., LINE (най-популярното приложение за изпращане на съобщения в Япония) заявява следното: „След получаване на искания от разследващи агенции и т.н. ние проверяваме доколко те са съобразени със закона, защитата на потребителите и т.н. След тази проверка ние отказваме искането, ако установим несъответствие със закона. Ако обхватът на искането е твърде широк за целите на разследването, ние искаме от разследващата агенция обяснение. Ако в обяснението не се съдържа основателна причина, не отговаряме на искането.“ Може да бъде намерен на следния адрес: https://linecorp.com/en/security/transparency/top

([100]) За всяко лице, което „извършва дейност в областта на телекомуникациите“ санкциите са 3 години лишаване от свобода със задължително полагане на труд или глоба в размер до 2 милиона йени.

([101]) „Действия, които могат да бъдат оправдани“, съгласно Наказателния кодекс са по-специално действията на телекомуникационната компания, посредством които тя се съобразява с мерки на държавата, които имат правна сила (задължителни мерки), например когато разследващите органи предприемат мерки въз основа на заповед, издадена от съдия. Вж. приложение II, раздел II, буква A, точка 2, буква б), подточка (2), с позоваване на Насоките относно защитата на лична информация в телекомуникационния сектор.

ограничения и гаранции (вж. съображение 118) ([102]). Освен това обстоятелството, че даден административен орган може да задържи лична информация „само когато това се налага за извършване на поставените му задачи, предвидени в законови и подзаконови актове“ (член 3, параграф 1 от ЗЗЛИСАО), също налага ограничения — най-малкото косвено — за първоначалното събиране.

3.2.2. *Независим надзор*

(131) В Япония събирането на информация в електронна форма в областта на наказателното правоприлагане е най-вече ([103]) от компетентността на полицията на префектурата ([104]), като в това отношение тя е подложена на различни видове надзор.

(132) На първо място, винаги когато информация в електронна форма се събира чрез принудителни средства (претърсване и изземване), полицията трябва да получи предварително разрешение от съда (вж. съображение 121). Поради това в тези случаи във връзка със събирането ще се извършва предварителна проверка от съдия, при стриктно прилагане на изискването за „достатъчен повод“.

(133) Макар че при искания за доброволно разкриване не се извършва предварителна проверка от съдия, стопанските субекти, до които са адресирани тези искания, могат да възразяват срещу тях без да се излагат на риск от каквито и да било негативни последици (и ще трябва да вземат под внимание въздействието на всяко разкриване на данни върху неприкосновеността на личния живот). Освен това съгласно член 192, параграф 1 от НПК полицейските служители трябва винаги да си сътрудничат с прокурора и да координират действията си с него (и с Комисията по въпросите на обществения ред на префектурата) ([105]). От своя страна, прокурорът може да дава необходимите общи указания, с които да определя стандартите за справедливо разследване, и/или да издава конкретни разпореждания по отделните разследвания (член 193 от НПК). Когато такива указания и/или разпореждания не бъдат изпълнени, прокуратурата може да образува производство за налагане на дисциплинарни мерки (член 194 от НПК). Следователно полицията на префектурата работи под контрола на прокуратурата.

(134) На второ място, съгласно член 62 от Конституцията всяка камара на японския парламент може да провежда разследвания по отношение на правителството, включително във връзка със законосъобразността на събирането на информация от полицията. За тази цел съответната камара може да изисква явяване и даване на показания от свидетели и/или представяне на записана информация. Тези правомощия за провеждане на разследвания са доразвити в Закона за парламента, по-специално в глава XII от него. По-специално член 104 от Закона за парламента предвижда, че правителството, публичните институции и останалите държавни ведомства „са длъжни да изпълняват исканията, отправени от една от двете камари или от парламентарна комисия, за предоставяне на доклади и записана информация, необходими за целите на разследване.“ Отказ да се изпълни такова искане се допуска единствено ако държавният орган посочи основателна причина, която бъде приета от парламента, или ако бъде направена официална декларация, че предоставянето на докладите или записите би „увредило сериозно националните интереси“ ([106]). Освен това членовете на парламента могат да отправят писмени въпроси към правителството (членове 74 и 75 от Закона за парламента) и в миналото подобни „писмени запитвания“ са били отправяни и във връзка с обработването на лична информация от администрацията ([107]). В помощ на изпълнението от парламента на ролята му при упражняването на контрол върху изпълнителната власт са предвидени задължения за докладване, каквото е например задължението по член 29 от Закона за подслушването.

(135) На трето място, полицията на префектурата е подложена на независим надзор и в рамките на изпълнителната власт. Този надзор се упражнява по-специално от комисиите по въпросите на обществения ред към префектурите, създадени на ниво префектури с цел да гарантират демократичното управление и политическия неутралитет на полицията ([108]). Тези комисии се състоят от членове, назначавани от управителя на префектурата със съгласието на префектурния съвет (измежду граждани, които не са заемали длъжност на държавен служител в полицията през последните пет години), и разполагат със сигурен мандат (по-конкретно, те могат да бъдат освобождавани само по основателна причина) ([109]). Според получената информация на тези комисии не могат да се дават инструкции, поради което може да се счита, че те са напълно независими ([110]).Що се отнася до задачите и правомощията на

([102]) По отношение на правата на засегнатите лица вж. раздел 3.1.

([103]) По принцип прокурорът (или помощник прокурор, действащ по разпореждане на прокурора) може да разследва престъпление, ако счита това за необходимо (член 191, параграф 1 от НПК).

([104]) Според получената информация Национална служба „Полиция“ не извършва наказателни разследвания по отделни случаи. Вж. приложение II, раздел II, буква A, точка 1, буква а).

([105]) Вж. също член 246 от НПК, в който се предвижда, че съдебната полиция е длъжна да изпрати преписката на прокуратурата, след като приключи разследването за извършено престъпление („принцип на изпращане във всички случаи“).

([106]) Друга възможност е парламентът да поиска от Комисията за упражняване на надзор и преразглеждане на изрично посочени тайни да извърши проучване във връзка с отказа за предаване на информация. Вж. член 104-II от Закона за парламента.

([107]) Вж. приложение II, раздел II, буква Б, точка 4.

([108]) Освен това съгласно член 100 от Закона за местната автономия местният парламент е оправомощен да разследва дейността на правоприлагащите органи, създадени на ниво префектура, в това число и полицията на префектурата.

([109]) Вж. членове 39—41 от Закона за полицията. Що се отнася до политическия неутралитет, вж. също член 42 от Закона за полицията.

([110]) Вж. приложение II, раздел II, буква Б, точка 3 („система на независим съвет“).

комисиите по въпросите на обществения ред към префектурите, съгласно член 38, параграф 3 във връзка с член 2 и член 36, параграф 2 от Закона за полицията те отговарят за „защитата на правата и свободите на физическите лица“. За тази цел те са оправомощени да „упражняват надзор“ ([111]) върху всички дейности по разследване, извършвани от полицията на префектурите, включително събирането на лични данни. По-специално комисиите „могат да дават на полицията на префектурата подробни насоки или насоки във връзка с конкретен случай за проверка за неправомерно поведение на полицейски служители, ако считат това за необходимо.“ ([112]) Когато началникът на полицията на префектурата ([113]) получи такава насока или самостоятелно узнае за възможен случай на неправомерно поведение (включително нарушение на закона или друго неизпълнение на служебните задължения), той е длъжен да разследва надлежно случая и да докладва за резултата от разследването пред комисията по въпросите на обществения ред към префектурата (член 56, параграф 3 от Закона за полицията). Ако счете това за необходимо, въпросната комисия може също така да възложи на един от своите членове да провери как напредва изпълнението. Този процес продължава докато комисията по въпросите на обществения ред към префектурата се увери, че по случая са предприети подходящи мерки.

(136) Наред с това, що се отнася до правилното прилагане на ЗЗЛИСАО компетентният министър или ръководител на ведомство (напр. Генералният комисар на НСП) разполага с правомощия за правоприлагане, които се упражняват под надзора на Министерството на вътрешните работи и съобщенията (МВРС). Съгласно член 49 от ЗЗЛИСАО МВРС „може да събира доклади за изпълнението на този закон“ от ръководителите на административните органи (министри). За осъществяването на тази функция по упражняване на надзор спомага и информацията, предоставяна от 51 „всестранни информационни центъра“ към МВРС (по един във всяка префектура в Япония), които всяка година работят по хиляди молби на физически лица ([114]) (които на свой ред могат да разкриват евентуални нарушения на закона). Ако счита това за необходимо за гарантиране на спазването на закона, МВРС може да изисква представяне на обяснения и материали и да дава становища относно обработването на личната информация от съответния административен орган (членове 50 и 51 от ЗЗЛИСАО).

3.2.3. *Индивидуална защита*

(137) В допълнение към надзора, който се упражнява служебно, физическите лица разполагат и с няколко възможности за индивидуална защита, които могат да бъдат оползотворени чрез сезиране на независими органи (например комисиите по въпросите на обществения ред към префектурите или КЗЛИ) или на японските съдилища.

(138) На първо място, във връзка с личната информация, събирана от административните органи, последните са длъжни да „полагат усилия да обработват правилно и бързо жалбите“, подадени по повод последващата обработка на събраната информация (член 48 от ЗЗЛИСАО). Глава IV от ЗЗЛИСАО, отнасяща се до индивидуалните права, не се прилага спрямо личната информация, съдържаща се в „документи, свързани със съдебни производства и иззети вещи“ (член 53-2, параграф 2 от НПК) — което обхваща личната информация, събрана в рамките на наказателно разследване, — но физическите лица могат да подават жалби, в които да се позовават на общите принципи на защита на данните, като например задължението личната информация да се запазва единствено „когато запазването е нужно за изпълнението на [задачите по правоприлагане]“ (член 3, параграф 1 от ЗЗЛИСАО).

(139) Наред с това член 79 от Закона за полицията гарантира на физическите лица, които имат опасения, свързани с „изпълнението на служебните задължения“ от страна на полицейските служители, правото да подадат жалба пред (компетентната) независима комисия по въпросите на обществения ред към префектурата. Комисията разглежда тези жалби „почтено“, спазвайки законодателството и разпоредбите, установени на местно равнище, и уведомява в писмен вид жалбоподателя за резултата. Тъй като е оправомощена да упражнява надзор и да „дава насоки“ на полицията на префектурата във връзка с „неправомерно поведение на служители“ (член 38, алинея 3 и член 43-2, параграф 1 от Закона за полицията), комисията може да изисква от полицията на префектурата да извършва разследвания за установяване на фактите, да предприема мерките, които са необходими с оглед на установеното при разследването, и да докладва за резултатите. Ако комисията счете, че проведеното от полицията разследване не е задоволително, тя може да даде и указания във връзка с обработването на жалбата.

(140) С цел да улесни обработването на жалбите НСП е издала „Съобщение“ до полицията и комисиите по въпросите на обществения ред към префектурите относно правилното обработване на жалбите, свързани с изпълнението на служебните задължения от полицейските служители. В този документ НСП формулира стандарти за тълкуването

([111]) Вж. член 5, параграф 3 и член 38, параграф 3 от Закона за полицията.

([112]) Вж. член 38, параграф 3 и член 43-2, параграф 1 от Закона за полицията. Ако „даде насока“ по смисъла на член 43-2, параграф 1, комисията по въпросите на обществения ред към префектурата може да възложи на комитет, определен от нея, да следи за изпълнението на насоката (параграф 2). Освен това комисията може да препоръчва налагане на дисциплинарни мерки или освобождаване от длъжност на началника на полицията на префектурата (член 50, алинея 2 от Закона за полицията) и на другите полицейски служители (член 55, алинея 4 от Закона за полицията).

([113]) Същото се отнася и за Областния ръководител на Столичната полиция на Токио (вж. член 48, алинея 1 от Закона за полицията).

([114]) Според получената информация през финансовата 2017 година (април 2017 г. — март 2018 г.) всеобхватните информационни центрове са обработили общо 5 186 молби на физически лица.

и прилагането на член 79 от Закона за полицията. Наред с другото от полицията на префектурата се изисква да въведе „система за обработване на жалбите“ и да обработва и докладва „незабавно“ всички жалби пред компетентната комисия по въпросите на обществения ред към префектурата. В Съобщението жалбите са определени като искания за поправяне „на всякакви конкретни неблагоприятни последици, настъпили вследствие на незаконно или неуместно поведение“ ([115]) или на „непредприемане на необходимите действия от полицейски служител при изпълнението на служебните му задължения“ ([116]), както и всяко „оплакване/недоволство във връзка с неуместен начин на изпълнение на служебни задължения от страна на полицейски служител“. По този начин е дадено широко определение за материалното приложно поле на жалбата, включващо всяко твърдение за неправомерно събиране на данни, и жалбоподателят не е нужно да доказва, че е претърпял каквито и да било вреди вследствие на действията на полицейски служител. Важно е да се отбележи, че в Съобщението се посочва, че на чужденците (наред с другото) трябва да се оказва помощ при изготвянето на жалба. След като получат жалба комисиите по въпросите на обществения ред към префектурите са задължени да гарантират, че полицията на префектурата проучва фактите, въвежда мерки „според резултата от проучването на фактите“ и докладва за постигнатите резултати. Ако комисията счете, че извършеното проучване е недостатъчно, тя дава указания за обработването на жалбата, които полицията на префектурата е длъжна да спазва. Въз основа на получените доклади и взетите мерки комисията изпраща уведомление до физическото лице като посочва наред с другото мерките, които са предприети по жалбата. В Съобщението на НСП се подчертава, че жалбите следва да се обработват „добросъвестно“ и резултатът следва да се съобщава „в срок […], който изглежда подходящ от гледна точка на социалните норми и здравия разум.“

(141) На второ място, като се има предвид, че съвсем естествено защитата ще трябва да се търси в чужбина чрез ползване на чужда система и на чужд език, с цел да улесни получаването на защита от физическите лица от ЕС, чиито лични данни са предадени на стопански субекти в Япония, след което достъп до тях са получили и органи на публичната власт, японското правителство използва правомощията си и създаде нарочен механизъм за обработване на жалбите в тази област и вземане на решения по тях, който се управлява и контролира от КЗЛИ. Този механизъм се базира на задължението за сътрудничество между японските публични органи, наложено със ЗЗЛИ, и на специалната роля на КЗЛИ във връзка с международното предаване на данни от трети държави съгласно член 6 от ЗЗЛИ и Основната политика (определена с постановление на Министерски съвет). Подробностите относно този механизъм се съдържат в официалните изявления, гаранции и ангажименти, предоставени от японското правителство и приложени към настоящото решение като приложение II. По отношение на механизма не са установени специфични изисквания и той може да се ползва от всяко физическо лице, независимо дали то е заподозряно или обвинено в извършването на престъпление.

(142) Съгласно механизма физическо лице, подозиращо, че негови данни, предадени от Европейския съюз, са били събрани или използвани от публични органи в Япония (включително органи, отговарящи за наказателното правоприлагане) в нарушение на приложимите правила, може да подаде жалба пред КЗЛИ (лично или чрез органа по защита на данните по смисъла на член 51 от ОРЗД). КЗЛИ е задължена да обработи жалбата като първата ѝ стъпка е да уведоми за нея компетентните публични органи, в това число и съответните органи, упражняващи надзор. Тези органи са длъжни да си сътрудничат с КЗЛИ, „включително като предоставят необходимата информация и релевантни материали, така че КЗЛИ да може да прецени дали събирането или последващото използване на личната информация е било извършено в съответствие с приложимите правила“ ([117]). Това задължение, произтичащо от член 80 от ЗЗЛИ (който налага на японските публични органи да си сътрудничат с КЗЛИ), се прилага по принцип и следователно се отнася и за прегледа на следствените мерки, предприети от такива органи, като тези органи освен това са поели ангажимент за такова сътрудничество чрез писмени уверения, дадени от ръководителите на компетентните министерства и държавни ведомства, както са отразени в приложение II.

(143) Ако преценката покаже, че е било допуснато нарушение на приложимите правила, „сътрудничеството между съответните публични органи и КЗЛИ включва задължение за отстраняване на нарушението“, което при незаконното събиране на лична информация обхваща и заличаването на съответните данни. Важно е да се отбележи, че посоченото задължение се изпълнява под надзора на КЗЛИ, която „преди да приключи работата по преценката, потвърждава, че са взети мерки за цялостно отстраняване на нарушението“.

(144) След приключване на работата по преценката КЗЛИ уведомява в разумен срок физическото лице за резултата от нея, включително за всички предприети коригиращи действия, доколкото са приложими. Същевременно КЗЛИ информира физическото лице за възможността да поиска от компетентния публичен орган потвърждение на резултата и за названието на органа, до който следва да бъде отправено подобно искане. Възможността да се

([115]) Изискването за наличие на „конкретни неблагоприятни последици“ предполага просто, че жалбоподателят трябва да е лично засегнат от поведението (или бездействието) на полицейския служител, а не че трябва да доказва наличието на вреда.

([116]) Спазването на закона, в това число и на правните изисквания за събирането и използването на лични данни, е част от тези задължения. Вж. член 2, параграф 2, алинея 3 от Закона за полицията.

([117]) При преценката КЗЛИ ще си сътрудничи с МВРС, което, както бе обяснено в съображение 136, може да изисква представяне на обяснения и материали и да дава становища относно обработването на личната информация от съответния административен орган (членове 50 и 51 от ЗЗЛИСАО).

получи такава информация, в това число и мотивите за решението на компетентния орган, може да бъде от полза за физическото лице при предприемането на евентуални следващи действия, включително при търсене на защита по съдебен ред. Достъпът до подробна информация за заключенията от преценката може да бъде ограничен, доколкото има основателни причини да се смята, че предоставянето на такава информация би могло да изложи на риск висящото разследване.

(145) Трето, физическо лице, което не е съгласно със съдебно решение за изземване (съдебна заповед) ([118]), отнасящо се до негови лични данни, или с полицейски или прокурорски мерки, предприети в изпълнение на такова решение, може да подаде молба за отмяна или изменение на въпросното решение или на съответните мерки (член 429, параграф 1 и член 430, параграфи 1 и 2 от НПК, член 26 от Закона за подслушването) ([119]). Ако второинстанционният съд прецени, че съдебната заповед или нейното изпълнение („процедура по изземване“) са незаконни, той ще уважи искането и ще разпореди иззетите вещи да бъдат върнати ([120]).

