Сборник съдебна практика

РЕШЕНИЕ НА СЪДА (голям състав)

16 юли 2020 година*

„Преюдициално запитване — Защита на физическите лица при обработването на лични данни — Харта на основните права на Европейския съюз — Членове 7, 8 и 47 — Регламент (ЕС) 2016/679 — Член 2, параграф 2 — Приложно поле — Предаване на лични данни на трети държави за търговски цели — Член 45 — Решение на Комисията относно адекватното ниво на защита —Член 46 — Предаване на данни с подходящи гаранции — Член 58 — Правомощия на надзорните органи — Обработване на предаваните данни от публичните органи на трета държава за цели, свързани с националната сигурност — Преценка на адекватността на нивото на защита, осигурено в третата държава — Решение 2010/87/ЕС — Стандартни клаузи за защита при предаването на лични данни на трети държави — Подходящи гаранции, предоставени от администратора — Валидност — Решение за изпълнение (ЕС) 2016/1250 — Адекватност на защитата, осигурявана от Щита за личните данни в отношенията между Европейския съюз и Съединените щати — Валидност — Жалба на физическо лице, чиито данни са предадени от Европейския съюз на Съединените щати“

По дело C-311/18

с предмет преюдициално запитване, отправено на основание член 267 ДФЕС от High Court (Висш съд, Ирландия) с акт от 4 май 2018 г., постъпил в Съда на 9 май 2018 г., в рамките на производство по дело

Data Protection Commissioner

срещу

Facebook Ireland Ltd,

Maximillian Schrems,

в присъствието на:

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Език на производството: английски.

СЪДЪТ (голям състав),

състоящ се от: K. Lenaerts, председател, R. Silva de Lapuerta, заместник-председател, Ал. Арабаджиев, A. Prechal, M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, L. S. Rossi и I. Jarukaitis, председатели на състави, M. Ilešič, T. von Danwitz (докладчик) и D. Šváby, съдии,

генерален адвокат: H. Saugmandsgaard Øe,

секретар: C. Strömholm, администратор,

предвид изложеното в писмената фаза на производството и в съдебното заседание от 9 юли 2019 г.,

като има предвид становищата, представени:

– за Data Protection Commissioner, от D. Young, solicitor, B. Murray и M. Collins, SC, и C. Donnelly, BL,

– за Facebook Ireland Ltd, от P. Gallagher и N. Hyland, SC, A. Mulligan и F. Kieran, BL, P. Nolan, C. Monaghan, C. O'Neill и R. Woulfe, solicitors,

– за г-н Schrems, от H. Hofmann, Rechtsanwalt, E. McCullough, J. Doherty и S. O'Sullivan, SC, и G. Rudden, solicitor,

– за The United States of America, от E. Barrington, SC, S. Kingston, BL, S. Barton и B. Walsh, solicitors,

– за Electronic Privacy Information Centre, от S. Lucey, solicitor, G. Gilmore и A. Butler, BL, и C. O'Dwyer, SC,

– за BSA Business Software Alliance Inc., от B. Van Vooren и K. Van Quathem, advocaten,

– за Digitaleurope, от N. Cahill, barrister, J. Cahir, solicitor, и M. Cush, SC,

– за Ирландия, от A. Joyce и M. Browne, в качеството на представители, подпомагани от D. Fennelly, BL,

– за белгийското правителство, от J.-C. Halleux и P. Cottin, в качеството на представители,

– за чешкото правителство, от M. Smolek, J. Vláčil, O. Serdula и A. Kasalická, в качеството на представители,

– за германското правителство, от J. Möller, D. Klebs и T. Henze, в качеството на представители,

– за френското правителство, от A.-L. Desjonquères, в качеството на представител,

– за нидерландското правителство, от C. S. Schillemans, K. Bulterman и M. Noort, в качеството на представители,

– за австрийското правителство, от J. Schmoll и G. Kunnert, в качеството на представители,