(146) Четвърто, като по-косвена форма на съдебен контрол съществува възможността физическо лице, което смята, че събирането на личната му информация като част от наказателно разследване е било извършено незаконно, да се позове на тази незаконосъобразност на образувания срещу него процес пред наказателния съд. Ако съдът се съгласи с това твърдение, доказателството ще бъде изключено като недопустимо.

(147) Накрая, съгласно член 1, параграф 1 от Закона за обезщетенията, дължими от държавата, съдът може да присъди обезщетение, когато при изпълнение на служебните си задължения държавен служител, който упражнява публична власт от името на държавата, е причинил незаконно и виновно (умишлено или по непредпазливост) вреди на съответното физическо лице. Съгласно член 4 от Закона за обезщетенията, дължими от държавата, отговорността на държавата за вреди почива на разпоредбите на Гражданския кодекс. В тази връзка член 710 от Гражданския кодекс предвижда, че отговорност се носи и за вредите, нанесени не само на имущество, тоест и за морални вреди (например под формата на „психично страдание“). Това включва случаите, при които неприкосновеността на личния живот на физическо лице е била накърнена чрез неправомерно наблюдение и/или събиране на негова лична информация (напр. незаконно изпълнение на съдебна заповед) ([121]).

(148) В допълнение към паричното обезщетение физическите лица могат при определени обстоятелства да се възползват и от правна защита под формата на съдебно разпореждане (напр. за заличаване на личните данни, събрани от публичните органи), чрез позоваване на правата им на неприкосновеност на личния живот, залегнали в член 13 от Конституцията ([122]).

(149) Във връзка с всички тези възможности за защита механизмът за решаване на спорове, създаден от японското правителство, предвижда, че физическо лице, което е останало неудовлетворено от резултата от процедурата, може да се обърне към КЗЛИ, „която информира лицето за различните възможности и за подробните процедури за получаване на защита съгласно законовите и подзаконовите актове на Япония“. Наред с това КЗЛИ „ще предостави на лицето подкрепа, включително съвети и помощ при сезиране на съответния административен или съдебен орган с евентуално искане“.

(150) Това включва упражняването на процесуалните права по реда, предвиден в Наказателно-процесуалния кодекс. Така например, „[к]огато вследствие на преценката се установи, че дадено физическо лице е заподозряно в извършването на престъпление, КЗЛИ уведомява лицето за това“ ([123]), както и за предвидената в член 259 от НПК възможност то да поиска от прокуратурата да бъде уведомено, ако тя реши да не образува наказателно производство. Освен това, ако вследствие на преценката се установи, че е било образувано дело, по което личната информация на лицето е била използвана и това дело е приключило, КЗЛИ ще информира лицето за възможността да се запознае с протокола от делото по реда на член 53 от НПК (и член 4 от Закона за досиетата по приключени наказателни

([118]) Това включва и заповедите за разрешаване на подслушване, за които Законът за подслушването предвижда специално изискване за уведомяване (член 23). Съгласно тази разпоредба разследващият орган трябва да уведоми писмено физическите лица, чиито комуникации са били прихванати (и съответно включени в записа от прихващането) за извършеното прихващане. Друг пример е член 100, параграф 3 от НПК, в който се предвижда, че когато по разпореждане на съда са били иззети пощенски пратки или телеграми, изпратени до или от обвиняемия, съдът трябва да уведоми изпращача или получателя за това, освен ако има опасност това да възпрепятства съдебното производство. Член 222, параграф 1 от НПК препраща към тази разпоредба във връзка с претърсванията и изземванията, извършвани от разследващите органи.

([119]) Тази молба не води автоматично до спиране на изпълнението на решението за изземване, но сезираният съд може да разпореди такова спиране до постановяване на решението по същество. Вж. член 429, параграф 2 и член 432 във връзка с член 424 от НПК.

([120]) Вж. приложение II, раздел II, буква B, подточка (1).

([121]) Вж. приложение II, раздел II, буква B, точка 2.

([122]) Вж. напр. Решение на Окръжен съд — Токио от 24 март 1988 г. (№ 2925), Решение на Окръжен съд — Осака от 26 април 2007 г. (№ 2925). Според Окръжен съд — Осака е необходимо да се вземат под внимание редица фактори, като например: (i) естеството и съдържанието на личната информация, за която става въпрос; (ii) начинът, по който тя е била събрана; (iii) неблагоприятните последици за физическото лице, в случай че информацията не бъде заличена; и iv) общественият интерес, включително неблагоприятните последици за публичния орган, в случай че информацията бъде заличена.

([123]) Във всеки случай, след образуването на наказателното производство прокурорът предоставя на обвиняемия възможност да се запознае с доказателствата (вж. членове 298–299 от НПК). По отношение на жертвите на престъпления, вж. членове 316–333 от НПК.

дела). Получаването на достъп до личното досие е от значение, тъй като то ще помогне на лицето да разбере по-добре проведеното срещу него разследване и съответно да подготви евентуален иск, с който да сезира съда (напр. иск за обезщетяване на вреди), ако счита, че данните му са били събрани или използвани неправомерно.

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

(151) Според японските власти в Япония няма закон, който да разрешава отправянето на задължителни искания на информация или „административно подслушване“ извън рамките на наказателните разследвания. Следователно, когато са налице съображения за национална сигурност информацията може да се получава единствено от източник на информация, до който всеки може да има свободен достъп, или чрез доброволно разкриване. Стопанските субекти, до които бъде отправено искане за доброволно съдействие (под формата на разкриване на информация в електронна форма), не са правно задължени да предоставят такава информация ([124]).

(152) Освен това според получената информация само четири държавни ведомства са оправомощени да събират информация в електронна форма, държана от японски стопански субекти, по съображения, свързани с националната сигурност: (i) Правителствената служба „Разузнаване и издирване“ (ПСРИ); (ii) Министерство на отбраната (МО); (iii) полицията (Национална служба „Полиция“ (НСП) ([125]) и полицията на префектурите); и iv) Агенция „Разузнаване във връзка с обществената сигурност“ (АРОС). ПСРИ обаче никога не събира информация пряко от стопанските субекти, включително чрез прихващане на съобщения. Когато тя получава информация от други държавни органи с цел да предостави анализ пред правителството, въпросните други органи трябва от своя страна да спазват законодателството, включително ограниченията и гаранциите, анализирани в настоящото решение. Следователно нейните дейности не са релевантни в контекста на прехвърлянето на данни.

3.3.1. *Правно основание и приложими ограничения/гаранции*

(153) Според получената информация МО събира информация (в електронна форма) на основание Закона за МО. Съгласно член 3 от този закон задачата на МО е да управлява и командва военните сили и „да осъществява дейностите, свързани с тях, с цел гарантиране на мира и независимостта на страната и безопасността на народа“. В член 4, параграф 4 се предвижда, че МО разполага с правомощия във връзка с „отбраната и охраната“, във връзка с действията, предприемани от силите за самоотбрана, както и във връзка с разгръщането на военните сили, включително събирането на информацията, необходима за осъществяването на тези дейности. То е оправомощено да събира информация (в електронна форма) от стопанските субекти само чрез доброволно съдействие.

(154) Що се отнася до полицията на префектурите, нейните отговорности и задължения включват „поддържането на обществения ред и сигурност“ (член 35, параграф 2 във връзка с член 2, параграф 1 от Закона за полицията). В рамките на тази компетентност полицията може да събира информация, но само на доброволна основа, без принудителни мерки. Освен това действията на полицията са „строго ограничени“ до необходимото за изпълнението на нейните задължения. Също така тя е длъжна да действа „безпристрастно, непредубедено, без предразсъдъци и справедливо“ и не трябва никога да злоупотребява с правомощията си „по какъвто и да било начин, който би засегнал правата и свободите на физическите лица, гарантирани от Конституцията на Япония (член 2 от Закона за полицията).

(155) И накрая, АРОС може да извършва разследвания съгласно Закона за предотвратяването на подривните дейности (ЗППД) и Закона за контролиране на организациите, извършили актове на безразборно масово убийство (ЗКО), когато тези разследвания са необходими, за да се подготви приемането на контролни мерки срещу някои организации ([126]). Съгласно тези два закона по искане на Генералния директор на АРОС Комисията за проучване на обществената сигурност може да издава определени „разпореждания“ (за наблюдение/забрани в случая на ЗКО ([127]), разпускане/забрани в случая на ЗППД ([128])) като в тази връзка АРОС може да провежда разследвания ([129]). Според получената информация тези разследвания се провеждат винаги на доброволна основа, което означава, че АРОС не

([124]) Поради това стопанските субекти могат свободно да изберат да не окажат съдействие, без какъвто и да е риск от санкции или други отрицателни последици. Вж. приложение II, раздел III, буква А, точка 1.

([125]) Впрочем, според получената информация основната роля на НСП е да координира разследванията, провеждани от различните департаменти на полицията на префектурата и да обменя информация с органи на други държави. Дори и в тази си роля НСП подлежи на надзор от страна на Националната комисия по въпросите на обществения ред, отговаряща наред с другото за защитата на правата и свободите на физическите лица (член 5, параграф 1 от Закона за полицията).

([126]) Вж. приложение II, раздел III, буква А, точка 1, подточка (3). Съответното приложно поле на тези два закона е ограничено, като ЗППД се отнася за „терористичните подривни дейности“, а ЗКО за „актове на безразборно масово убийство“ (което означава „терористична подривна дейност“ по смисъла на ЗППД „чрез която безразборно са убити голям брой хора“).

([127]) Вж. членове 5 и 8 от ЗКО. Разпореждането за извършване на наблюдение води и до задължение за докладване от страна на образуването, засегнато от мярката. Във връзка с процесуалните гаранции, и по-специално изискванията за прозрачност и за предварително разрешение, издадено от Комисията за проучване на обществената сигурност, вж. членове 12, 13, 15–27 от ЗКО.

([128]) Вж. членове 5 и 7 от ЗППД. Във връзка с процесуалните гаранции, и по-специално изискванията за прозрачност и за предварително разрешение, издадено от Комисията за проучване на обществената сигурност, вж. членове 11–25 от ЗППД.

([129]) Вж. член 27 от ЗППД и членове 29 и 30 от ЗКО.

може да принуждава притежателя на лична информация да предостави такава информация ([130]). Във всеки отделен случай проверките и разследването се ограничават само до строго необходимото за постигане на целите на проверката и при никакви обстоятелства не ограничават „неоснователно“ правата и свободите, гарантирани от Конституцията на Япония (член 3, параграф 1 от ЗППД/ЗКО). Освен това съгласно член 3, параграф 2 от ЗППД/ЗКО АРОС не трябва при никакви обстоятелства да злоупотребява с тези проверки, нито с разследванията, извършвани с цел да се подготвят такива проверки. Ако служител на АРОС е злоупотребил с властта, предоставяна му от съответния закон, като е принудил дадено лице да направи нещо, което не е длъжно да прави, или като се е намесил в упражняването на правата от дадено лице, могат да му бъдат наложени наказателните санкции, предвидени в член 45 от ЗППД или член 42 от ЗКО. И накрая, в двата закона изрично се посочва, че техните разпоредби, включително предоставените с тях правомощия, „не могат при никакви обстоятелства да се тълкуват разширително“ (член 2 от ЗППД/ЗКО).

(156) Във всички описани в настоящия раздел случаи на достъп на държавни органи по съображения за национална сигурност се прилагат ограниченията, посочени от Върховния съд на Япония във връзка с разследванията на доброволна основа, което означава, че събирането на информация (в електронна форма) трябва да е съобразено с принципите на необходимост и пропорционалност („целесъобразен метод“) ([131]). Както бе изрично потвърдено от японските органи, „събирането и обработката на информация се осъществяват само доколкото са необходими за изпълнението на конкретни задължения на компетентния публичен орган, и то при наличие на конкретни заплахи“. Следователно „това изключва масовото и безразборно събиране или достъп до лична информация по съображения, свързани с националната сигурност“ ([132]).

(157) Също така, след като бъде събрана, всяка лична информация, запазена от публичните органи за целите на националната сигурност, попада в приложното поле на ЗЗЛИСАО и съответно се ползва от предвидената в него защита, когато става въпрос за последващото ѝ съхраняване, използване и разкриване (вж. съображение 118).

3.3.2. *Независим надзор*

(158) По отношение на събирането на лична информация за целите на националната сигурност се прилагат няколко нива на надзор от трите власти.

(159) Първо, чрез своята специализирана комисия японският парламент може да разгледа въпроса за законосъобразността на разследванията като използва правомощията си за упражняване на парламентарен контрол (член 62 от Конституцията, член 104 от Закона за парламента; вж. съображение 134). За изпълнението на тази надзорна функция спомагат предвидените конкретни задължения за докладване във връзка с дейностите, осъществявани съгласно някои от посочените по-горе правни основания ([133]).

(160) Второ, в рамките на изпълнителната власт съществуват няколко механизма за упражняване на надзор.

(161) Що се отнася до МО надзорът се осъществява от Служба „Спазване на законодателството“, която се ръководи от главния инспектор (СГИ) ([134]). Тя е създадена на основание член 29 от Закона за Министерство на отбраната като служба в рамките на МО, поставена под надзора на министъра на отбраната (пред когото докладва), но е независима от оперативните подразделения на МО. СГИ има за задача да гарантира спазването на законовите и подзаконовите актове, както и да осигурява правилното изпълнение на служебните задължения от служителите на МО. Тя е оправомощена също така да извършва т.нар. „проверки в областта на отбраната“, които могат да се извършват както на редовни интервали от време („редовни проверки в областта на отбраната“), така и по отделни поводи („специални проверки в областта на отбраната“), като в миналото те са обхващали и проверките за правилното обработване на личната информация ([135]). При извършването на тези проверки СГИ може да влиза в обекти

([130]) Вж. приложение II, раздел III, буква А, точка 1, подточка (3).

([131]) Вж. приложение II, раздел III, буква А, точка 2, буква б): „От съдебната практика на Върховния съд следва, че за да се отправи искане за доброволно съдействие до стопански субект, това искане трябва да е необходимо за разследването на предполагаемото престъпление и да е разумно с оглед на постигането на целта на разследването. Въпреки че разследванията, провеждани от разследващите органи в областта на националната сигурност, се различават както по правното си основание, така и по своята цел от разследванията, провеждани от разследващите органи в областта на правоприлагането, основните принципи за „необходимост от разследване“ и „целесъобразност на метода“ се прилагат по аналогия в областта на националната сигурност и следва да бъдат спазвани като надлежно се вземат под внимание специфичните за всеки отделен случай обстоятелства.“

([132]) Вж. приложение II, раздел III, буква А, точка 2, буква б).

([133]) Вж. напр. член 36 от ЗППД/член 31 от ЗКО (за АРОС).

([134]) Ръководителят на СГИ е бивш прокурор. Вж. приложение II, раздел III, буква Б, точка 3.

([135]) Вж. приложение II, раздел III, буква Б, точка 3. Даден е пример, според който редовната проверка в областта на отбраната, извършена през 2016 г. относно наличието на „Съзнание/Готовност за спазване на правните изисквания“, е обхванала наред с другото и „актуалното положение във връзка със защитата на личната информация“ (управление, съхранение и др.). В изготвения след проверката доклад са били посочени случаи на нецелесъобразно управление на данни и е бил отправен призив към подобрения в това отношение. МО е публикувало доклада на своя уебсайт.

(служебни помещения) и да изисква да ѝ бъдат предоставени документи или информация, в това число и обяснения от заместника на заместник–министъра на МО. Всяка проверка приключва с доклад до министъра на отбраната, в който се излагат заключенията и необходимите мерки за внасяне на подобрения (чието изпълнение може също да бъде проверено чрез допълнителни проверки). Докладът на свой ред представлява основата за издаване на инструкции от министъра на отбраната за предприемане на мерките, необходими за промяна на положението; заместникът на заместник–министъра е натоварен с осъществяването на тези мерки и трябва да докладва за предприетите действия.

(162) Във връзка с полицията на префектурата надзорът се осъществява от независимите комисии по въпросите на обществения ред към префектурите, както е обяснено в съображение 135 относно наказателното правоприлагане.

(163) И накрая, както беше посочено, APOC може да извършва разследвания само доколкото това е необходимо за приемането на разпореждания за забрана, разпускане или наблюдение съгласно ЗППД/ЗКО, като по отношение на тези разпореждания независимата ([136]) Комисия за проучване на обществената сигурност извършва предварителни проверки. Освен това редовните/периодичните проверки (при които се разглеждат цялостно операциите, провеждани от APOC) ([137]) и специалните вътрешни проверки ([138]) на дейностите на отделните дирекции/отдели и др. се осъществяват от определени за целта инспектори и могат да доведат до издаването на инструкции до ръководителите на съответните дирекции и т.н. за предприемане на коригиращи мерки или мерки за внасяне на подобрения.

(164) Тези механизми за упражняване на надзор, подсилени чрез възможността физическите лица да предизвикат намесата на КЗЛИ в качеството ѝ на независим надзорен орган (вж. по-долу съображение 168), осигуряват адекватни гаранции срещу рисковете от злоупотреба от страна на японските органи с правомощията им в областта на националната сигурност, както и срещу всяко неправомерно събиране на информация в електронна форма.

3.3.3. *Индивидуална защита*

(165) Когато става дума за индивидуална защита във връзка с личната информация, събрана и съответно „запазена“ от административни органи, последните са длъжни да „полагат усилия да обработват правилно и бързо жалбите“, отнасящи се до обработката (член 48 от ЗЗЛИСАО).