– за полското правителство, от B. Majczyna, в качеството на представител,

– за португалското правителство, от L. Inez Fernandes, A. Pimenta и C. Vieira Guerra, в качеството на представители,

– за правителството на Обединеното кралство, от S. Brandon и D. Guðmundsdóttir, в качеството на представители, подпомагани от J. Holmes, QC, и C. Knight, barrister,

– за Европейския парламент, от M. J. Martínez Iglesias и A. Caiola, в качеството на представители,

– за Европейската комисия, от D. Nardi, H. Krämer и H. Kranenborg, в качеството на представители,

– за Европейския комитет по защита на данните (ЕКЗД), от A. Jelinek и K. Behn, в качеството на представители,

след като изслуша заключението на генералния адвокат, представено в съдебното заседание от 19 декември 2019 г.,

постанови настоящото

Решение

1 Преюдициалното запитване по същество се отнася до:

– тълкуването на член 3, параграф 2, първо тире, членове 25 и 26 и член 28, параграф 3 от Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 1995 г., стр. 31; Специално издание на български език, 2007 г., глава 13, том 17, стр. 10) във връзка с член 4, параграф 2 ДЕС и членове 7, 8 и 47 от Хартата на основните права на Европейския съюз (наричана по-нататък „Хартата“),

– тълкуването и валидността на Решение 2010/87/ЕС на Комисията от 5 февруари 2010 година относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46 (ОВ L 39, 2010 г., стр. 5), изменено с Решение за изпълнение (ЕС) 2016/2297 на Комисията от 16 декември 2016 г. (ОВ L 344, 2016 г., стр. 100) (наричано по-нататък „решението СК“), както и до

– тълкуването и валидността на Решение за изпълнение (ЕС) 2016/1250 на Комисията от 12 юли 2016 година съгласно Директива 95/46 относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (ОВ L 207, 2016 г., стр. 1, наричано по-нататък „решението ЩЛД“).

2 Запитването е отправено в рамките на спор между Data Protection Commissioner (Комисар за защита на личните данни, Ирландия) (наричан по-нататък „комисарят“), от една страна, и Facebook Ireland Ltd и г-н Maximillian Schrems, от друга страна, по повод на подадена от последния жалба относно предаването на личните му данни от Facebook Ireland на Facebook Inc. в Съединените щати.

Правна уредба

Директива 95/46

3 Член 3 от Директива 95/46 е бил озаглавен „Приложно поле“ и параграф 2 от него е посочвал:

„Настоящата директива не се прилага за обработването на лични данни:

– при извършване на дейности, извън приложното поле на правото на Общността, например дейностите, предвидени в дял V и дял VI от Договора за Европейския съюз, и във всички случаи при дейности по обработването на данни, отнасящи се до обществената сигурност, отбраната, държавната сигурност (включително икономическото благосъстояние на държавата, когато процесът на обработка е свързан[…] с държавната сигурност) и при дейности на държавата в областта на наказателното право,

– […]“.

4 Член 25 от тази директива е гласял:

„1. Държавите членки предвиждат, че предаването на лични данни […] на трета страна[…] може да се извършва, само ако без да се засяга спазването на националните разпоредби, приети в съответствие с другите разпоредби на настоящата директива, въпросната трета страна гарантира достатъчна степен на защита.

2. Достатъчният характер на степента на защита, предоставяна от трета страна, се преценява в светлината на всички обстоятелства, свързани с операцията по предаването на данни или набор от операции по предаване на данни; […]

[…]

6. Комисията може да констатира, в съответствие с процедурата, посочена в член 31, параграф 2, че трета страна гарантира достатъчна степен на защита по смисъла на параграф 2 на настоящия член, по силата на вътрешното си законодателство или на международните споразумения, сключени от нея, и по-конкретно след приключване на преговорите, упоменати в параграф 5, за защитата на личния живот и на основните свободи и права на лицата.

Държавите членки предприемат необходимите мерки за спазване на решението на Комисията“.

5 Член 26, параграфи 2 и 4 от посочената директива е предвиждал:

„2. Без да се засягат разпоредбите на параграф 1, дадена държава членка може да разреши предаването или набора от предавания за трета страна, която не осигурява достатъчна степен на защита по смисъла на член 25, параграф 2, ако администраторът предостави достатъчни гаранции по отношение на защитата на личния живот и основните права и свободи на лицата и по отношение на упражняването на съответните права; такива гаранции могат, в частност, да произтичат от съответни договорни клаузи.

[…]

4. Ако Комисията реши, в съответствие с процедурата, предвидена в член 31, параграф 2, че някои стандартни договорни клаузи предлагат достатъчни гаранции, както изисква параграф 2, държавите членки вземат необходимите мерки, за да спазят решението на Комисията“.

6 Съгласно член 28, параграф 3 от същата директива:

„В частност, на всеки орган са предоставени:

– правомощия по разследване, като право на достъп до данните, съставляващи предмет на операциите по обработка, както и право на събиране на цялата информация, необходима за изпълнението на функциите по надзора,

– ефективни правомощия на намеса, като например право на предоставяне на становища, преди извършването на операции по обработка на данни съгласно член 20, и гарантиране на подходяща публичност на подобни становища; право на разпореждане на блокиране, изтриване или унищожаване на данни, на въвеждане на временна или окончателна забрана върху обработването, на отправяне на предупреждение или строга забележка към администратора, както и право да сезира националния парламент или други политически институции,

– правомощие да води съдебни дела, когато са нарушени националните разпоредби, приети в съответствие с настоящата директива, или [да свежда] тези нарушения до знанието на съдебните власти.

[…]“.

ОРЗД

7 Директива 95/46 е отменена и заменена с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 2016 г., стр. 1, наричан по-нататък „ОРЗД“).

8 Съображения 6, 10, 101, 103, 104, 107—109, 114, 116 и 141 от ОРЗД гласят:

„(6) Бързото технологично развитие и глобализацията създадоха нови предизвикателства пред защитата на личните данни. Значително нарасна мащабът на обмена и събирането на лични данни. Технологиите позволяват и на частните дружества, и на публичните органи да използват лични данни в безпрецедентни мащаби, за да упражняват дейността си. Физическите лица все по-често оставят лична информация, която е публично достъпна и в световен мащаб. Технологиите преобразиха както икономиката, така и социалния живот и следва да улесняват още повече свободното движение на лични данни в Съюза и предаването на данни до трети държави и международни организации, като същевременно гарантират високо ниво на защита на личните данни.

[…]

(10) За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза, нивото на защита на правата и свободите на физическите лица във връзка с обработването на такива данни следва да бъде равностойно във всички държави членки. Следва да се гарантира последователно и еднородно прилагане в рамките на Съюза на правилата за защита на основните права и свободи на физическите лица във връзка с обработването на лични данни. По отношение на обработването на лични данни, необходимо за спазване на правно задължение, за изпълнение на задача от обществен интерес или при упражняване на официалните правомощия, предоставени на администратора на лични данни, на

държавите членки следва да се позволи да запазят или да въведат национални разпоредби, които да уточняват по-нататък реда за прилагане на правилата на настоящия регламент. Наред с общите и хоризонтални актове относно защитата на данните, с които се прилага Директива 95/46/ЕО, държавите членки имат и специално секторно законодателство в области, които се нуждаят от по-специфични разпоредби. Настоящият регламент оставя и известна свобода на действие на държавите членки да конкретизират съдържащите се в него правила, включително по отношение на обработването на специални категории лични данни („чувствителни данни“). В този смисъл настоящият регламент не изключва право на държавите членки, което определя обстоятелствата за специални случаи на обработване, включително по-точно определяне на условията, при които обработването на лични данни е законосъобразно.