(166) Освен това за разлика от наказателните разследвания, съгласно ЗЗЛИСАО физическите лица (включително чуждестранните граждани, живеещи в чужбина) по принцип имат право на разкриване ([139]), поправяне (включително заличаване) и преустановяване на използването/предоставянето. Независимо от това, ръководителят на административния орган може да откаже разкриването на информация „за която има основателни причини […] да се смята, че ако бъде разкрита, има вероятност да навреди на националната сигурност“ (член 14, точка iv) от ЗЗЛИСАО), като той може да стори това дори без да се разкрива съществуването на такава информация (член 17 от ЗЗЛИСАО). По същия начин, въпреки че физическото лице има право да поиска преустановяване на използването или заличаване съгласно член 36, параграф 1, точка i) от ЗЗЛИСАО в случай че административният орган е получил информацията незаконно или я запазва или използва извън рамките на необходимото за постигане на посочената цел, органът може да отхвърли искането, ако счете, че преустановяването на използването „има вероятност да попречи на правилното изпълнение на действията, отнасящи се до целта, за която се използва запазената лична информация, поради естеството на въпросните действия“ (член 38 от ЗЗЛИСАО). При все това, когато е възможно лесно да бъдат отделени и изключени отделни части, по отношение на които може да се приложи изключение, административните органи са задължени да разрешат поне частично разкриване (вж. напр. член 15, параграф 1 от ЗЗЛИСАО) ([140]).

([136]) Съгласно Закона за създаване на Комисия за проучване на обществената сигурност председателят и членовете на Комисията „са независими при упражняването на правомощията си“ (член 3). Те се назначават от министър-председателя със съгласието на двете камари на японския парламент и могат да бъдат освобождавани от длъжност само при наличие на „основание“ за това (напр. лишаване от свобода, неправомерно поведение, умствено или физическо увреждане, откриване на производство по несъстоятелност).

([137]) Регламент за периодичните проверки, извършвани от Агенция „Разузнаване във връзка с обществената сигурност“ (Генерален директор на APOC, Инструкция № 4, 1986 г.).

([138]) Регламент за специалните проверки, извършвани от Агенция „Разузнаване във връзка с обществената сигурност“ (Генерален директор на APOC, Инструкция № 11, 2008 г.). Специални проверки се извършват когато генералният директор на APOC сметне това за необходимо.

([139]) Става дума за правото лицето да получи копие на „Запазената лична информация“.

([140]) Вж. също възможността за „разкриване по усмотрение“ дори в случаите, когато „неподлежаща на разкриване информация“ е включена в „Запазената лична информация“, която се иска да бъде разкрита (член 16 от ЗЗЛИСАО).

(167) Във всички случаи административният орган трябва да вземе писмено решение в определен срок (30 дни, като при определени условия срокът може да бъде удължен с още 30 дни). Ако искането бъде отхвърлено или удовлетворено само частично или ако физическото лице смята по други причини, че поведението на административния орган е „неправомерно или несправедливо“, въпросното физическо лице може да поиска преразглеждане по административен ред съгласно Закона за административното обжалване ([141]). В такъв случай ръководителят на административния орган, разглеждащ жалбата, се консултира с Апелативния съвет по въпросите на разкриването на информация и защита на личната информация (членове 42 и 43 от ЗЗЛИСАО) — специализиран, независим съвет, чиито членове се назначават от министър-председателя със съгласието на двете камари на парламента. Според получената информация Апелативният съвет може да извърши проверка ([142]), при което може да поиска от административния орган да предостави запазената лична информация, включително цялото класифицирано съдържание, както и друга информация и документи. Въпреки че крайният доклад, който се изпраща на жалбоподателя и на административния орган и се прави обществено достояние, не е правно обвързващ, направените в него заключения се следват в почти всички случаи ([143]).Освен това лицето има възможност да обжалва апелативното решение по съдебен ред съгласно Закона за административното съдопроизводство. Това дава възможност за осъществяване на съдебен контрол върху прибягването до изключение(я) по съображения, свързани с националната сигурност, включително относно това дали е налице злоупотреба с такова изключение, или то все още е оправдано.

(168) С цел да улесни упражняването на гореописаните права, предоставяни от ЗЗЛИСАО, МВРС е създало 51 „всеобхватни информационни центъра“, които предоставят обединена информация за тези права, за приложимите процедури за отправяне на искания и за различните възможности за правна защита ([144]). Що се отнася до административните органи, те са длъжни да предоставят „информация, която допринася за конкретизирането на задържаната лична информация, която се държи“ ([145]) и да предприемат „други подходящи мерки като вземат под внимание удобството на лицето, което възнамерява да подаде искане“ (член 47, параграф 1 от ЗЗЛИСАО).

(169) Както при разследванията в областта на наказателното правоприлагане, така и в областта на националната сигурност, физическите лица могат да получат индивидуална защита като се свържат директно с КЗЛИ. Това ще задейства специалната процедура за разрешаване на спорове, създадена от японското правителство за физическите лица от ЕС, чиито лични данни са предадени въз основа на настоящото решение (вж. подробните обяснения в съображения 141–144 и 149).

(170) Наред с това физическите лица могат да търсят защита по съдебен ред под формата на иск за обезщетяване на вреди, предявен съгласно Закона за обезщетенията, дължими от държавата, който обхваща и неимуществените вреди, а при определени условия и заличаването на събраните данни (вж. съображение 147).

4. ЗАКЛЮЧЕНИЕ: АДЕКВАТНО НИВО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ, ПРЕДАВАНИ ОТ ЕВРОПЕЙСКИЯ СЪЮЗ КЪМ СТОПАНСКИ СУБЕКТИ В ЯПОНИЯ

(171) Комисията счита, че ЗЗЛИ, в съчетание с Допълнителните правила, съдържащи се в приложение I и официалните изявления, гаранции и ангажименти, съдържащи се в приложение II, осигуряват ниво на защита на личните данни, предадени от Европейския съюз, което по същество е равностойно на нивото, гарантирано от Регламент (ЕС) 2016/679.

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

([141]) Закон за административното обжалване (Закон № 160 от 2014 г.), и по-специално член 1, параграф 1.

([142]) Вж. член 9 от Закона за създаване на Апелативния съвет по въпросите на разкриването на информация и защита на личната информация (Закон № 60 от 2003 г.).

([143]) Според получената информация, през последните 13 години от 2005 г. насам (когато ЗЗЛИСАО е влязъл в сила) административният орган не се е съобразил с доклада само в два от над 2000 случая, въпреки факта, че административните решения са били оспорвани от Апелативния съвет в редица случаи. Освен това, когато административният орган вземе решение, което се разминава с констатациите от доклада, той трябва да посочи ясно причините да постъпи така. Вж. приложение II, раздел III, буква В, във връзка с член 50, параграф 1, точка iv) от Закона за административното обжалване.

([144]) Всеобхватните информационни центрове — по един във всяка префектура — предоставят на гражданите обяснения относно личната информация, събирана от публичните органи (напр. съществуващите бази данни), и приложимите правила за защита на данните (ЗЗЛИСАО), включително и за начините, по които могат да упражнят правата си на разкриване, поправяне или спиране на използването на данните. Същевременно тези центрове работят като точка за контакт за подаване на запитвания/жалби от граждани. Вж. приложение II, раздел II, буква В, точка 4, буква а).

([145]) Вж. също членове 10 и 11 от ЗЗЛИСАО, отнасящи се до „Регистър на досиетата с лична информация“, които обаче съдържат големи изключения по отношение на „досиетата с лична информация“, изготвени или получени за целите на наказателните разследвания или съдържащи сведения, свързани с националната сигурност и други важни държавни интереси (вж. член 10, параграф 2, подточки i) и ii) от ЗЗЛИСАО).

(173) Накрая, въз основа на наличната информация за правния ред на Япония, в това число изявленията, гаранциите и ангажиментите, поети от японското правителство и посочени в приложение II, Комисията счита, че всяко вмешателство във връзка с основните права на лицата, чиито лични данни са предадени от Европейския съюз към Япония, от страна на японските 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.

(174) Поради това, предвид изложените в настоящото решение констатации Комисията смята, че Япония осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз към ССОЛИ в Япония, по отношение на които се прилага ЗЗЛИ, освен в случаите, когато получателят попада в една от категориите, изброени в член 76, параграф 1 от ЗЗЛИ и всички или част от целите на обработването съответства(т) на една от целите, предвидени в тази разпоредба.

(175) Въз основа на това Комисията стига до заключението, че стандартът за адекватно ниво на защита, предвиден в член 45 от Регламент (ЕС) 2016/679, тълкуван като се взема под внимание Хартата на основните права на Европейския съюз, по-специално в решението по делото *Schrems* ([146]), е изпълнен.

5. ДЕЙСТВИЯ НА ОРГАНИТЕ ПО ЗАЩИТА НА ДАННИТЕ И ИНФОРМАЦИЯ ДО КОМИСИЯТА

(176) Според практиката на Съда на ЕС ([147]) 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 Япония 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.

(177) 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 японските органи на изявленията, гаранциите и ангажиментите, посочени в приложение II. За да се улесни този процес, от японските органи се очаква да информират Комисията за съществените промени, имащи отношение към настоящото решение и свързани с обработването на лични данни от стопанските субекти или с ограниченията и гаранциите, приложими към достъпа до лични данни от страна на публичните органи. Това следва да включва всички решения, приети от КЗЛИ съгласно член 24 от ЗЗЛИ, с които се признава, че трета държава осигурява ниво на защита, което е равностойно на нивото, гарантирано в Япония.

(178) На следващо място, за да се даде възможност на Комисията да изпълнява ефективно функцията си по извършване на мониторинг, държавите членки следва да я информират за всички релевантни действия, предприети от националните органи по защита на данните (ОЗД), по-специално във връзка със запитвания или жалби на субекти на данни от ЕС във връзка с предаване на лични данни от Европейския съюз към стопански субекти в Япония. Комисията следва да бъде информирана и за всякакви признаци, че действията на японските 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.

(179) 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. 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. Същевременно, както е обяснено от Съда в решението му по делото Schrems ([148]) и е признато в член 58, параграф 5 от ОРЗД, когато ОЗД поставя под въпрос, включително въз основа на получена жалба, съгласуваността на дадено решение на Комисията относно адекватно ниво на защита с основните права на неприкосновеност на личния живот и на защита на данните на лицето, националното законодателство трябва да предвижда правни способи, позволяващи на съответния орган да представи възраженията си пред национална юрисдикция, и ако последната споделя съмненията, трябва да спре производството и да сезира Съда на ЕС с преюдициално запитване ([149]).

([146]) Вж. бележка под линия 3 по-горе.
([147]) Решение по делото *Schrems*, точка 76.
([148]) Решение по делото *Schrems*, точка 65.
([149]) 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 счита за основателни, пред националните юрисдикции, така че ако последните споделят съмненията на органа относно валидността на решението на Комисията, да отправят преюдициално запитване с цел проверка на валидността на решението.“

6. **ПЕРИОДИЧНИ ПРЕГЛЕДИ НА КОНСТАТАЦИЯТА ЗА АДЕКВАТНО НИВО НА ЗАЩИТА**

(180) В приложение на член 45, параграф 3 от Регламент (ЕС) 2016/679 ([150]) и с оглед на факта, че нивото на защита, осигурявано от японския 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 Япония, са все още фактически и правно обосновани.

(181) 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 ОРЗД, дали следва да се запази същият двугодишен цикъл. При всички случаи последващите прегледи следва да се извършват най-малко веднъж на четири години ([151]). Прегледът следва да обхваща всички аспекти от функционирането на настоящото решение, и по-специално прилагането на Допълнителните правила (като се обръща специално внимание на защитата в случай на последващо предаване), прилагането на правилата относно съгласието, включително в случай на оттеглянето му, ефективността при упражняването на индивидуалните права, както и ограниченията и гаранциите във връзка с достъпа на държавните органи, включително механизма за правна защита, посочен в приложение II към настоящото решение. Той следва да обхваща също ефективността на надзора и правоприлагането, що се отнася до правилата, които се прилагат спрямо ССТЛИ и в областта на наказателното правоприлагане и националната сигурност.

(182) При извършването на прегледа Комисията следва да се срещне с КЗЛИ, придружена, ако е целесъобразно, от други японски 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 (ЕКЗД). В рамките на съвместния преглед Комисията следва да поиска от КЗЛИ 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 ([152]). 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 японските органи или на други заинтересовани страни в Япония, ЕКЗД, отделни ОЗД, групи на гражданското общество, съобщения в медиите или всякакви други налични източници на информация.

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

7. **СПИРАНЕ НА ПРИЛАГАНЕТО НА РЕШЕНИЕТО ЗА АДЕКВАТНО НИВО НА ЗАЩИТА**

(184) Ако въз основа на редовните проверки, проверките *ad hoc* или друга налична информация Комисията стигне до заключение, че вече не може да се счита, че нивото на защита, предоставяна от японския правен ред, по същество е равностойно на нивото в Европейския съюз, тя следва да уведоми за това компетентните японски органи и да поиска предприемане на подходящи мерки в определен разумен срок. Това включва както правилата, приложими за стопанските субекти, така и тези, приложими за японските публични органи, отговарящи за наказателното правоприлагане или националната сигурност. Така например тази процедура ще бъде задействана в случаите, когато последващите предавания — включително въз основа на решенията, приети от КЗЛИ по силата на член 24 от ЗЗЛИ, с които се признава, че трета държава осигурява ниво на защита, което е равностойно на нивото, гарантирано в Япония — вече няма да се извършват при прилагане на гаранциите, осигуряващи непрекъснатостта на защитата по смисъла на член 44 от ОРЗД.

(185) Ако след изтичане на посочения срок компетентните японски органи не са успели да покажат по задоволителен начин, че настоящото решение продължава да почива на адекватно ниво на защита, Комисията, в приложение на член 45, параграф 5 от Регламент (ЕС) 2016/679, следва да започне процедурата за частично или пълно спиране на прилагането на настоящото решение или за неговата отмяна. Като алтернативна възможност Комисията следва да започва процедурата за изменение на настоящото решение, по-специално чрез въвеждане на допълнителни условия за извършването на предаване на данни или чрез ограничаване на обхвата на констатацията за адекватност на нивото на защита само до предаванията на данни, за които непрекъснатостта на защитата по смисъла на член 44 от ОРЗД е гарантирана.

([150]) 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.“

([151]) 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 ЕКЗД, Референтен документ относно адекватното ниво на защита, WP 254 rev. 01.

([152]) Вж. също приложение II, раздел IV: „При извършването на периодичния преглед на решението относно адекватното ниво на защита КЗЛИ и Европейската комисия ще обменят информация относно обработването на данни съгласно условията, посочени в констатацията за адекватно ниво на защита, включително изложените в настоящото изявление.“

(186) В частност, Комисията следва да започва процедурата за спиране на прилагането или за отмяна на решението, ако има индикации, че Допълнителните правила, 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 японските органи не спазват изявленията, гаранциите и ангажиментите, посочени в приложение II към настоящото решение.

(187) 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 японски органи не предоставят информацията или поясненията, необходими за оценката на нивото на защита на личните данни, предавани от Европейския съюз към Япония, или за спазването на настоящото решение. В тази връзка Комисията следва да взема предвид степента, в която съответната информация може да бъде набавена от други източници.

(188) При надлежно обосновани съображения за спешност, като например опасност от сериозно нарушаване на правата на субектите на данни, Комисията следва да разглежда необходимостта от приемане на решение — което ще следва да се прилага веднага — за спиране на прилагането или за отмяна на настоящото решение, съгласно предвиденото в член 93, параграф 3 от Регламент (ЕС) 2016/679 във връзка с член 8 от Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета ([153]).

8. **ЗАКЛЮЧИТЕЛНИ СЪОБРАЖЕНИЯ**

(189) Европейският комитет по защита на данните публикува становището си ([154]), като то бе взето предвид при изготвянето на настоящото решение.

(190) Европейският парламент прие резолюция относно стратегия за електронна търговия, в която призова Комисията да даде приоритет и ускори приемането на решения относно адекватността по отношение на важни търговски партньори и като спазва условията, предвидени в Регламент (ЕС) 2016/679, тъй като те са важен механизъм за осигуряване на гаранции при предаването на лични данни от Европейския съюз ([155]).Европейският парламент прие също така резолюция относно адекватността на нивото на защитата на личните данни, предоставяна от Япония ([156]).

(191) Мерките, предвидени в настоящото решение, са в съответствие със становището на комитета, учреден съгласно член 93, параграф 1 от ОРЗД,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

1. За целите на член 45 от Регламент (ЕС) 2016/679 Япония осигурява адекватно ниво на защита на личните данни, предавани от Европейския съюз към стопански субекти, третиращи лична информация в Япония, които са подчинени на Закона за защита на личната информация, допълнен с Допълнителните правила, посочени в приложение I, заедно с официалните изявления, гаранции и ангажименти, съдържащи се в приложение II.

([153]) Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

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

([155]) Европейски парламент, Резолюция от 12 декември 2017 г. „Към стратегия за електронна търговия“ (2017/2065 (INI)). Вж. по-специално точка 8 („[…] припомня, че лични данни могат да се предават на трети държави, без да се използват общи задължения в търговските споразумения, когато са изпълнени изискванията — както в настоящия момент, така и в бъдеще — заложени в […] глава V на Регламент (ЕС) 2016/679; признава, че решенията относно адекватността, включително частичните и специфичните решения за отделните сектори, представляват основен механизъм за защита на предаването на лични данни от ЕС към трета държава; отбелязва, че ЕС е приел решения относно адекватността само с четири от своите 20 най-големи търговски партньори…“) и точка 9 („призовава Комисията да даде приоритет и ускори приемането на решения относно адекватността, при условие че третите държави гарантират, по силата на вътрешното си законодателство или на международните си ангажименти, степен на защита, която „по същество е равностойна“ на гарантираната в ЕС …“).

([156]) Резолюция на Европейския парламент от 13 декември 2018 г. „Адекватност на нивото на защитата на личните данни, предоставяна от Япония“ (2018/2979 (RSP).

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) радио- и телевизионни оператори, издатели на вестници, комуникационни агенции или други организации на пресата (включително всички лица, които упражняват дейност, свързана с пресата), доколкото те обработват лични данни за целите на пресата;

б) лица, които по занятие упражняват писателска дейност, доколкото тя засяга лични данни;

в) университети и други организации или групи, които имат за цел извършването на академични проучвания, или лица, принадлежащи към такава организация или група, доколкото те обработват лични данни за целите на академични проучвания;

г) религиозни образувания, доколкото те обработват лични данни за целите на религиозни дейности (включително всички свързани дейности); както и

д) политически образувания, доколкото те обработват лични данни за целите на тяхната политическа дейност (включително всички свързани дейности).

Член 2

Когато компетентните органи в държавите членки упражнят, с цел защита на физическите лица във връзка с обработване на техни лични данни, правомощията си по член 58 от Регламент (ЕС) 2016/679 и това доведе до спиране или окончателна забрана на потоците от данни към конкретен стопански субект в Япония в рамките на приложното поле, посочено в член 1, 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, с цел да прецени дали Япония продължава да осигурява адекватно ниво на защита по смисъла на член 1.

2. Държавите членки и Комисията се информират взаимно за случаите, в които Комисията за защита на личната информация или всеки друг компетентен японски 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 японските 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 две 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 японски органи.

5. Ако Комисията открие признаци, че вече не се осигурява адекватно ниво на защита, тя информира компетентните японски власти. Ако е необходимо, Комисията може да реши да спре прилагането на настоящото решение, да го измени или отмени или да ограничи приложното му поле, по-специално, когато са налице признаци, че:

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

б) японските 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 японските публични органи за целите на наказателното правоприлагане или националната сигурност.

Комисията може да представи проект за такива мерки и когато липсата на съдействие от страна на японското правителство не позволява на Комисията да определи дали констатацията, съдържаща се в член 1, параграф 1 от настоящото решение, е засегната.

Член 4

Адресати на настоящото решение са държавите членки.

Съставено в Брюксел на 23 януари 2019 година.

За Комисията
Věra JOUROVÁ
Член на Комисията

ПРИЛОЖЕНИЕ 1

ДОПЪЛНИТЕЛНИ ПРАВИЛА СЪГЛАСНО ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНАТА ИНФОРМАЦИЯ ЗА ТРЕТИРАНЕТО НА ЛИЧНИ ДАННИ, ПРЕДАДЕНИ ОТ ЕС ВЪЗ ОСНОВА НА РЕШЕНИЕ ОТНОСНО АДЕКВАТНОСТТА

Съдържание

[Термини]

„Закон“	Законът за защита на личната информация (Закон № 57, 2003 г.).
„Постановление на Министерския съвет“	Постановление на Министерския съвет за прилагане на Закона за защита на личната информация (Постановление на Министерския съвет № 507, 2003 г.)
„Правила“	Правила за прилагане на Закона за защита на личната информация (Правила на Комисията за защита на личната информация № 3, 2016 г.)
„Насоки относно общите правила“	Насоки относно Закона за защита на личната информация (том относно общите правила) (Известие на Комисията за защита на личната информация № 65, 2015 г.)
„ЕС“	Европейският съюз заедно с неговите държави членки и, в светлината на Споразумението за ЕИП, Исландия, Лихтенщайн и Норвегия
„ОРЗД“	Регламент на Европейския парламент и на Съвета 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)
„решение относно адекватността“	Решението на Европейската комисия, че трета държава или територия в тази трета държава и др. осигурява адекватно ниво на защита на личните данни съгласно член 45 от ОРЗД.

За целите на извършването на взаимно и безпрепятствено предаване на лични данни между Япония и ЕС Комисията за защита на личната информация определи ЕС за чужда държава, която установява система за защита на личната информация, призната за разполагаща с равностойни стандарти на тези в Япония по отношение на защитата на правата и интересите на лицата въз основа на член 24 от Закона, а Европейската комисия по същото време реши, че Япония осигурява адекватно ниво на защита на личните данни съгласно член 45 от ОРЗД.

Взаимното и безпрепятствено предаване на лични данни между Япония и ЕС ще се извършва по начин, чрез който се осигурява високо ниво на защита на правата и интересите на лицата. За да се осигури това високо ниво на защита по отношение на получаваната от ЕС лична информация въз основа на решение относно адекватността и предвид факта, че, въпреки високата степен на сближаване между двете системи, съществуват някои значими разлики, Комисията за защита на личната информация прие настоящите допълнителни правила въз основа на разпоредбите на Закона по отношение на прилагането и др. на сътрудничество с правителствата на други страни и с оглед на осигуряване на подходящо третиране на личната информация, която стопански субекти, третиращи лична информация, получават от ЕС въз основа на решение относно адекватността, както и на подходящо и ефективно изпълнение на задълженията, посочени в такива правила ([1]).

([1]) Членове 4, 6, 8, 24, 60 и 78 от Закона и член 11 от Правилата.

По-специално, в член 6 от Закона е предвидено правомощие за предприемане на необходимите законодателни и други действия с цел осигуряване на засилена защита на личната информация и създаване на съобразена с международни норми система по отношение на личната информация чрез по-строги правила, които допълват и надхвърлят правилата, посочени в Закона и Постановлението на Министерския съвет. Поради това Комисията за защита на личната информация, в качеството си на компетентен орган за управлението на цялостното администриране на Закона, в съответствие с член 6 от Закона има правомощието да установи по-строги разпоредби, като формулира настоящите допълнителни правила, осигуряващи по-високо ниво на защита на правата и интересите на лицата по отношение на третирането на лични данни, получавани от ЕС въз основа на решение относно адекватността, включително по отношение на определението на лична информация, изискваща специална грижа, в съответствие с член 2, параграф 3 от Закона и запазените лични данни в съответствие с член 2, параграф 7 от Закона (включително по отношение на съответния период на запазване).

На тази основа допълнителните правила са обвързващи за третиращите лична информация стопански субекти, които получават лични данни, предавани от ЕС въз основа на решение относно адекватността, и така се задължават да спазват правилата. Тъй като правилата са правно обвързващи, спазването на всички права и задължения може да бъде осигурено от Комисията за защита на личната информация по същия начин като спазването на разпоредбите на Закона, който тези правила допълват с по-строги и/или по-подробни правила. В случай на нарушение на правата и задълженията, произтичащи от допълнителните правила, лицата могат да получат защита от съдилищата по същия начин като по отношение на разпоредбите на Закона, който тези правила допълват с по-строги и/или по-подробни правила.

Що се отнася до правоприлагането от страна на Комисията за защита на личната информация – в случай че стопански субект, третиращ лична информация, не спазва едно или повече от задълженията по допълнителните правила, Комисията за защита на личната информация има правомощието да приеме мерки в съответствие с член 42 от Закона. Що се отнася до личната информация, получавана от ЕС въз основа на решение относно адекватността, като цяло, ако стопански субект, третиращ лична информация, не предприеме действия в съответствие с препоръка, получена в съответствие с член 42, параграф 1 от Закона, без законно основание ([2]), това се смята за тежко нарушение с непосредствено отражение върху правата и интересите на дадено лице по смисъла на член 42, параграф 2 от Закона.

1) Лична информация, изискваща специална грижа (член 2, параграф 3 от Закона)

Член 2, параграф 3 от Закона

3) В настоящия закон „лична информация, изискваща специална грижа“ означава лична информация, която е свързана с расата, убежденията, социалния статус, медицинското досие, съдебното досие, факта, че са претърпени вреди в резултат от престъпление, или други описания на засегнатото лице и която съгласно постановление на Министерския съвет е определена като информация, чието третиране изисква специална грижа с цел засегнатото лице да не бъде подложено на несправедлива дискриминация, предразсъдъци или други неблагоприятни последици.

Член 2 от Постановлението на Министерския съвет

Описанията и др., които се посочват в постановление на Министерския съвет съгласно член 2, параграф 3 от Закона, са тези описания и др., които съдържат които и да е от следните сведения (с изключение на тези, посочени в медицинското досие или съдебното досие на засегнатото лице):

i) наличието на физически увреждания, умствени увреждания, психични разстройства (включително нарушения в развитието) или други физически и психически функционални увреждания по смисъла на правила на Комисията за защита на личната информация;

ii) резултатите от медицински или друг преглед (наречени „медицински преглед и др.“ в следващата точка) на заинтересованото лице за превенция и ранно откриване на заболяване, извършен от лекар или друго лице, изпълняващо задължения, свързани с медицината (наречени „лекар и др.“ в следващата точка);

iii) фактът, че на заинтересованото лице са предоставени насоки за подобряване на психическото или физическото състояние или са предписани медицински грижи или рецепта от страна на лекар и др. въз основа на резултатите от медицински преглед и др. или поради болест, нараняване или други психически или физически промени;

iv) фактът, че спрямо заинтересованото лице, в качеството му на заподозряно лице или ответник, са извършени арест, претърсване, изземване, задържане, наказателно преследване или други процедури, свързани с престъпление;

([2]) Под законно основание се разбира събитие от извънреден характер извън контрола на стопанския субект, третиращ лична информация, което не може да бъде разумно предвидено (например природни бедствия) или случай, в който необходимостта да се предприемат действия във връзка с дадена препоръка, издадена от Комисията за защита на личната информация в съответствие с член 42, параграф 1 от Закона, е отпаднала поради предприемането на алтернативни действия от страна на стопанския субект, третиращ лична информация, с които нарушението се отстранява напълно.

v) фактът, че спрямо заинтересованото лице, в качеството му на ненавършил пълнолетие нарушител или ненавършило пълнолетие лице, заподозряно в нарушение, е извършено разследване, предприети са мерки за наблюдение и защита, проведено е изслушване или е прието решение, приета е охранителна мярка или е извършена друга процедура, свързана със защитата на ненавършили пълнолетие лица, в съответствие с член 3, параграф 1 от Закона за ненавършилите пълнолетие лица.

Член 5 от Правилата

Физическите и психическите функционални увреждания, които се посочват в правилата на Комисията за защита на личната информация съгласно член 2, точка i) от Постановлението, са следните увреждания:

i) физическите увреждания, посочени в таблицата, приложена към Закона за благосъстоянието на лицата с физически увреждания (Закон № 283 от 1949 г.);

ii) умствените увреждания, посочени в Закона за благосъстоянието на лицата с умствени увреждания (Закон № 37 от 1960 г.);

iii) психичните разстройства, посочени в Закона за психичното здраве и благосъстоянието на лицата с психични разстройства (Закон № 123 от 1950 г.) (включително нарушенията в развитието, посочени в член 2, параграф 1 от Закона за подпомагане на лицата с нарушения в развитието и с изключение на умствените увреждания, посочени в Закона за благосъстоянието на лицата с умствени увреждания);

iv) болест, за която няма установени методи на лечение, или други специфични болести, чиято сериозност съгласно член 4, параграф 1 от Закона за цялостно подпомагане на ежедневния и социалния живот на лицата с увреждания (Закон № 123 от 2005 г.) е равностойна на тези, посочени от министъра на здравеопазването, труда и социалните грижи в споменатия параграф.

Ако лични данни, получени от ЕС въз основа на решение относно адекватността, съдържат данни за сексуалния живот, сексуалната ориентация или синдикалната принадлежност на дадено физическо лице, които в ОРЗД са определени като специални категории лични данни, стопанските субекти, третиращи лична информация, са задължени да третират тези лични данни по същия начин като личната информация, изискваща специална грижа, по смисъла на член 2, параграф 3 от Закона.

2) Запазени лични данни (член 2, параграф 7 от Закона)

Член 2, параграф 7 от Закона

7) В настоящия закон „запазени лични данни“ означава лични данни, за които даден стопански субект, третиращ лична информация, има право да разкрива, коригира, допълва или изтрива тяхното съдържание, да прекратява тяхната употреба, да ги заличава или да прекратява предоставянето им на трети страни и които не са такива, за които в постановление на Министерския съвет е посочено, че е възможно да накърнят обществения интерес или други интереси, ако тяхното наличие или отсъствие бъде оповестено, нито такива, които трябва да бъдат изтрити в срок от не повече от една година съгласно Постановлението на Министерския съвет.

Член 4 от Постановлението на Министерския съвет

Данните, които се посочват в постановление на Министерския съвет съгласно член 2, параграф 7, са тези лични данни:

i) във връзка с които съществува риск от увреждане на живота, телесната неприкосновеност или имуществото на дадено засегнато лице или трета страна, ако наличието или отсъствието на въпросните лични данни бъде оповестено;

ii) във връзка с които съществува риск от насърчаване или предизвикване на незаконно или несправедливо действие, ако наличието или отсъствието на въпросните лични данни бъде оповестено;

iii) във връзка с които съществува риск от застрашаване на националната сигурност, разрушаване на връзките на доверие с друга държава или международна организация или изпадане в неизгодна позиция при преговори с друга държава или международна организация, ако наличието или отсъствието на въпросните лични данни бъде оповестено;

iv) във връзка с които съществува риск от възпрепятстване на поддържането на обществения ред и сигурност, например предотвратяването, противодействието или разследването на престъпления, ако наличието или отсъствието на въпросните лични данни бъде оповестено.

Член 5 от Постановлението на Министерския съвет

Срокът, предвиден в Постановлението на Министерския съвет съгласно член 2, параграф 7 от Закона, е шест месеца.

Личните данни, получени от ЕС въз основа на решение относно адекватността, трябва да се третират като запазени лични данни по смисъла на член 2, параграф 7 от Закона, независимо от срока, в който те трябва да бъдат заличени.

Ако лични данни, получени от ЕС въз основа на решение относно адекватността, попадат в обхвата на лични данни, за които в Постановлението на Министерския съвет е посочено, че е „възможно да накърнят обществения интерес или други интереси, ако тяхното наличие или отсъствие бъде оповестено“, не се изисква тези данни да бъдат третирани като запазени лични данни (вж. член 4 от Постановлението на Министерския съвет, Насоки относно общите правила, „2-7. Запазени лични данни“).

3) Посочване на цел на употреба, ограничение поради цел на употреба (член 15, параграф 1, член 16, параграф 1 и член 26, параграфи 1 и 3 от Закона)

Член 15, параграф 1 от Закона

1) Когато третират лична информация, стопанските субекти, третиращи лична информация, посочват целта на употребата на личната информация (наричана по-нататък „цел на употреба“) по възможно най-ясен начин.

Член 16, параграф 1 от Закона

1) Стопанските субекти, третиращи лична информация, не третират лична информация, без предварително да са получили съгласието на засегнатите лица, отвъд необходимото за постигане на цел на употреба, посочена в съответствие с разпоредбите на предходния член.

Член 26, параграфи 1 и 3 от Закона

1) Когато стопански субект, третиращ лична информация, получава лични данни от трета страна, той потвърждава следните сведения в съответствие с правилата на Комисията за защита на личната информация. (пропуснато)

i) (пропуснато)

ii) обстоятелствата, при които въпросната трета страна е придобила тези лични данни;

3) Когато стопански субект, третиращ лична информация, в съответствие с разпоредбите на параграф 1 е извършил потвърждение, той пази запис за датата на получаване на личните данни, сведение относно въпросното потвърждение и други сведения съгласно правилата на Комисията за защита на личната информация.

Ако стопански субекти, третиращи лична информация, третират лична информация отвъд необходимото за постигане на цел на употреба, посочена в член 15, параграф 1 от Закона, те получават съгласието на заинтересованото лице предварително (член 16, параграф 1 от Закона). Когато получават лични данни от трета страна, стопанските субекти, третиращи лична информация, потвърждават в съответствие с Правилата различни сведения, като например обстоятелствата, при които тези лични данни са придобити от въпросната трета страна, и записват тези сведения (член 26, параграфи 1 и 3 от Закона).

Когато стопански субект, третиращ лична информация, получава лични данни от ЕС въз основа на решение относно адекватността, обстоятелствата по отношение на придобиването на тези лични данни, които се потвърждават и записват в съответствие с член 26, параграфи 1 и 3, включват целта на употреба, поради която данните са получени от ЕС.

По подобен начин, когато стопански субект, третиращ лична информация, получава от друг стопански субект, третиращ лична информация, лични данни, предадени преди това от ЕС въз основа на решение относно адекватността, обстоятелствата по отношение на придобиването на тези лични данни, които се потвърждават и записват в съответствие с член 26, параграфи 1 и 3, включват целта на употреба, поради която данните са получени.

В горепосочените случаи от стопанския субект, третиращ лична информация, се изисква да посочва целта на употреба на въпросните лични данни в обхвата на целта на употреба, поради която данните са получени първоначално или впоследствие, както е потвърдено и записано в съответствие с член 26, параграфи 1 и 3, и да използва тези данни в рамките на въпросния обхват (както е посочено в член 15, параграф 1 и член 16, параграф 1 от Закона).

4) Ограничение за предоставяне на трета страна в чужда държава на лични данни (член 24 от Закона; Член 11-2 от Правилата)

Член 24 от Закона

Освен в случаите, посочени във всяка точка на параграф 1 от предходния член, когато стопански субект, третиращ лична информация, предоставя на трета страна (с изключение на лице, което установява система, отговаряща на стандартите, посочени в правилата на Комисията за защита на личната информация, поради необходимост от непрекъснато предприемане на действия, които са равностойни на тези, които стопанските субекти, третиращи лична информация, вземат по отношение на третирането на лични данни в съответствие с разпоредбите на настоящия раздел; по-нататък същото в настоящия член) в чужда държава (държава или регион извън територията на Япония; по-нататък същото) (с изключение на тези, посочени съгласно правилата на Комисията за защита на личната информация като чужди държави, които установяват система за защита на личната информация, призната за разполагаща с равностойни стандарти на тези в Япония по отношение на защитата на правата и интересите на лицата; по-нататък същото в настоящия член) лични данни, получава предварително съгласието на заинтересованото лице за предоставянето на данните на трета страна в чужда държава. В този случай разпоредбите на предходния член не се прилагат.

Член 11-2 от Правилата

Стандартите, които се посочват в правилата на Комисията за защита на личната информация в съответствие с член 24 от Закона, трябва да включват всеки от следните елементи:

i) стопанският субект, третиращ лична информация, и лицето, което получава лични данни, са осигурили по отношение на третирането на личните данни от лицето, което получава данните, прилагането на мерките в съответствие с разпоредбите на глава IV, раздел I от Закона чрез подходящ и разумен метод;

ii) лицето, което получава личните данни, е получило признаване въз основа на международна рамка относно третирането на лична информация.