[…]

(101) Потоци от лични данни към и от страни извън Съюза и международни организации са необходими за разширяването на международната търговия и международното сътрудничество. Нарастването на тези потоци породи нови предизвикателства и опасения във връзка със защитата на личните данни. Когато обаче лични данни се предават от Съюза на администратори, обработващи лични данни или други получатели в трети държави или на международни организации, нивото на защита на физическите лица, гарантирано в Съюза с настоящия регламент, не следва да бъде излагано на риск, включително в случаите на последващо предаване на лични данни от третата държава или международната организация на администратори или обработващи лични данни в същата или друга трета държава или международна организация. Във всеки случай предаването на данни на трети държави и международни организации може да се извършва единствено в пълно съответствие с настоящия регламент. Предаването може да се извършва, само ако администраторът или обработващият лични данни изпълняват условията, установени в разпоредбите на настоящия регламент относно предаването на лични данни на трети държави или международни организации, при спазване на другите разпоредби на настоящия регламент.

[…]

(103) Комисията може да реши, с действие по отношение на целия Съюз, че определени трети държави или територия или конкретен сектор в трета държава, или дадена международна организация предоставя адекватно ниво на защита на данните, като по този начин осигури правна сигурност и еднообразно прилагане навсякъде в Съюза по отношение на третата държава или международна организация, за които се смята, че предоставят такова ниво на защита. В тези случаи предаването на лични данни на такава трета държава или международна организация може да се извършва, без да е необходимо допълнително разрешение. Комисията може също така да реши да отмени такова решение, след като е отправила предизвестие и е предоставила пълна обосновка на третата държава или международната организация.

(104) В съответствие с основните ценности, въз основа на които е създаден Съюзът, по-специално защитата на правата на човека, в оценката си на третата държава или на територия или на конкретен сектор в третата държава, Комисията следва да вземе предвид как се зачитат в конкретната трета държава принципите на правовата държава, достъпът до правосъдие и международните норми и стандарти за правата на човека, както и нейното общо и секторно право, включително законодателството ѝ в областта на обществената сигурност, отбраната и националната сигурност, а също и обществения ред и наказателното право. При приемането на решение относно адекватното ниво на защита за територия или конкретен сектор в трета държава, следва да се вземат предвид ясни и обективни критерии, като например специфични дейности по обработване и обхватът на

приложимите правни стандарти и на действащото законодателство в третата държава. Третата държава следва да предостави гаранции, които осигуряват адекватно ниво на защита, което по същество е равностойно на нивото, гарантирано в рамките на Съюза, по-специално когато личните данни се обработват в един или няколко конкретни сектора. Третата държава следва по-специално да осигури ефективен независим надзор в областта на защитата на данните и да предвиди механизми за сътрудничество с органи по защита на данните на държавите членки, а на субектите на данните следва да бъдат предоставени действителни и приложими права и ефективни средства за административна и съдебна защита.

[…]

(107) Комисията може да приеме, че дадена трета държава или територия или конкретен сектор в трета държава, или дадена международна организация вече не осигурява адекватно ниво на защита на данните. В резултат на това предаването на лични данни на тази трета държава или международна организация следва да бъде забранено, докато не бъдат изпълнени изискванията по настоящия регламент относно предаването на данни с подходящи гаранции, включително задължителни фирмени правила и дерогации в особени случаи. В такъв случай следва да се предвиди провеждане на консултации между Комисията и такива трети държави или международни организации. Комисията следва своевременно да уведоми третата държава или международната организация за основанията и да започне консултации с нея с цел да намери решение на този проблем.