Когато стопански субект, третиращ лична информация, предоставя на трета страна в чужда държава лични данни, които е получил от ЕС въз основа на решение относно адекватността, получава предварително съгласието на заинтересованото лице за предоставянето на данните на трета страна в чужда държава в съответствие с член 24 от Закона, след като на заинтересованото лице е била предоставена необходимата информация за обстоятелствата около предаването на данните, за да може то да вземе решение относно съгласието си, с изключение на случаите по следните точки:

i) когато третата страна е в държава, посочена съгласно Правилата като чужда държава, която установява система за защита на личната информация, призната за разполагаща с равностойни стандарти на тези в Япония по отношение на защитата на правата и интересите на лицата;

ii) когато стопанският субект, третиращ лична информация, и третата страна, която получава личните данни, са предприели по отношение на третирането на личните данни от третата страна мерки, осигуряващи ниво на защита, равностойно на посоченото в Закона, четен заедно с настоящите Правила, чрез подходящ и разумен метод (договор, други форми на обвързващи споразумения или обвързващи договорености в рамките на корпоративна група);

iii) в случаите по всяка от точките на член 23, параграф 1 от Закона.

5) Анонимно обработена информация (член 2, параграф 9 и член 36, параграфи 1 и 2 от Закона)

Член 2, параграф 9 от Закона

9) В настоящия закон „анонимно обработена информация“ означава информация, свързана с дадено физическо лице, която може да бъде изготвена в резултат от обработката на лична информация по начин, който не позволява нито идентифицирането на физическото лице чрез действията, посочени в следните точки в съответствие с разделението на личната информация във всяка от тези точки, нито възстановяването на личната информация.

i) лична информация, попадаща в обхвата на параграф 1, точка i);

Заличаване на част от описания и др., съдържащи се във въпросната лична информация (включително замяна на посочената част от описания и др. с други описания и др. посредством нерегулярен метод, който не позволява възстановяването на посочената част от описания и др.);

ii) лична информация, попадаща в обхвата на параграф 1, точка ii);

Заличаване на всички лични идентификационни кодове, съдържащи се във въпросната лична информация (включително замяна на посочените лични идентификационни кодове с други описания и т.н. посредством нерегулярен метод, който не позволява възстановяването на посочените лични идентификационни кодове).

Член 36, параграф 1 от Закона

1) Стопански субект, който третира лична информация, следва, когато изготвя анонимно обработена информация (ограничена до информацията, включена в анонимно обработвани бази данни и др., по-нататък също), да обработва личната информация в съответствие със стандартите, посочени в правилата на Комисията за защита на личната информация като необходими, за да се гарантира невъзможността да се идентифицира дадено физическо лице и да се възстанови личната информация, използвана за изготвянето на анонимните данни.

Член 19 от Правилата

Стандартите, предвидени в правилата на Комисията за защита на личната информация в член 36, параграф 1 от Закона, са следните:

i) заличаване изцяло или частично на описанията и др., съдържащи се в лична информация, чрез които може да се идентифицира дадено физическо лице (включително замяна на такива описания и др. с други описания и т.н. посредством нерегулярен метод, който не позволява възстановяването на целите описания и др. или части от тях);

ii) заличаване на всички лични идентификационни кодове, съдържащи се в лична информация (включително замяна на такива кодове с други описания и т.н. посредством нерегулярен метод, който не позволява възстановяването на отделните идентификационни кодове);

iii) заличаване на кодовете (само кодовете, свързващи множествена информация действително третирана от стопански субект, третиращ лична информация), които свързват лична информация и информация, получена в резултат от предприетите мерки спрямо личната информация (включително замяна на упоменатите кодове с други кодове, които не могат да свържат посочената лична информация и информацията, получена в резултат от предприети мерки спрямо тази лична информация, с помощта на нерегулярен метод, който не позволява възстановяването на посочените кодове);

iv) заличаване на характерни описания и др. (включително замяна на такива описания и др. с други описания и др. с помощта на нерегулярен метод, който не позволява възстановяването на характерните описания и др.);

v) освен действията, изложени във всички предходни точки, предприемане на подходящи действия въз основа на отчитане на атрибутите и др. на базите данни с лична информация, като например разлика между описания и др., съдържащи се в лична информация, и описания и др., съдържащи се в друга лична информация, включена в базата данни с лична информация, която съдържа упоменатата лична информация.

Член 36, параграф 2 от Закона

2) При изготвянето на анонимно обработена информация и в съответствие със стандартите, посочени в правилата на Комисията за защита на личната информация като необходими за предотвратяване на изтичането на информация, свързана с описания и т.н. и индивидуални идентификационни кодове, заличени от лична информация, използвана за изготвянето на анонимно обработена информация, и информация, свързана с метод на обработка, използван в съответствие с разпоредбите на предходния параграф, даден стопански субект, третиращ лична информация, следва да предприема действия за контрол на сигурността на тази информация.

Член 20 от Правилата

Стандартите, предвидени в правилата на Комисията за защита на личната информация в член 36, параграф 2 от Закона, са следните:

i) ясно определяне на правомощията и отговорността на всяко лице, третиращо информация, свързана с описанията и т.н. и индивидуалните идентификационни кодове, които са били заличени от лична информация, използвана за изготвянето на анонимно обработена информация, и информация, свързана с даден метод на обработване, приложен съгласно разпоредбите на член 36, параграф 1 (ограничено до информация, чието използване може да доведе до възстановяване на личната информация) (наричана по-нататък „информация, отнасяща се до метода на обработване и др.“ в настоящия член);

ii) установяване на правила и процедури относно третирането на информация, отнасяща се до метода на обработване и др., подходящо третиране на информация, отнасяща се до метода на обработване и др., в съответствие с правилата и процедурите, като се оценяват условията на третирането и въз основа на оценката се предприемат необходимите действия за подобрение;

iii) предприемане на необходими и подходящи действия за възпрепятстване на лицата, които нямат законни правомощия да третират информация, отнасяща се до метода на обработване и др., да третират такава информация.

Личната информация, получена от ЕС въз основа на решение относно адекватността, се счита за анонимно обработена информация по смисъла на член 2, параграф 9 от Закона единствено ако стопанският субект, третиращ лична информация, предприема мерки, посредством които анонимизирането на лицата става необратимо за всеки, включително като заличава информацията, отнасяща се до метода на обработване и др. (т.е. информацията, свързана с описанията и др. и индивидуалните идентификационни кодове, които са били заличени от личната информация, използвана за изготвянето на анонимно обработена информация, и информацията, свързана с даден метод на обработване, приложен съгласно разпоредбите на член 36, параграф 1 от Закона (ограничено до информация, чието използване може да доведе до възстановяване на личната информация).

ПРИЛОЖЕНИЕ 2

Нейно Превъзходителство г-жа Вера Йоурова, комисар на Европейската комисия по въпросите на правосъдието, потребителите и равнопоставеността между половете

Ваше Превъзходителство,

Приветствам конструктивните дискусии между Япония и Европейската комисия, насочени към изграждането на рамка за предаването на лични данни между ЕС и Япония.

В резултат от искането, отправено от Европейската комисия до правителството на Япония, изпращам приложен документ, в който се прави преглед на правната рамка относно достъпа до информация от правителството на Япония.

Този документ се отнася до много министерства и агенции на правителството на Япония, а по отношение на съдържанието на документ, съответните министерства и агенции (секретариат на Министерския съвет, Национална полицейска служба, Комисия за защита на личната информация, Министерството на вътрешните работи и съобщенията, Министерството на правосъдието, Агенция „Разузнаване във връзка с обществената сигурност“, Министерство на отбраната) са отговорни за пасажите, свързани с обхвата на техните съответни компетенции. Моля, вижте по-долу въпросните министерства и агенции заедно със съответните подписи.

Комисията за защита на личната информация приема всякакви въпроси по този документ и ще координира необходимите отговори между съответните министерства и агенции.

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,

Yoko Kamikawa

Министър на правосъдието

Настоящият документ е изготвен от Министерството на правосъдието и следните министерства и агенции.

Koichi Hamano

Съветник, секретариат на Министерския съвет

Schunichi Kuryu

Генерален комисар на Националната полицейска служба

Mari Sonoda

Генерален секретар на Комисията за защита на личната информация

Mitsuru Yasuda

Заместник-министър в Министерството на вътрешните работи и съобщенията

Seimei Nakagawa

Агенция „Разузнаване във връзка с обществената сигурност“

Kenichi Takahashi

Административен заместник-министър на отбраната

14 септември 2018 г.

Събиране и използване на лична информация от японските публични органи за целите на наказателното правоприлагане и националната сигурност

Настоящият документ предоставя преглед на правната рамка за събирането и използването на лична (електронна) информация от японските публични органи за целите на наказателното правоприлагане и националната сигурност (наричано по-нататък „достъп на държавните органи“), по-специално по отношение на наличните правни основания, приложимите условия (ограничения) и гаранции, включително възможностите за независим надзор и индивидуална защита. Този преглед е адресиран до Европейската комисия с оглед изразяване на ангажимент и предоставяне на гаранции, че достъпът на държавните органи до лична информация, предавана от ЕС на Япония, ще бъде ограничен до това, което е необходимо и пропорционално, и подложен на независим надзор и че засегнатите лица ще могат да получат правна защита в случай на евентуално нарушение на основните им права на неприкосновеност на личния живот и защита на данните. В документа се предвижда също създаването на нов механизъм за правна защита, управляван от Комисията за защита на личната информация (КЗЛИ), в рамките на който ще се разглеждат жалби от граждани на ЕС относно достъпа на държавните органи до техните лични данни, предадени от ЕС на Япония.

I. **Общи правни принципи от значение за достъпа на държавните органи**

Тъй като представлява израз на упражняване на публична власт, достъпът на държавните органи трябва да се осъществява при пълно зачитане на закона (принцип за законност). В Япония личната информация както в частния, така и публичния сектор е защитена от многослоен механизъм.

А. Конституционна рамка и принцип за законност

В член 13 от Конституцията и в съдебната практика правото на неприкосновеност на личния живот се признава като конституционно право. В тази връзка Върховният съд постанови, че е естествено физическите лица да не желаят тяхната лична информация да бъде оповестявана на трети лица без основателна причина и че това тяхно желание следва да бъде защитено ([1]). Допълнителна защита е включена в член 21, параграф 2 от Конституцията, който гарантира зачитането на тайната на съобщенията, и член 35 от Конституцията, който гарантира правото на лицата да не бъдат обект на претърсвания и изземвания без съдебна заповед, т.е. събирането на лична информация, включително достъпът, чрез принудителни средства винаги трябва да се основава на съдебна заповед. Подобна заповед може да бъде издадена само за разследването на вече извършено престъпление. Поради това в правната уредба на Япония събирането на информация чрез принудителни средства за целите на (не наказателно разследване, а) националната сигурност, не се разрешава.

Освен това в съответствие с принципа за законност принудителното събиране на информация трябва да бъде изрично разрешено от закона. В случай на непринудително/доброволно събиране, информацията се придобива от източник със свободен достъп или въз основа на искане за доброволно разкриване, т.е. искане, което не може да бъде наложено на физическото или юридическото лице, което разполага с информацията. Това обаче е допустимо единствено доколкото публичният орган е компетентен за провеждане на разследването, като се има предвид, че всеки публичен орган може да действа единствено в рамките на своята административна юрисдикция, предвидена от закона (независимо дали неговите дейности засягат правата и свободите на физически лица). Този принцип се отнася до способността на органа да събира лична информация.

Б. Специални правила относно защитата на лична информация

Законът за защита на личната информация (ЗЗЛИ) и Законът за защита на лична информация, съхранявана от административни органи (ЗЗЛИСАО), които се основават на Конституцията и съдържат допълнителни подробности относно нейните разпоредби, гарантират правото на лична информация както в частния, така и в публичния сектор.

Член 7 от ЗЗЛИ постановява, че КЗЛИ следва да формулира „Основна политика за защита на личната информация“ (Основна политика). Основната политика, която е приета с решение на Министерския съвет в качеството му на централен орган на японското правителство (министър-председател и министри), определя насоките за защитата на личната информация в Япония. По този начин КЗЛИ, в качеството си на независим надзорен орган, служи като „команден център“ на системата за защита на личната информация в Япония.

Винаги когато даден административен орган събира лична информация, независимо дали това става чрез принудителни средства или не, по принцип ([2]) той трябва да спазва изискванията на ЗЗЛИСАО. ЗЗЛИСАО е общ закон, приложим за обработката на „запазена лична информация“ ([3]) от „административни органи“ (както са определени в член 2, параграф 1 от ЗЗЛИСАО). Поради това той обхваща съответно и обработката на данни в областта на наказателното правоприлагане и националната сигурност. Сред публичните органи, оправомощени да прилагат достъп на държавни органи, всички органи с

([1]) Върховен съд, решение от 12 септември 2003 г. (2002(Ju) № 1656).

([2]) За изключения във връзка с глава 4 от ЗЗЛИСАО, вж. по-долу т. 16.

([3]) „Запазена лична информация“ в член 2, параграф 5 от ЗЗЛИСАО означава лична информация, изготвена или получена от служител на даден административен орган в хода на негови служебни задължения и съхранявана от административния орган за служебна употреба от страна на неговите служители.

изключение на полицията на префектурите се считат за национални държавни органи, попадащи в обхвата на определението за „административни органи“. Обработването на лична информация от полицията на префектурите се урежда от наредби на префектите ([4]), с които се определят принципите за защита на личната информация, права и задължения, равностойни на тези в ЗЗЛИСАО.

II. **Достъп на държавните органи за целите на наказателното правоприлагане**

А) Правни основания и ограничения

1) Събиране на лична информация чрез принудителни средства

а) Правни основания

Съгласно член 35 от Конституцията, правото на всички лица техните домове, документи и вещи да бъдат защитени от достъп, претърсвания и изземвания не трябва да се нарушава освен при наличието на съдебна заповед, издадена въз основа на „достатъчен повод“ и описваща конкретното място, което да бъде претърсено, и нещата, които да бъдат иззети. Следователно принудителното събиране на електронна информация от органи на публичната власт в рамките на дадено наказателно разследване може да се извършва само въз основа на съдебна заповед. Това се отнася както за събирането на електронни записи, съдържащи (лична) информация, така и за прихващането на съобщения в реално време (т.нар. подслушване). Единственото изключение от това правило (което обаче не важи в контекста на електронното предаване на лична информация от чужбина) е член 220, параграф 1 от Наказателно-процесуалния кодекс ([5]), съгласно който прокурор, помощник прокурор или служител на съдебната полиция може, при задържането на заподозряно лице или хванат на местопрестъплението нарушител, да извърши, ако е необходимо, претърсване и изземване на място по време на ареста.

В член 197, параграф 1 от Наказателно-процесуалния кодекс се предвижда принудителните мерки за разследване да „не се прилагат, освен ако в настоящия кодекс не са предвидени специални разпоредби“. Правните основания по отношение на принудителното събиране на електронна информация са член 218, параграф 1 от Наказателно-процесуалния кодекс (съгласно който прокурор, помощник прокурор или служител на съдебната полиция може, ако това е необходимо за разследването на престъпление, да извърши претърсване, изземване или проверка въз основа на заповед, издадена от съдия) и член 222-2 от Наказателно-процесуалния кодекс (съгласно който принудителни мерки за прихващане на електронни съобщения без съгласието на всяка от страните се прилагат въз основа на други закони). Последната разпоредба препраща към Закона за подслушването за целите на наказателното разследване (Закон за подслушването), където в член 3, параграф 1 се предвиждат условията, при които съобщенията, свързани с някои тежки престъпления, могат да бъдат подслушвани въз основа на съдебна заповед, издадена от съдия ([6]).

По отношение на полицията, отговорност за разследването на всички престъпления носи полицията на префектурите, докато Национална служба „Полиция“ (НСП) не извършва никакви наказателни разследвания въз основа на Наказателно-процесуалния кодекс.

б) Ограничения

Принудителното събиране на електронна информация е ограничено от Конституцията и закона за делегиране на правомощия в съответствие с тълкуването им в съдебната практика, в която по-специално са посочени критериите, които да се прилагат от съда при издаването на съдебна заповед. Освен това ЗЗЛИСАО налага редица ограничения, приложими както за събирането, така и за третирането на информация (а местните наредби възпроизвеждат до голяма степан същите критерии за полицията на префектурите).

1) Ограничения, произтичащи от Конституцията и закона за делегиране на правомощия

Съгласно член 197, параграф 1 от Наказателно-процесуалния кодекс, принудителни разпоредби „не се прилагат, освен ако в настоящия кодекс не са предвидени специални разпоредби“. В член 218, параграф 1 от Наказателно-процесуалния кодекс се посочва, че изземването и др. могат да се извършват въз основа на заповед, издадена от съдия, само „ако е необходимо за

([4]) Всяка префектура има своя „наредба на префекта“ относно защитата на лична информация от полицията на префектурата. Не съществува превод на английски на текстовете на тези наредби.

([5]) В член 220, параграф 1 от Наказателно-процесуалния кодекс се предвижда, когато прокурор, помощник прокурор или служител на съдебната полиция извършват арест на заподозряно лице, те да могат, ако е необходимо, да предприемат следните мерки: а) влизане в жилището на друго лице и др. с цел търсене на заподозряното лице; б) претърсване, изземване или проверка на място по време на ареста.

([6]) По-специално тази разпоредба предвижда, че „прокурорът или служителят от съдебната полиция може, в случаите попадащи в някоя от следните точки, когато е налице ситуация, която предполага в достатъчна степен, че ще се проведе комуникация във връзка с извършване или подготовка на престъпление, конспирация за последващи действия, като например унищожаване на доказателства и др., инструкции и друга комуникация относно престъплението, посочено във всяка една от точките (по-долу наричани „серия престъпления“ във втора и трета точка), както и комуникация, съдържаща подробности за съответното престъпление (наричани по-долу в този параграф „комуникации, свързани с престъпление“), и в случаите, когато е изключително трудно престъпникът да бъде идентифициран или ситуациите/подробностите по подготовката да бъдат уточнени по друг начин, да подслушва комуникации, свързани с престъпление, въз основа на съдебна заповед за подслушване, издадена от съдия и посочваща средствата за комуникация, уточнени с телефонен номер и други номера/кодове за идентифициране на източника или получателя на телефонното обаждане, които заподозряното лице използва въз основа на договор с телефонен оператор и др. (освен комуникациите, за които не е налице подозрение, че са „комуникации, свързани с престъпление“) или комуникации, за които има основания да се подозира, че ще бъдат използвани като „комуникации, свързани с престъпление“. Така подслушването на комуникации, свързани с престъпление чрез съответното средство за комуникация може да бъде извършено.“

разследването на престъпление“. Въпреки че критериите за определяне на необходимостта не са допълнително уточнени в позитивното право, Върховният съд ([7]) е постановил, че за да се оцени необходимостта от определени разпоредби, съдията следва да извърши цялостна оценка, като вземе предвид по-специално следните елементи:

а) сериозност на престъплението и начин на извършването му;

б) стойност и значение на иззетите като доказателства материали;

в) вероятност иззетите материали да бъдат укрити или унищожени;

г) степен на неблагоприятните последици, причинени от изземването;

д) други имащи отношение условия.