(108) При липсата на решение относно адекватното ниво на защита администраторът или обработващият лични данни следва да предприеме мерки, за да компенсира липсата на защита на данни в дадена трета държава чрез подходящи гаранции за субекта на данните. Такива подходящи гаранции може да се състоят в използването на задължителни фирмени правила, стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от надзорен орган, или договорни клаузи, разрешени от надзорен орган. Тези гаранции следва да осигуряват спазването на изискванията относно защитата на данните и на правата на субектите на данни, подходящи при обработване в рамките на Съюза, включително наличието на приложими права на субектите на данни и на ефективни средства за правна защита, включително с цел получаване на ефективна административна или съдебна защита и предявяване на искове за обезщетение в Съюза или в трета държава. Те следва да се отнасят по-специално до спазването на общите принципи, свързани с обработването на лични данни, и до принципите за защита на данните на етапа на изготвяне и по подразбиране. […]

(109) Възможността администраторът или обработващият лични данни да използва стандартни клаузи за защита на данните, приети от Комисията или от надзорен орган, не следва да възпрепятства администраторите или обработващите лични данни да включат стандартни клаузи за защита на данните в договор с по-голям обхват, като договор между обработващия лични данни и друг обработващ лични данни, нито да добавят други клаузи или допълнителни гаранции, при условие че същите не противоречат пряко или косвено на стандартните договорни клаузи, приети от Комисията или от надзорен орган, нито засягат основните права или свободи на субектите на данни. Администраторите и обработващите лични данни следва да бъдат насърчавани да предоставят допълнителни гаранции чрез договорни ангажименти, които допълват стандартните клаузи за защита.

[…]

(114) Във всеки случай, когато Комисията не е взела решение относно адекватното ниво на защита на данните в трета държава, администраторът или обработващият данни следва да използва решения, които предоставят приложими и действителни права на субектите на данни по отношение на обработването на техните данни в Съюза след предаването на тези данни, така че те да продължат да се ползват от основните права и гаранциите.

[…]

(116) Трансграничното движение на лични данни извън Съюза може да увеличи риска физическите лица да не могат да упражнят правата на защита на данните, по-специално да се защитят срещу неправомерна употреба или разкриване на тези данни. В същото време надзорните органи могат да бъдат изправени пред невъзможността да разглеждат жалби или да провеждат разследвания, свързани с дейности, извършвани извън техните граници. Техните усилия за сътрудничество в трансграничния контекст могат да бъдат възпрепятствани и от недостатъчни правомощия за предотвратяване или защита, различаващи се правни режими, както и от практически пречки като ограничения на ресурсите. […]

[…]

(141) Всеки субект на данни следва да има право да подаде жалба до един надзорен орган, по-специално в държавата членка на обичайно[то] си местопребиваване, както и право на ефективни правни средства за защита в съответствие с член 47 от Хартата, ако счита, че правата му по настоящия регламент са нарушени или ако надзорният орган не предприема действия по подадена жалба, изцяло или частично отхвърля или оставя без разглеждане жалба или не предприема действия, когато такива са необходими, за да се защитят правата на субекта на данни. […]“.

9 Член 2, параграфи 1 и 2 от този регламент предвижда:

„1. Настоящият регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

2. Настоящият регламент не се прилага за обработването на лични данни:

а) в хода на дейности, които са извън приложното поле на правото на Съюза;

б) от държавите членки, когато извършват дейности, които попадат в приложното поле на дял V, глава 2 от ДЕС;

в) от физическо лице в хода на чисто лични или домашни занимания;

г) от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност“.

10 Член 4 от посочения регламент гласи:

„За целите на настоящия регламент:

[…]

2) „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

[…]

7) „администратор“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държава членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка;

8) „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

9) „получател“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели“; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

[…]“.