Ограниченията са следствие и от изискването в член 35 от Конституцията да се демонстрира наличието на „достатъчен повод“. Съгласно стандарта за „достатъчен повод“ заповеди могат да се издават, ако: [1] съществува необходимост от наказателно разследване (вж. решението на Върховния съд от 18 март 1969 г. (1968 (Shi) № 100), посочено по-горе), [2] е налице ситуация, при която се смята, че заподозряното лице (обвиняемият) е извършило престъпление (член 156, параграф 1 от Правилата за наказателното производство) ([8]) [3] Заповедта за разследване на тялото, вещите, жилището или всяко друго местонахождение на лице, различно от заподозряното лице, следва да се издава единствено когато може да се предполага с основание, че вещите, които следва да бъдат иззети, съществуват (член 102, параграф 2 от Наказателно-процесуалния кодекс). Когато съдията счита, че документните доказателства, представени от разследващите органи не дават достатъчно основание да се подозира извършването на престъпление, той отхвърля искането за издаване на съдебна заповед. В това отношение следва да се отбележи, че съгласно Закона за наказване на организираната престъпна дейност и контрол на облагите от престъпна дейност „подготвителните актове“ за извършване на планирано престъпление (напр. събиране на средства за извършване на терористичен акт) сами по себе си представляват престъпления и поради това може да бъдат обект на задължително разследване въз основа на съдебна заповед.

Не на последно място, когато заповедта се отнася до разследване на тялото, вещите, жилището или всяко друго местонахождение на лице, различно от заподозряното или обвиняемото лице, тя се издава само когато има основания да се допусне, че вещите, които ще бъдат иззети, съществуват (член 102, параграф 2 и член 222, параграф 1 от Наказателно-процесуалния кодекс).

Що се отнася конкретно до прихващането на съобщения за целите на наказателното разследване въз основа на Закона за подслушването, то може да се извършва само ако строгите изисквания, предвидени в член 3, параграф 1 от този Закон, са изпълнени. Съгласно тази разпоредба за прихващането винаги се изисква предварителна съдебна заповед, която се издава само в ограничен брой случаи ([9]).

2) Ограничения, произтичащи от ЗЗЛИСАО

Що се отнася до събирането ([10]) и по-нататъшното третиране (включително по-специално запазването, управлението и използването) на лична информация от административните органи, ЗЗЛИСАО предвижда по-специално следните ограничения:

а) Съгласно член 3, параграф 1 от ЗЗЛИСАО, административните органи могат да запазват лична информация само когато това се налага за изпълнението на функциите, попадащи в обхвата на тяхната компетентност, както е предвидено в законовите и подзаконовите актове. Когато запазват лична информация, от тях се изисква също така да уточнят (доколкото е възможно) за каква цел ще я използват. Съгласно член 3, параграфи 2 и 3 от ЗЗЛИСАО, административните органи не запазват лична информация извън обхвата, необходим за постигането на целта на така уточнената употреба, и не променят целта на употребата повече от това, което разумно може да се счита за подходящо по отношение на първоначалната цел.

б) Съгласно член 5 от ЗЗЛИСАО ръководителят на административен орган полага усилия да поддържа запазената лична информация точна и актуална дотолкова, доколкото това е необходимо за постигане на целта на употребата на данните.

в) Съгласно член 6, параграф 1 от ЗЗЛИСАО ръководителят на административен орган взема необходимите мерки за предотвратяване на изтичане, загуба или увреждане на запазените лични данни, както и за доброто им управление.

г) Съгласно член 7 от ЗЗЛИСАО никой служител, включително бивш служител, не може да разкрива придобитата лична информация на друго лице без основателна причина или да използва тази информация за несправедлива цел.

([7]) Решение от 18 март 1969 г. (1968 (Shi) № 100).

([8]) Член 156, параграф 1 от Правилата за наказателното производство гласи: „При подаване на заявката, посочена в параграф 1 от предходния член, заявителят предоставя материали, въз основа на които заподозреният или обвиняемият следва да се счита за извършил престъпление.“

([9]) Вж. бележка под линия 6.

([10]) В член 3, параграфи 1 и 2 от ЗЗЛИСАО се ограничава степента на запазване, а по този начин и събирането на лична информация.

д) Освен това съгласно член 8, параграф 1 от ЗЗЛИСАО ръководителят на административен орган не трябва да използва запазени лични данни или да ги предоставя на друго лице за цели, различни от посочената цел на употребата, освен ако в законовите и подзаконовите актове е предвидено друго. В член 8, параграф 2 се съдържат изключения от това правило в определени случаи, но те важат само ако извънредното разкриване на данни е малко вероятно да причини „несправедлива“ вреда на правата и интересите на субекта на данните или на трето лице.

е) Съгласно член 9 от ЗЗЛИСАО, когато запазената лична информация се предоставя на друго лице, ръководителят на административен орган налага ограничения, ако е необходимо, върху целта или метода на употреба или всякакви други необходими ограничения. Ръководителят може също така да поиска от получаващото лице да вземе необходимите мерки за предотвратяване на изтичане на информацията и за доброто ѝ управление.

ж) Съгласно член 48 от ЗЗЛИСАО ръководителят на административен орган се стреми да обработва всички жалби по отношение на третирането на лична информация надлежно и експедитивно.

2) Събиране на лична информация чрез заявки за доброволно сътрудничество (Доброволно разследване)

а) Правно основание

Освен чрез принудителни средства личната информация се получава или от свободно достъпен източник или благодарение на доброволно разкриване на информация, включително от страна на стопански субекти, притежаващи такава информация.

По отношение на втория случай с член 197, параграф 2 от Наказателно-процесуалния кодекс на прокуратурата и съдебната полиция се дават правомощия да извършват „писмени запитвания в областта на разследванията“ (т.нар. „въпросници“). Съгласно Наказателно-процесуалния кодекс от запитаните лица се иска да докладват на разследващите органи. Въпреки това няма начин те да бъдат принудени да докладват, ако публичните служби или публичните и/или частните организации, които са получили запитванията, откажат да се съобразят. Ако те не отговорят на запитванията, не може да им бъде наложена наказателна или друга санкция. Ако разследващите органи смятат исканата информация за абсолютно необходима, те трябва да си я набавят чрез претърсване и изземване въз основа на съдебна заповед.

Като се има предвид нарастващото познаване от страна на лицата на техните права на неприкосновеност на личния живот, както и обемът на работата, създаван от такива искания, стопанските субекти стават все по-предпазливи при отговора на подобни искания ([11]). Когато решават дали да сътрудничат, стопанските субекти вземат предвид естеството на поисканата информация, връзката им с лицето, чиято информация е засегната, рисковете за репутацията им, рисковете от съдебни спорове, и др.

б) Ограничения

Що се отнася до принудителното събиране на електронна информация, доброволното разследване е ограничено от Конституцията, според тълкуванията в съдебната практика, както и от закона за делегиране на правомощия. Освен това стопанските субекти нямат законно право да разкриват информация в определени ситуации. Не на последно място в ЗЗЛИСАО са предвидени редица ограничения както за събирането, така и за третирането на информация (като местните наредби възпроизвеждат по същество същите критерии за полицията на префектурите).

1) Ограничения, произтичащи от Конституцията и закона за делегиране на правомощия

Предвид член 13 от Конституцията Върховният съд налага ограничения за доброволните разследвания, извършвани от разследващи органи, в две решения от 24 декември 1969 г. (1965 (A) № 1187) и 15 април 2008 г. (2007 (A) № 839). Тези решения се отнасят до случаи, в които личната информация (под формата на изображения) е събрана чрез фотографиране или филмиране, но констатациите важат и за доброволните (непринудителни) разследвания, свързани с намеса в личния живот на лицата като цяло. Поради това те важат и трябва да се спазват и по отношение на събирането на лична информация чрез доброволни разследвания, като се имат предвид специфичните обстоятелства във всеки отделен случай.

Съгласно тези решения законосъобразността на доброволните разследвания зависи от изпълнението на три критерия, а именно:

— „подозрение за престъпление“ (т.е. трябва да се прецени дали е извършено престъпление),

— „необходимост от разследване“ (т.е. трябва да се прецени дали искането остава в рамките на това, което е необходимо за целите на разследването), както и

([11]) Вж. също уведомлението, издадено от Национална служба „Полиция“ на 7 декември, 1999 г. (по-долу), в което се изтъква същият аргумент.

— „целесъобразност на методите“ (т.е. трябва да се прецени дали доброволното разследване е „подходящо“ или разумно от гледна точка на постигането на целите на разследването) ([12]).

Като цяло, като се вземат предвид горепосочените три критерия, законосъобразността на доброволните разследвания се оценява от гледна точка на това дали те могат да се считат за разумни в съответствие със социално приетите стандарти.

Изискването разследването да бъде „необходимо“ произтича също така директно от член 197 от Наказателно-процесуалния кодекс и е потвърдено в инструкциите на Национална служба „Полиция“ (НСП) към полицията на префектурите по отношение на използването на „въпросници“. В уведомлението на НСП от 7 декември 1999 г. са определени редица процесуални ограничения, включително изискването за използване на „въпросници“ само ако това е необходимо за целите на разследването. Освен това член 197, параграф 1 от Наказателно-процесуалния кодекс е ограничен до наказателни разследвания и поради това може да се прилага само когато е налице конкретно съмнение за вече извършено престъпление. От друга страна това правно основание не важи за събирането и използването на лична информация, когато все още няма нарушение на закона.

2) Ограничения по отношение на определени стопански субекти

В някои области важат допълнителни ограничения въз основа на защитата, предоставена с други закони.

Най-напред разследващите органи и телекомуникационните компании, които разполагат с лични данни, са длъжни да спазват поверителността на съобщенията, гарантирана с член 21, параграф 2 от Конституцията ([13]). Освен това телекомуникационните компании имат същото задължение по силата на член 4 от Закона за далекосъобщенията ([14]). В съответствие с „Насоките за защита на личните данни в далекосъобщенията“, издадени от Министерство на вътрешните работи и съобщенията (МВРС) въз основа на Конституцията и Закона за далекосъобщенията, в случаите, в които тайната на съобщенията е под въпрос, телекомуникационните компании не трябва да разкриват лична информация относно поверителността на съобщенията на трети лица, освен когато са получили съгласието на физическото лице или ако могат да се позоват на една от „основателните причини“ за неспазване на Наказателния кодекс. Последните са свързани с „действията, които могат да бъдат оправдани“ (член 35 от Наказателния кодекс), и „самозащитата“ (член 36 от Наказателния кодекс) и „избягването на настояща опасност“ (член 37 от Наказателния кодекс). Съгласно Наказателния кодекс „действията, които могат да бъдат оправдани“ са единствено действията на телекомуникационната компания за съобразяване с принудителните мерки на държавата, което изключва доброволните разследвания. Следователно ако разследващите органи поискат лична информация чрез „въпросник“ (член 197, параграф 2 от Наказателно-процесуалния кодекс), на телекомуникационната компания е забранено да разкрие тези данни.

На второ място, стопанските субекти са длъжни да откажат искания за доброволно сътрудничество, когато законът им забранява да разкриват лична информация. Така например това включва случаи, в които субектът е длъжен да съблюдава поверителността на информацията, например в съответствие с член 134 от Наказателния кодекс ([15]).

3) Ограничения въз основа на ЗЗЛИСАО

Що се отнася до събирането и по-нататъшното третиране на лична информация от административни органи, в ЗЗЛИСАО се предвиждат ограниченията, обяснени по-горе в раздел II.А.1, буква б), точка 2. Еквивалентни ограничения произтичат от наредбите на префектурите, които важат за тяхната полиция.

Б) Надзор

1) Съдебен надзор

За събирането на лични данни чрез принудителни средства трябва да има съдебна заповед ([16]) и следователно то подлежи на предварително разглеждане от съдия. В случай че разследването е било незаконно, съдията може да изключи така събраните доказателства от последващия наказателен съдебен процес. Дадено лице може да поиска подобно изключване от наказателния съдебен процес, като заяви, че разследването е било незаконно.

([12]) Сериозността на престъплението и спешността са фактори, които се използват за преценяване на „целесъобразността на методите“.
([13]) Член 21, параграф 2 от Конституцията гласи: „Не се налага цензура и не се нарушава поверителността на средствата за комуникация.“
([14]) Член 4 от Закона за далекосъобщенията гласи: „(1) Поверителността на комуникациите, третирани от телекомуникационна компания, не се нарушава. (2) Никое лице, наето в телекомуникационна компания, не разкрива тайни, получени по време на изпълнение на служебни задължения, по отношение на комуникациите, третирани от телекомуникационна компания. Същото важи дори след като лицето е напуснало поста си.“
([15]) Член 134 от Наказателния кодекс гласи: „(1) Когато лекар, фармацевт, фармацевтичен дистрибутор, акушер, адвокат, правен защитник, нотариус или друго лице, официално упражняващо подобна професия, разкрива, без основателни причини, поверителна информация за друго лице, която е станала известна при упражняването на съответната професия, те се наказват с лишаване от свобода, съчетано с работа за не повече от 6 месеца или с глоба от не повече от 100 000 йени. (2) Същото важи в случаи, в които лице, което упражнява или е упражнявало религиозна дейност, разкрива, без основателни причини, поверителна информация за друго лице, която е станала известна при упражняването на тези религиозни дейности.“
([16]) За изключението от това правило, вж. бележка под линия 5.

2) Надзор въз основа на ЗЗЛИСАО

В Япония министърът или ръководителят на всяко министерство или агенция има правомощия за надзор и правоприлагане въз основа на ЗЗЛИСАО, а министърът на вътрешните работи и комуникациите може да разследва прилагането на ЗЗЛИСАО от всички други министерства.

Ако министърът на вътрешните работи и съобщенията — например въз основа на разследването на статуса на изпълнение на ЗЗЛИСАО ([17]), на обработването на жалби или на запитванията, отправени до един от неговите всестранни информационни центрове — намери това необходимо за постигане на целта на ЗЗЛИСАО, той може да поиска от ръководителя на административен орган да представи материали и обяснения относно третирането на лични данни от съответния административен орган по силата на член 50 от ЗЗЛИСАО. Министърът може да отправя становища до ръководителя на административен орган във връзка с обработката на лична информация от този орган, когато смята това за необходимо за постигане на целите на този Закон. Освен това министърът може например да поиска преразглеждане на мерките чрез действия, които може да предприеме по силата на членове 50 и 51 от Закона, когато има подозрения, че е налице нарушение или неподходящо прилагане на Закона. Това помага да се гарантира еднаквото прилагане и спазването на ЗЗЛИСАО.

3) Надзор от страна на Комисиите по въпросите на обществения ред по отношение на полицията

Що се отнася до полицейската администрация, НСП подлежи на надзор от страна на Националната комисия по въпросите на обществения ред, а полицията на префектурите подлежи на надзор от една от регионалните Комисии по въпросите на обществения ред, установени във всяка префектура. Всеки един от тези органи за надзор осигурява демократичното управление и политическата неутралност на полицейската администрация.

Националната комисия по въпросите на обществения ред отговаря за въпросите, които попадат в сферата на нейната компетентност по силата на Закона за полицията и други закони. Това включва назначаването на генералния комисар на НСП и местните висши полицейски служители, както и създаването на всеобхватни политики, в които се определят основни насоки или мерки по отношение на управлението на НСП.

Комисиите по въпросите на обществения ред на префектурите са съставени от членове, представляващи хората в съответната префектура, въз основа на Закона за полицията, и управляват полицията на префектурите като независима система от съвети. Членовете се назначават от управителя на префектурата със съгласието на префектурния съвет съгласно член 39 от Закона за полицията. Техният мандат е тригодишен и те могат да бъдат уволнени против волята си само по определени причини, изброени в закона (като например невъзможност да изпълняват задълженията си, нарушение на служебните задължения, неправомерно поведение и т.н.), като по този начин се гарантира тяхната независимост (вж. членове 40 и 41 от Закона за полицията). Освен това, за да се гарантира тяхната политическа неутралност, в член 42 от Закона за полицията на членовете на Комисията се забранява да служат едновременно като членове на законодателен орган, изпълнителен орган или друг политически орган, както и да участват активно в политически движения. Всяка Комисия попада под юрисдикцията на съответния управител на префектура, но това не дава правомощия на управителя да издава инструкции, свързани с изпълнението на нейните функции.

Съгласно член 38, параграф 3 във връзка с член 2 и член 36, параграф 2 от Закона за полицията Комисиите по въпросите на обществения ред към префектурите отговарят за „защитата на правата и свободите на физическите лица“. За тази цел те получават доклади от началниците на полицията на префектурите във връзка с дейностите в рамките на тяхната юрисдикция, включително в рамките на редовни заседания, провеждани три или четири пъти месечно. Комисиите предоставят насоки по тези въпроси чрез изготвянето на всеобхватни политики.

Освен това, като част от тяхната надзорна функция, Комисиите могат да издават инструкции към полицията на префектурите в конкретни случаи, в които те смятат това за необходимо в контекста на дадена инспекция на дейностите на полицията или на нарушения от страна на нейните служители. Също така Комисиите могат, когато сметнат за необходимо, да определят някой от своите членове, за да направи преглед на изпълнението на издадените инструкции (член 43-2 от Закона за полицията).