11 Член 23 от същия регламент гласи:

„1. В правото на Съюза или правото на държава членка, което се прилага спрямо администратора или обработващия лични данни, чрез законодателна мярка може да се ограничи обхватът на задълженията и правата, предвидени в членове 12—22 и в член 34, както и в член 5, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 12—22, когато подобно ограничение е съобразено със същността на основните права и свободи и представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантира:

а) националната сигурност;

б) отбраната;

в) обществената сигурност;

г) предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от и предотвратяването на заплахи за обществената сигурност;

[…]

2. По-специално, всяка законодателна мярка, посочена в параграф 1, съдържа специални разпоредби най-малко, където е целесъобразно, по отношение на:

а) целите на обработването или категориите обработване;

б) категориите лични данни;

в) обхвата на въведените ограничения;

г) гаранциите за предотвратяване на злоупотреби или незаконен достъп или предаване;

д) спецификацията на администратора или категориите администратори;

е) периодите на съхранение и приложимите гаранции, като се вземат предвид естеството, обхватът и целите на обработването или категориите обработване;

ж) рисковете за правата и свободите на субектите на данни; и

з) правото на субектите на данни да бъдат информирани за ограничаването, освен ако това би било в разрез с целта на ограничаването“.

12 Глава V от ОРЗД, озаглавена „Предаване на лични данни на трети държави или международни организации“, включва членове 44—50 от този регламент. Съгласно член 44, озаглавен „Общ принцип на предаването на данни“:

„Предаване на лични данни, които се обработват или са предназначени за обработване след предаването на трета държава или на международна организация, се осъществява само при условие че са спазени другите разпоредби на настоящия регламент, само ако администраторът и обработващият лични данни спазват условията по настоящата глава, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация. Всички разпоредби на настоящата глава се прилагат, за да се направи необходимото нивото на защита на физическите лица, осигурено от настоящия регламент, да не се излага на риск“.

13 Член 45 от този регламент, озаглавен „Предаване на данни въз основа на решение относно адекватното ниво на защита“, предвижда в параграфи 1—3:

„1. Предаване на лични данни на трета държава или международна организация може да има, ако Комисията реши, че тази трета държава, територия или един или повече конкретни сектори в тази трета държава, или въпросната международна организация осигуряват адекватно ниво на защита. За такова предаване не се изисква специално разрешение.

2. При оценяване на адекватността на нивото на защита Комисията отчита по-специално следните елементи:

а) върховенството на закона, спазването на правата на човека и основните свободи, съответното законодателство — както общо, така и секторно, включително в областта на обществената сигурност, отбраната, националната сигурност и наказателното право и достъпа на публичните органи до лични данни, а също и прилагането на такова законодателство, правилата за защита на данните, професионалните правила и мерките за сигурност, включително правилата за последващо предаване на лични данни на друга трета държава или международна организация, които се спазват в тази държава или международна

организация, съдебната практика, както и действителните и приложими права на субектите на данни и ефективната административна и съдебна защита за субектите на данни, чиито лични данни се предават;

б) наличието и ефективното функциониране на един или повече независими надзорни органи във въпросната трета държава или на които се подчинява дадена международна организация, отговорни за осигуряване и прилагане на правилата за защита на данните, включително адекватни правомощия за прилагане, за подпомагане и консултиране на субектите на данни при упражняването на техните права и осъществяване на сътрудничество с надзорните органи на държавите членки; и

в) международните ангажименти, които съответната трета държава или международна организация е поела, или други задължения, произтичащи от правно обвързващи конвенции или инструменти, както и от участието ѝ в многостранни или регионални системи, по-конкретно по отношение на защитата на личните данни.

3. След оценка на адекватността на нивото на защита Комисията може чрез акт за изпълнение да реши, че дадена трета държава, територия или един или повече конкретни сектори в тази трета държава, или дадена международна организация осигуряват адекватно ниво на защита по смисъла на параграф 2 от настоящия член. 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. В акта за изпълнение се уточнява неговото териториално и секторно приложение и, ако е приложимо, се посочват надзорният орган или органи, посочени в параграф 2, буква б) от настоящия член. Актът за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в член 93, параграф 2“.

14 Член 46 от посочения регламент, озаглавен „Предаване на данни с подходящи гаранции“, предвижда в параграфи 1—3:

„1. При липса на решение съгласно член 45, параграф 3, администраторът или обработващият лични данни може да предава лични данни на трета държава или международна организация само ако е предвидил подходящи гаранции и при условие че са налице приложими права на субектите на данни и ефективни правни средства за защита.

2. Подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени, без да се изисква специално разрешение от надзорния орган, посредством:

а) инструмент със задължителен характер и с изпълнителна сила между публичните органи или структури;

б) задължителни фирмени правила в съответствие с член 47;

в) стандартни клаузи за защита на данните, приети от Комисията в съответствие с процедурата по разглеждане, посочена в член 93, параграф 2;

г) стандартни клаузи за защита на данните, приети от надзорен орган и одобрени от Комисията съгласно процедурата по разглеждане, посочена в член 93, параграф 2;

д) одобрен кодекс за поведение съгласно член 40, заедно със задължителни ангажименти с изпълнителна сила на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни; или

е) одобрен механизъм за сертифициране съгласно член 42, заедно със задължителни и изпълними ангажименти на администратора или обработващия лични данни в третата държава да прилагат подходящите гаранции, включително по отношение на правата на субектите на данни.

3. При условие че компетентният надзорен орган е дал разрешение, подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени по-специално и посредством:

а) договорни клаузи между администратора или обработващия лични данни и администратора, обработващия лични данни или получателя на личните данни в третата държава или международната организация; или

б) разпоредби, които да се включват в административните договорености между публичните органи или структури, съдържащи действителни и приложими права на субектите на данни“.

15 Член 49 от същия регламент, озаглавен „Дерогации в особени случаи“, посочва:

„1. При липса на решение относно адекватното ниво на защита съгласно член 45, параграф 3 или на подходящи гаранции съгласно член 46, включително задължителни фирмени правила, предаване или съвкупност от предавания на лични данни на трета държава или международна организация се извършва само при едно от следните условия:

а) субектът на данните изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран за свързаните с предаването възможни рискове за субекта на данните поради липсата на решение относно адекватното ниво на защита и на подходящи гаранции;

б) предаването е необходимо за изпълнението на договор между субекта на данните и администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;

в) предаването е необходимо за сключването или изпълнението на договор, сключен в интерес на субекта на данните между администратора и друго физическо или юридическо лице;

г) предаването е необходимо поради важни причини от обществен интерес;

д) предаването е необходимо за установяването, упражняването или защитата на правни претенции;

е) предаването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

ж) предаването се извършва от регистър, ко[й]то съгласно правото на Съюза или правото на държавите членки е предназначен[…] да предоставя информация на обществеността и е достъп[ен] за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

Когато предаването не може да се основава на разпоредба на членове 45 или 46, включително разпоредби относно задължителни фирмени правила, и не е приложима нито една от дерогациите в особени случаи, посочени в първата алинея на настоящия параграф, предаването на данни на трета държава или международна организация може да се извършва само ако

предаването не е повторяемо, засяга само ограничен брой субекти на данни, необходимо е за целите на неоспоримите законни интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данни и администраторът е оценил всички обстоятелства, свързани с предаването на данните, и въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни. Администраторът уведомява надзорния орган за предаването на данни. В допълнение към предоставянето на информацията, посочена в членове 13 и 14, администраторът информира субекта на данни за предаването, както и за преследваните неоспорими[…] законни интереси.

2. Предаването съгласно параграф 1, първа алинея, буква ж) не трябва да включва всички лични данни или всички категории лични данни, съдържащи се в регистъра. Когато регистърът е предназначен за справка от лица, които имат законен интерес, предаването се извършва единствено по искане на тези лица или ако те са получателите.

3. Параграф 1, първа алинея, букви а), б) и в) и параграф 1, втора алинея не се прилагат за дейности, извършвани от публичните органи при упражняването на техните публични правомощия.

4. Обществеият интерес, посочен в параграф 1, първа алинея, буква г) се признава в правото на Съюза или правото на държавата членка, което се прилага спрямо администратора.