([17]) За да се гарантира прозрачност и да се улесни надзорът от страна на МВРС, от ръководителя на административния орган се изисква, в съответствие с член 11 от ЗЗЛИСАО, да записва всеки елемент, посочен в член 10, параграф 1 от ЗЗЛИСАО, като например името на административния орган, който съхранява досието, целта на използване на досието, метода на събиране на личната информация и т.н. (т.нар. Регистър на досиетата с лична информация). Въпреки това досиетата с лична информация, които попадат в обхвата на член 10, параграф 2 от ЗЗЛИСАО, като например тези, които са изготвени или получени в рамките на наказателно разследване или по въпроси, свързани с националната сигурност, са освободени от задължението да уведомяват МВРС и да ги включват в публичния регистър. Независимо от това съгласно член 7 от Закона за управление на публичните регистри и архивите, ръководителят на административен орган е длъжен винаги да записва класификацията, заглавието, срока и мястото на съхранение и т.н. на административни документи („Регистър за управление на досиетата с административни документи“). Индексираната информация за двата регистъра се публикува в интернет и позволява на физическите лица да проверяват какъв вид лични данни се съдържат в досието и кой административен орган съхранява данните.

4) Надзор от страна на Парламента (Диета)

Парламентът може да провежда разследвания във връзка с дейностите на публични органи и за тази цел да изисква представяне на документи и даване на показания от свидетели (член 62 от Конституцията). В този контекст компетентната комисия в Парламента може да проучи целесъобразността на дейностите по събиране на информация, извършвани от полицията.

Тези правомощия за провеждане на разследвания са доуточнени в Закона за Парламента. По силата на член 104 от него, Парламентът може да изисква от правителството и публичните агенции да предоставят доклади и записана информация, необходими за целите на негово разследване. Освен това членовете на Парламента могат да отправят писмени запитвания съгласно член 74 от Закона за Парламента. Тези запитвания трябва да бъдат одобрени от председателя на камарата. По принцип Министерският съвет трябва да им отговори писмено в срок от седем дни (когато е невъзможно да се отговори в рамките на този срок, трябва да се посочи основанието и да се определи нов срок — член 75 от Закона за Парламента). В миналото писмените запитвания от членове на Парламента са обхващали и третирането на лична информация от администрацията ([18]).

B) Индивидуални правни средства за защита

Съгласно член 32 от Конституцията на Япония на никого не може да бъде отказвано правото на достъп до съд. Освен това член 17 от Конституцията гарантира правото на всяко лице да съди държавата или публичен орган за обезщетение (както е предвидено в закона) за вреди, претърпени от него вследствие на незаконосъобразно действие на публично длъжностно лице.

1) Защита по съдебен ред срещу принудително събиране на информация въз основа на заповед (член 430 от Наказателно-процесуалния кодекс)

Съгласно член 430, параграф 2 от Наказателно-процесуалния кодекс лице, което не е удовлетворено от мерките, предприети от полицейски служител във връзка с изземване на вещи (включително ако те съдържат лична информация) въз основа на заповед, може да подаде искане (т.нар. квазижалба) до компетентния съд за отмяна или изменение на тези мерки.

Такова искане може да бъде подадено, без да се налага лицето да изчаква делото да приключи. Ако съдът намери, че изземването не е било необходимо, или че има други основания то да бъде сметнато за незаконно, той може да нареди отмяната или изменението на тези мерки.

2) Защита по съдебен ред съгласно Гражданския процесуален кодекс и Закона за обезщетенията

Ако смятат, че тяхното право на неприкосновеност на личния живот съгласно член 13 от Конституцията е било нарушено, лицата могат да предявят граждански иск, с който да поискат изтриването на лична информация, събрана в рамките на наказателно разследване.

Освен това физическо лице може да подаде иск за компенсиране на вреди въз основа на Закона за обезщетенията и съответните членове на Гражданския процесуален кодекс, ако смята, че неговото право на неприкосновеност на личния живот е било нарушено и са му нанесени вреди в резултат от събиране на негова лична информация или наблюдение ([19]). Трябва да се има предвид, че „вредата“, за която може да бъде поискана компенсация, не се ограничава до имуществена вреда (член 710 от Гражданския процесуален кодекс), така че терминът обхваща и „психично страдание“. Размерът на компенсацията за това психично страдание се определя от съдията въз основа на „свободна преценка, като се вземат предвид различни фактори във всеки отделен случай“ ([20]).

Съгласно член 1, параграф 1 от Закона за обезщетенията се дава право на компенсация, когато i) държавен служител, който упражнява публична власт от името на държавата или на публично ведомство и ii) изпълнява служебните си задължения, е причинил iii) умишлено или по непредпазливост iv) незаконно v) вреди на друго лице.

Лицето трябва да подаде иск в съответствие с Гражданския процесуален кодекс. Съгласно приложимите правила то може да направи това в съда, който има юрисдикция над мястото, където е извършен деликтът.

([18]) Вж. например писменото запитване от Камарата на съветниците № 92 от 27 март 2009 г. относно обработката на информация, събрана в рамките на наказателни разследвания, включително нарушаване на задълженията за поверителност от страна на полицията и органите за съдебно преследване.

([19]) Пример за подобен иск е Делото за списъка на Агенцията по отбрана (Районен съд на Ниигата, решение от 11 май, 2006 г. (2002(Wa) No.514). В този случай служител на Агенцията по отбрана изготвил, съхранявал и разпространил списък на лицата, които са подали в агенцията искане за разкриване на административни документи. В списъка била включена лична информация за ищеца. Като изтъква, че е налице нарушаване на неговото право на неприкосновеност на личния живот, на правото му да бъде информиран и т.н., ищецът иска ответникът да заплати компенсация за нанесени вреди съгласно член 1, параграф 1 от Закона за обезщетенията. Искането е частично удовлетворено от съда, който присъжда на ищеца частична компенсация.

([20]) Върховен съд, решение от 5 април, 1910 г. (1910(O) No.71).

3) Индивидуални правни средства за защита срещу незаконни/недобросъвестни разследвания от страна на полицията: жалба пред комисията по въпросите на обществения ред към префектурата (член 79 от Закона за полицията)

Съгласно член 79 от Закона за полицията ([21]), както е пояснен допълнително в инструкция от ръководителя на НСП за полицията на префектурите и комисиите по въпросите на обществения ред към префектурите ([22]), физически лица могат да подават писмени жалби ([23]) пред компетентната комисия по въпросите на обществения ред на съответната префектура срещу всяко незаконно или недобросъвестно поведение на полицейски служител, който изпълнява служебните си задължения; като това включва задължения по отношение на събирането и използването на лична информация. Комисията разглежда тези жалби „почтено“ в съответствие със законодателството и разпоредбите, установени на местно равнище, и уведомява в писмен вид жалбоподателя за резултата.

Въз основа на правомощията си да упражнява надзор съгласно член 38, параграф 3 от Закона за полицията, Комисията по въпросите на обществения ред към съответната префектура дава указание на полицията на префектурата да извършва разследване за установяване на фактите, да предприема мерките, които са необходими с оглед на установеното при разследването, и да ѝ докладва за резултатите. Когато сметне за необходимо, Комисията може да дава указания и относно обработването на жалбата, например ако счита, че извършеното от полицията разследване не е достатъчно. Това изпълнение е описано в известието на НСП до ръководителите на полицията на префектурите.

Уведомлението до жалбоподателя за резултатите от разследването се прави и в светлината на полицейските доклади относно разследването и мерките, взети по искане на Комисията.

4) Индивидуални правни средства за защита съгласно ЗЗЛИСАО и Наказателно-процесуалния кодекс

а) Закон за защита на личната информация, съхранявана от административни органи (ЗЗЛИСАО)

Съгласно член 48 от ЗЗЛИСАО административните органи трябва да полагат усилия за правилното и експедитивното обработване на жалби във връзка с третиране на лична информация. Като средство за предоставяне на консолидирана информация на физически лица (например относно налични права за разкриване, поправяне и спиране на използването съгласно ЗЗЛИСАО) и като звено за контакти във връзка със запитвания, МВРС създаде всестранни информационни центрове за разкриване на информация / защита на личната информация във всяка префектура въз основа на член 47, параграф 2 от ЗЗЛИСАО. Чуждестранни лица също могат да отправят запитвания. Например през 2017 финансова година (от април 2017 г. до март 2018 г.) общият брой на случаите, в които всестранните информационни центрове са отговорили на запитвания, е 5186.

Членове 12 и 27 от ЗЗЛИСАО предоставят на физическите лица правото да поискат разкриване и поправяне на задържани лични данни. Освен това съгласно член 36 от ЗЗЛИСАО физическите лица могат да поискат спирането на използването или изтриването на тяхната запазена лична информация, когато административният орган не е получил по законен път запазената лична информация или задържа или използва тази информация в нарушение на закона.

Що се отнася обаче до лична информация, която е събрана (независимо дали въз основа на заповед или чрез въпросник) и запазена за целите на наказателни разследвания ([24]), тази информация по принцип попада в категорията „лична информация, съдържаща се в документи, свързани със съдебни производства и иззети вещи“. Затова тази лична информация се изключва от приложното поле на индивидуалните права в Глава 4 от ЗЗЛИСАО съгласно член 53-2 от Наказателно-процесуалния кодекс ([25]). Вместо това по отношение на обработката на такава лична информация и правата на лицата на достъп и поправяне се прилагат специални правила съгласно Наказателно-процесуалния кодекс и Закона за досиетата по

([21]) Член 79 от Закона за полицията (откъс):
1. Всеки, който има оплакване срещу изпълнението на служебните задължения от служител на полицията на някоя префектура, може да подаде писмена жалба до Комисията по въпросите на обществения ред на съответната префектура чрез процедурата, определена в наредбата за Националната комисия по въпросите на обществения ред.
2. Комисията по въпросите на обществения ред към съответната префектура, която е получила жалба, за каквато става дума в предходния параграф, разглежда тази жалба „почтено“ в съответствие със законодателството и наредбите на местно равнище и уведомява в писмен вид жалбоподателя за резултата, освен в следните случаи:
   1) На жалбоподателя е предявено обвинение за възпрепятстване на законното изпълнение на задълженията на полицията на префектурата;
   2) Настоящото местопребиваване на жалбоподателя е неизвестно;
   3) Срещу жалбоподателя и други жалбоподатели вече е предявено съвместно обвинение и другите жалбоподатели вече са уведомени за резултата от съвместната жалба.

([22]) НСП, Известие за правилното обработване на жалбите, свързани с изпълнението на служебните задължения от полицейските служители, 13 април, 2001 г., с приложение 1 „Стандарти относно тълкуването/прилагането на член 79 от Закона за полицията“.

([23]) Съгласно известието на НСП (вж. предишната бележка под линия), на лицата, които срещат трудности при формулирането на писмена жалба, трябва да бъде оказана помощ. Това изрично включва чужденците.

([24]) От друга страна, има документи, които не са класифицирани като документи, свързани със съдебни процеси, тъй като сами по себе си те не представляват информация, получена чрез заповед или писмени запитвания по свързани с разследване въпроси, а са създадени въз основа на такива документи. В такъв случай член 45, параграф 1 от ЗЗЛИСАО не се отнася до дадена лична информация, затова тази информация не се изключва от приложното поле на глава 4 от ЗЗЛИСАО.

([25]) Член 53-2, параграф 2 от Наказателно-процесуалния кодекс предвижда, че разпоредбите на глава IV от ЗЗЛИСАО не се прилагат по отношение на лична информация, съдържаща се в документи, свързани със съдебни производства и иззети вещи.

приключени наказателни дела (вж. по-долу) ([26]). Това изключване е оправдано от различни фактори, като защитата на неприкосновеността на личния живот на засегнатите лица, поверителността на разследванията и правилното провеждане на съдебния процес. Като се има предвид това, разпоредбите на глава 2 от ЗЗЛИСАО относно принципите на третиране на такава информация остават приложими.

б) Наказателно-процесуален кодекс

Съгласно Наказателно-процесуалния кодекс възможностите за достъп до лична информация, събрана за целите на наказателно разследване, зависят както от етапа на процедурата, така и от ролята на лицето в разследването (заподозрян, обвиняем, жертва и пр.).

Като изключение от правилото в член 47 от Наказателно-процесуалния кодекс, че документите, свързани със съдебния процес, няма да бъдат публично оповестявани преди започването на процеса (тъй като това може да накърни честта и / или правото на неприкосновеност на личния живот на засегнатите лица и да възпрепятства разследването/процеса), на жертвата на престъпление по принцип се позволява да разгледа тази информация до степен, считана за разумна, като се вземе предвид целта на разпоредбата на член 47 от Наказателно-процесуалния кодекс ([27]).

Що се отнася до заподозрените, те по правило научават, че са обект на наказателно разследване по време на разпит от съдебната полиция или прокурор. Ако впоследствие прокурорът реши да не образува производство, той незабавно уведомява заподозрения за това при поискване от негова страна (член 259 от Наказателно-процесуалния кодекс).

В допълнение към това, след образуването на производство прокурорът дава на обвиняемия и / или неговия правен съветник възможност да разгледат доказателствата предварително, преди да изиска тяхното разглеждане от съда (член 299 от Наказателно-процесуалния кодекс). Това дава възможност на обвиняемия да провери своята лична информация, събрана в рамките на наказателно разследване.

И накрая, защитата на личната информация, събрана в контекста на наказателно разследване, независимо дали се отнася до заподозрян, обвиняем или друго лице (например жертва на престъпление), се гарантира чрез задължението за поверителност (член 100 от Закона за националната публична служба), а заплахата от санкция в случай на изтичане на поверителна информация гарантира тази защита при изпълнение на задължения в рамките на публичната служба (член 109 xii) от Закона за националната публична служба).

5) Индивидуални правни средства за защита срещу незаконни/недобросъвестни разследвания от страна на публични органи: жалби до КЗЛИ

Съгласно член 6 от ЗЗЛИ правителството предприема необходимите действия в сътрудничество с правителствата на трети държави за изграждане на съответстваща на международните норми система относно личната информация чрез насърчаване на сътрудничеството с международни организации и други международни рамки. Въз основа на тази разпоредба основната политика относно защитата на лична информация (приета с решение на Министерския съвет) делегира на независимия орган за защита на данните на Япония (КЗЛИ) като орган, компетентен за цялостното администриране на ЗЗЛИ, правомощието да предприема необходимите действия за преодоляване на различията по отношение на системите и операциите между Япония и съответната чужда държава с оглед на гарантиране на правилното третиране на лична информация, получена от тази държава.

Освен това, както е предвидено в член 61, подточки i) и ii) от ЗЗЛИ, на КЗЛИ е поверена задачата да формулира и популяризира основна политика, както и да служи като медиатор по отношение на жалбите, подадени срещу стопански субекти. И накрая, административните органи поддържат тясна комуникация и сътрудничество помежду си (член 80 от ЗЗЛИ).

Въз основа на тези разпоредби КЗЛИ разглежда жалбите, подадени от физически лица, както следва:

а) Физическо лице, което подозира, че негови данни, предадени от Европейския съюз, са били събрани или използвани от публични органи в Япония, включително органи, отговарящи за дейностите, за които става дума в Глава II и Глава III от настоящото „Представителство“, в нарушение на приложимите правила, включително такива, до които се отнася това „Представителство“, може да подаде жалба пред КЗЛИ (лично или чрез органа по защита на данните).

б) КЗЛИ разглежда жалбата, включително като използва правомощията си съгласно членове 6, 61, точка ii) и 80 от ЗЗЛИ, и информира компетентните публични органи, включително съответните надзорни органи, за жалбата.

([26]) Съгласно Наказателно-процесуалния кодекс и Закона за досиетата по приключени наказателни дела достъпът до и поправката на иззети вещи, както и документи / лична информация относно съдебни производства, са обект на уникална и специфична система от правила, която има за цел защитата на правото на неприкосновеност на личния живот на засегнатите лица, поверителността на разследванията, правилното провеждане на съдебния процес и т. н.

([27]) По-конкретно, разглеждането на информацията, отнасяща се до обективни доказателства, по принцип е позволено на жертвите на престъпления, що се отнася до дела, по които не се налага наказателно преследване, и за които важи участието на жертвата, посочено в член 316-33 от Наказателно-процесуалния кодекс, за да бъде защитата на жертвите на престъпления по-удовлетворителна.

Тези органи са длъжни да си сътрудничат с КЗЛИ съгласно член 80 от ЗЗЛИ, включително като предоставят необходимата информация и съответни материали, така че КЗЛИ да може да прецени дали събирането или последващото използване на личната информация е било извършено в съответствие с приложимите правила. При извършването на тази преценка КЗЛИ си сътрудничи с МВРС.

в) Ако преценката покаже, че е било допуснато нарушение на приложимите правила, сътрудничеството между съответните публични органи и КЗЛИ включва задължение за отстраняване на нарушението.

В случай на незаконно събиране на лична информация в рамките на приложимите правила, това включва изтриване на събраната лична информация.

В случай на нарушение на приложимите правила КЗЛИ потвърждава, преди да приключи работата по преценката, че са взети мерки за цялостно отстраняване на нарушението.

г) След приключване на работата по преценката КЗЛИ уведомява в разумен срок физическото лице за резултата от нея, включително за всички предприети коригиращи действия, доколкото това е приложимо. Чрез това уведомление КЗЛИ информира физическото лице и за възможността да поиска от компетентния публичен орган потвърждение на резултата, както и за органа, до който следва да бъде отправено подобно искане.

Достъпът до подробна информация за заключенията от преценката може да бъде ограничен, доколкото има основателни причини да се смята, че предоставянето на такава информация би могло да изложи на риск текущо разследване.

Когато жалбата се отнася до събирането или използването на лични данни в областта на наказателното правоприлагане, КЗЛИ — в случай, че преценката покаже, че е било образувано дело, в рамките на което става дума за лична информация на лицето, и това дело е приключило — информира лицето за възможността да се запознае с протокола от делото по реда на член 53 от Наказателно-процесуалния кодекс и член 4 от Закона за досиетата по приключени наказателни дела.

Когато вследствие на преценката се установи, че дадено физическо лице е заподозряно в извършването на престъпление, КЗЛИ уведомява лицето за това, както и за възможността да подаде заявление съгласно член 259 от Наказателно-процесуалния кодекс.

д) Ако дадено физическо лице въпреки това не е удовлетворено от резултата от процедурата, може да се обърне към КЗЛИ, която информира лицето за различните възможности и за подробните процедури за получаване на защита съгласно законовите и подзаконовите актове на Япония. Наред с това КЗЛИ предоставя на лицето подкрепа, включително съвети и помощ при сезиране на съответния административен или съдебен орган с евентуално искане.

III. **Достъп на държавните органи за целите на националната сигурност**

A. Правни основания и ограничения за събирането на лична информация

1) Правни основания за събиране на информация от съответното министерство/агенция

Както е посочено по-горе, събирането на лична информация за целите на националната сигурност от административни органи трябва да бъде в обхвата на тяхната административна юрисдикция.

В Япония не съществува съдебна практика, която позволява събирането на информация чрез задължителни средства само за целите на националната сигурност. Съгласно член 35 от Конституцията е възможно да се събира лична информация принудително само въз основа на заповед, издадена от съд за разследване на престъпление. Такава заповед може да бъде издадена само за целите на наказателно разследване. Това означава, че японската правна система не разрешава събиране на/достъп до информация чрез задължителни средства по съображения, свързани с националната сигурност. Вместо това в областта на националната сигурност заинтересованите министерства или агенции могат да получат информация от източници със свободен достъп или от стопански субекти или физически лица чрез доброволно разкриване. Стопанските субекти, които получават искания за доброволно сътрудничество, нямат правно задължение да предоставят такава информация и следователно не са изправени пред отрицателни последствия, ако откажат да сътрудничат.

Редица министерства и агенции имат отговорности в областта на националната сигурност.

1) Секретариат на правителството

Секретариатът на правителството извършва събиране и търсене на информация във връзка с важни политики на правителството ([28]), описани в член 12-2 от Закона за правителството ([29]). Въпреки това секретариатът на правителството няма правомощия за събиране на лична информация пряко от стопанските субекти. Той събира, обединява, анализира и оценява информацията от материали със свободен достъп, други публични органи и т.н.

2) НСП/Полиция на префектурите

Във всяка префектура полицията е оправомощена да събира информация в рамките на обхвата на своята компетентност съгласно член 2 от Закона за полицията. Възможно е Националната служба „Полиция“ да събира директно информация в рамките на обхвата на своята компетентност по силата на закона за полицията. Това се отнася по-специално за дейностите на Бюрото за сигурност на НСП и Министерството на външните работи и разузнаването. Съгласно член 24 от Закона за полицията Бюрото за сигурност отговаря за въпроси, свързани с полицията ([30]), а Министерството на външните работи и разузнаването отговаря за въпроси, свързани с чужди граждани, както и с японски граждани, чиито дейности са базирани в чужди държави.

3) Агенция „Разузнаване във връзка с обществената сигурност“ (АРОС).

Прилагането на Закона за предотвратяването на подривните дейности (ЗППД) и Закона за контролиране на организациите, извършили актове на безразборно масово убийство (ЗКО) е задача основно на Агенцията „Разузнаване във връзка с обществената сигурност“ (АРОС). Това е агенция на Министерство на правосъдието.

В ЗППД и ЗКО се посочва, че административни разпоредби (т.е. мерки за ограничаване на дейностите на тези организации, тяхното прекратяване и т.н.) могат да бъдат предприети, при спазване на строги условия, срещу организации, извършили определени сериозни терористични актове („терористични подривни дейности“ и „актове на безразборно масово убийство“) в нарушение на „обществената сигурност“ или „основната система на обществото“, по силата на Конституцията. „Терористичните подривни дейности“ попадат в обхвата на ЗППД (вж. член 4, който обхваща дейности като бунт, подбуждане на чужда агресия, убийство с политически намерения и т.н.), а ЗКО работи по „актове на безразборно масово убийство“ (вж. член 4 от ЗКО). Само точно определени организации, представляващи специфична вътрешна или външна заплаха за обществената сигурност, могат да бъдат предмет на разпореждания по ЗППД или ЗКО.

За тази цел ЗППД и ЗКО предоставят юридически правомощия за разследване. Основните правомощия за разследване на служителите на АРОС са посочени в член 27 от ЗППД и член 29 от ЗКО. Разследванията, провеждани от АРОС съгласно тези разпоредби, се извършват до необходимата степен съгласно горепосочените разпореждания за контрол на организации (напр. радикални лявоориентирани групи, сектата „*Aum Shinrikyo*“ и някои местни групи, тясно свързани със Северна Корея, са сочени като примери за обекти на разследване в миналото). Въпреки това тези проучвания не могат да разчитат на задължителни средства и затова организация, която притежава лична информация, не може да бъде принудена да предостави тази информация.

Събирането и използването на информацията, разкрита на АРОС на доброволна основа, подлежи на съответните гаранции и ограничения, предвидени от закона, като например, *наред с другото*, тайната на съобщенията, гарантирана от Конституцията, и правилата относно третирането на лична информация съгласно ЗЗЛИСАО.

4) Министерство на отбраната (МО)

Що се отнася до събирането на информация от Министерството на отбраната (МО), то събира информация въз основа на член 3 и 4 от Закона за създаване на Министерството на отбраната до степента, необходима за упражняване на дейностите в неговата административна юрисдикция, включително по отношение на отбраната и охраната, действия, които трябва да бъдат предприети от силите за самоотбрана, както и във връзка с разгръщането на сухопътни, морски и въздушни сили за самоотбрана. Министерство на отбраната може да събира информация за тези цели само чрез доброволно сътрудничество и от свободно достъпни източници. То не събира информация за широката общественост.

2) Ограничения и гаранции

а) Законови ограничения

1) Общи ограничения, основани на ЗЗЛИСАО

ЗЗЛИСАО представлява общ закон, приложим по отношение на събирането и обработването на лични данни от административни органи във всички области на дейност на тези органи. Поради това ограниченията и гаранциите, описани в раздел II, буква б) (2), се прилагат също и за запазването, съхраняването, използването и т.н. на лична информация в областта на националната сигурност.

([28]) Това се извършва от Службата за разузнаване на правителството съгласно член 4 от Заповедта за организация на секретариата на правителството.

([29]) Това включва „събирането и търсенето на разузнавателна информация относно важни политики на правителството“.

([30]) Полицията отговаря за дейностите по контрол на престъпленията, свързани с обществената безопасност и интересите на нацията. Това включва контрол на престъпленията и събиране на информация за незаконни деяния, свързани с екстремистки лявоориентирани групи, дясноориентирани групи и дейности, насочени против Япония.

2) Специални ограничения, приложими за полицията (НСП и полицията на префектурите)

Както е посочено по-горе в раздела относно събирането на информация за целите на правоприлагането, полицията може да събира информация само в рамките на своята компетентност и при това може, съгласно член 2, параграф 2 от Закона за полицията, да действа единствено до степен, „строго ограничена“ до изпълнението на нейните задължения, и по начин, който е „безпристрастен, непредубеден, без предразсъдъци и справедлив“. Освен това „с нейните правомощия никога не може да се злоупотребява по какъвто и да е начин, засягащ правата и свободите на лицата, гарантирани в Конституцията на Япония“.

3) Специални ограничения, приложими за АРОС

Както в член 3от ЗППД, така и в член 3 от ЗКО е постановено, че разследванията, провеждани съгласно тези актове се извършват само в минималната степен, необходима за постигане на преследваната цел, и не се извършват по начин, който неоснователно ограничава основните права на човека. Освен това съгласно член 45 от ЗППД и член 42 от ЗКО, ако служител на АРОС злоупотреби със своите правомощия, това представлява престъпление, което се наказва с по-тежки наказателни санкции от тези за „общи“ злоупотреби с правомощия в други области на публичния сектор.

4) Специални ограничения, приложими за МО

Що се отнася до събирането/организирането на информация от Министерството на отбраната, както е посочено в член 4 от Закона за създаване на Министерство на отбраната, дейността на това Министерство за събиране на информация се ограничава до „необходимото“ за изпълнение на неговите задължения във връзка със 1) защитата и охраната, 2) действията, които трябва да бъдат предприети от силите за самоотбрана, 3) организацията, броя на личния състав, структурата, оборудването и разполагането на сухопътни, морски и въздушни сили за самоотбрана.

б) Други ограничения

Както беше обяснено по-горе в раздел II.А.2) б) (1) относно наказателните разследвания, „от съдебната практика на Върховния съд следва, че за да се отправи искане за доброволно съдействие до стопански субект, това искане трябва да е необходимо за разследването на предполагаемото престъпление и да е разумно с оглед на постигането на целта на разследването.

Въпреки че разследванията, провеждани от разследващите органи в областта на националната сигурност, се различават както по правното си основание, така и по своята цел от разследванията, провеждани от разследващите органи в областта на правоприлагането, основните принципи за „необходимост от разследване“ и „целесъобразност на метода“ се прилагат по аналогия в областта на националната сигурност и следва да бъдат спазвани, като надлежно се вземат под внимание специфичните за всеки отделен случай обстоятелства.

Комбинирането на горепосочените ограничения гарантира, че събирането и обработката на информация се осъществяват само доколкото са необходими за изпълнението на конкретни задължения на компетентния публичен орган, и то при наличие на конкретни заплахи. Това изключва масовото и безразборно събиране или достъп до лична информация по съображения, свързани с националната сигурност.

Б. Надзор

1) Надзор, основан на ЗЗЛИСАО

Както беше обяснено по-горе в раздел II.Б.2), в публичния сектор на Япония министърът или ръководителят на всяко министерство или агенция разполага с правомощия да контролира и налага спазването на ЗЗЛИСАО в своето министерство или агенция. Освен това министърът на вътрешните работи и комуникациите може да проучи състоянието на прилагането на закона, да изисква от всеки министър да предаде материали и обяснения въз основа на членове 49 и 50 от Закона, както и да представи на всеки министър становища въз основа на член 51 от Закона. Например, той може да отправи искане за преразглеждане на мерките чрез действия по силата на членове 50 и 51 от Закона.

2) Надзор върху полицията от страна на Комисиите по въпросите на обществения ред

Както е обяснено по-горе в раздел „II. Събиране на информация за целите на наказателното правоприлагане“, независимите комисии по въпросите на обществения ред осъществяват надзор върху дейностите на полицията на префектурите.

По отношение на Национална служба „Полиция“ (НСП) надзорните функции се упражняват от Националната комисия по въпросите на обществения ред. Съгласно член 5 от Закона за полицията тази комисия отговаря, по-специално, за „защитата на правата и свободите на физическите лица“. За тази цел тя следва по-специално да установи всеобхватни политики, определящи разпоредби за управлението на дела, предвидени във всяка позиция на член 5, параграф 4 от Закона за полицията, и определящи основни насоки или мерки, които следва да бъдат използвани за извършване на посочените дейности. Националната комисия по въпросите на обществения ред (НКВОР) има същата степен на независимост като комисиите по въпросите на обществения ред към префектурите (КВОРП).

3) Надзор на Министерството на отбраната от Службата на главния инспектор за спазване на законодателството

Службата на главния инспектор за спазване на законодателството (СГИ), която се ръководи от главния инспектор, е независима служба в Министерството на отбраната (МО), което е под прекия надзор на министъра на отбраната съгласно член 29 от Закона за създаване на Министерство на отбраната. СГИ може да извършва проверки на съответствието на действията на длъжностни лица от МО със законовите и подзаконовите разпоредби. Тези инспекции се наричат „проверки в областта на отбраната“.

СГИ провежда инспекции като независима служба, за да гарантира спазването на законодателството в цялото министерство, включително силите за самоотбрана. Службата изпълнява своите задължения независимо от оперативните отдели на Министерството на отбраната. След инспекция СГИ изготвя доклад с констатациите си, заедно с необходимите мерки за подобрение, и ги представя директно и незабавно на министъра на отбраната. Въз основа на доклада на СГИ министърът на отбраната може да издава заповеди за изпълнение на необходимите мерки за коригиране на положението. Заместникът на заместник-министъра отговаря за прилагането на тези мерки и докладва на министъра на отбраната за състоянието на прилагането.

Като доброволна мярка за прозрачност констатациите на проверките в областта на отбраната се публикуват на уебсайта на Министерството на отбраната (въпреки че това не се изисква от закона).

Съществуват три категории проверки в областта на отбраната:

i) редовни проверки в областта на отбраната, които се извършват периодично ([31]);

ii) проверки в областта на отбраната, които се извършват с цел да се провери дали ефективно са взети мерки за подобрение; както и

iii) специални проверки в областта на отбраната, които се извършват по конкретни въпроси, разпоредени от министъра на отбраната.

В контекста на такива проверки генералният инспектор може да поиска доклади от съответната служба, да поиска представяне на документи, да получи достъп до обекти за извършване на проверката, да поиска обяснения от заместника на заместник-министъра и т.н. Като се вземе предвид естеството на инспекционните задачи на СГИ, тази служба се оглавява от много старши правни експерти (бивш прокурор по надзора).

4) Надзор на АРОС

АРОС извършва както редовни, така и специални проверки на операциите на своите отделни служби и бюра (Служба за разузнаване във връзка с обществената сигурност, разузнавателни служби и подслужби и т.н.). За целите на редовното инспектиране като инспектор(и) се назначава(т) помощник генерален директор и/или директор. Такива проверки се отнасят и до управлението на личната информация.

5) Надзор от страна на парламента

Що се отнася до събирането на информация за целите на правоприлагането, японският парламент, чрез своята компетентна комисия, може да разгледа законосъобразността на дейностите по събиране на информация в областта на националната сигурност. Разследващите правомощия на парламента се основават на член 62 от Конституцията и членове 74 и 104 от японския Закон за Парламента.

B. Индивидуални правни средства за защита

Индивидуална правна защита може да се осъществява по същите пътища, както в сферата на наказателното правоприлагане. Това включва и нов механизъм за правна защита, управляван и контролиран от КЗЛИ, за разглеждане и разрешаване на жалби от граждани на ЕС. Във връзка с това, моля, вижте съответните пасажи от раздел II.B.

Освен това съществуват специални възможности за индивидуална защита в областта на националната сигурност.

Личната информация, събирана от административен орган за целите на националната сигурност, подлежи на разпоредбите на глава 4 от ЗЗЛИСАО. Това включва правото да се изисква оповестяване на информация (член 12), поправка (включително добавяне или заличаване) (член 27) на запазена лична информация, както и право да се поиска спиране на употребата на лична информация в случай, че административният орган е получил съответната информация

([31]) Като пример за проверка, свързана с въпросите, обхванати от настоящото Представителство, може да се посочи Редовната проверка в областта на отбраната във връзка със „Знания/Подготвеност за спазване на правните изисквания“, тъй като защитата на личната информация е един от основните акценти на проверката. По-конкретно, въпросната проверка се отнася до състоянието на управлението, съхранението и т.н. на личната информация. В своя доклад СГИ установи няколко незадоволителни аспекта в управлението на личната информация, които следва да бъдат подобрени, като например липсата на защита на информацията чрез парола. Докладът може да бъде намерен на интернет страницата на Министерството на отбраната.

по незаконосъобразен начин (член 36). При все това в областта на националната сигурност упражняването на тези права се подчинява на определени ограничения: исканията за оповестяване, коригиране или временно спиране не могат да бъдат одобрявани, когато се отнасят до „информация, за която ръководител на административен орган има основателни причини да приеме, че нейното разкриване има вероятност да навреди на националната сигурност, да причини вреди на отношенията на взаимно доверие с друга държава или международна организация или да доведе до неизгодна позиция в преговори с друга държава или международна организация“ (член 14, подточка iv)). Поради това не всяко доброволно събиране на информация, свързана с националната сигурност, попада в обхвата на това освобождаване, тъй като винаги се изисква конкретна оценка на рисковете, свързани с нейното оповестяване.

Освен това, ако искането е отхвърлено на основание на това, че се счита, че въпросната информация не може да бъде оповестявана по смисъла на член 14, подточка iv), лицето може да подаде административна жалба за преразглеждане на това решение, като например твърди, че условията, посочени в член 14, подточка iv) не са изпълнени в разглеждания случай. В този случай преди да вземе решение, началникът на съответния административен орган се консултира със съответния Апелативен съвет по въпросите на оповестяването на информация и защита на личната информация. Съветът ще разгледа жалбата от независима гледна точка. Съветът е тясно специализиран и независим орган, чиито членове се назначават от министър-председателя със съгласието на двете камари на японския парламент и се подбират сред експерти с изключителен опит ([32]). Съветът притежава силни разследващи правомощия, включително възможност да изисква документи и оповестяване на въпросната лична информация, да провежда обсъждане при закрити врата и да прилага процедура по индекса на Вон ([33]). След това Съветът изготвя писмен доклад, чието съдържание се съобщава на засегнатото лице ([34]). Констатациите, съдържащи се в този доклад, се оповестяват публично. Въпреки че формално погледнатото докладът не е правно обвързващ, съответните административни органи съблюдават почти всички доклади ([35]).

Накрая, съгласно член 3, параграф 3 от Закона за административното съдопроизводство лицето може да подаде иск до съда за отмяна на решение, взето от административен орган, да не оповестява лична информация.

IV. **Периодичен преглед**

При извършването на периодичния преглед на решението относно адекватното ниво на защита КЗЛИ и Европейската комисия ще обменят информация относно обработването на данни съгласно условията, посочени в констатацията за адекватно ниво на защита, включително изложените в настоящото изявление.

([32]) Вж. член 4 от Закона за създаване на Апелативния съвет по въпросите на оповестяването на информация и защита на личната информация.

([33]) Вж. член 9 от Закона за създаване на Апелативния съвет по въпросите на оповестяването на информация и защита на личната информация.

([34]) Вж. член 16 от Закона за създаване на Апелативния съвет по въпросите на оповестяването на информация и защита на личната информация.

([35]) През последните 3 години не е имало случай, при който съответният административен орган да приеме решение, което да се различава от заключенията на Съвета. В миналото има изключително малък брой такива случаи: само два случая от общо 2 000 случая от 2005 г. (годината, в която ЗЗЛИСАО влиза в сила). Когато административният орган издава констатация/решение, което се различава от заключенията на Съвета, съгласно член 50, параграф 1, точка 4 от Закона за административното обжалване, както се прилага със замяната на член 42, параграф 2 от ЗЗЛИСАО, той следва ясно да посочи причините за това.