5. При липсата на решение относно адекватното ниво на защита, правото на Съюза или правото на държава членка може, по важни причини от обществен интерес, изрично да определи ограничения за предаването на специални категории данни на трета държава или международна организация. Държавите членки съобщават тези разпоредби на Комисията.

6. Администраторът или обработващият лични данни документира оценката, както и подходящите гаранции по параграф 1, втора алинея от настоящия член в регистрите, посочени в член 30“.

16 Съгласно член 51, параграф 1 от ОРЗД:

„Всяка държава членка осигурява един или повече независими публични органи, които са отговорни за наблюдението на прилагането на настоящия регламент, за да се защитят основните права и свободи на физическите лица във връзка с обработването и да се улесни свободното движение на личните данни в рамките на Съюза („надзорен орган“)“.

17 Съгласно член 55, параграф 1 от този регламент „[в]секи надзорен орган е компетентен да изпълнява задачите и да упражнява правомощията, възложени му в съответствие с настоящия регламент, на територията на своята собствена държава членка“.

18 Съгласно член 57, параграф 1 от посочения регламент:

„Без да се засягат останалите задачи, определени с настоящия регламент, на своята територия всеки надзорен орган:

а) наблюдава и осигурява прилагането на настоящия регламент;

[…]

е) разглежда жалбите, подадени от субект на данни […] и разследва предмета на жалбата, доколкото това е целесъобразно, и информира жалбоподателя за напредъка и резултатите от разследването в разумен срок, особено ако е необходимо по-нататъшно разследване или координиране с друг надзорен орган;

[…]“.

19 Съгласно член 58, параграфи 2 и 4 от същия регламент:

„2. Всеки надзорен орган има всички от посочените по-долу корективни правомощия:

[…]

е) да налага временно или окончателно ограничаване, в т.ч. забрана, на обработването на данни;

[…]

й) да разпорежда преустановяването на потока на данни към получател в трета държава или към международна организация;

[…]

4. Упражняването на правомощията, предоставени на надзорния орган по силата на настоящия член, се осъществява при осигуряване на подходящи гаранции, в т.ч. ефективни съдебни средства за правна защита и справедлив съдебен процес, определени в правото на Съюза и правото на държава членка в съответствие с Хартата“.

20 Член 64, параграф 2 от ОРЗД посочва:

Всеки надзорен орган, председателят на [Европейския комитет по защита на данните (ЕКЗД)] или Комисията може да поиска разглеждането на въпрос с общо приложение или с последици в повече от една държава членка от Комитета с цел получаване на становище, по-специално когато даден компетентен надзорен орган не изпълнява задълженията за взаимопомощ съгласно член 61 или за съвместни операции съгласно член 62“.

21 Съгласно член 65, параграф 1 от този регламент:

„С цел да осигури правилно и последователно прилагане на настоящия регламент в отделните случаи, Комитетът приема решение със задължителен характер в следните случаи:

[…]

в) когато компетентният надзорен орган не е поискал становището на Комитета в случаите, посочени в член 64, параграф 1, или не се е съобразил със становището на Комитета, дадено по член […]64. В този случай всеки засегнат надзорен орган или Комисията може да отнесе въпроса до Комитета“.

22 Член 77 от посочения регламент, озаглавен „Право на подаване на жалба до надзорен орган“, посочва:

„1. Без да се засягат които и да било други административни или съдебни средства за правна защита, всеки субект на данни има право да подаде жалба до надзорен орган, по-специално в държавата членка на обичайно местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, отнасящи се до него, нарушава разпоредбите на настоящия регламент.

2. Надзорният орган, до когото е подадена жалбата, информира жалбоподателя за напредъка в разглеждането на жалбата и за резултата от нея, включително за възможността за съдебна защита съгласно член 78“.

23 Член 78 от същия регламент, озаглавен „Право на ефективна съдебна защита срещу надзорен орган“, предвижда в параграфи 1 и 2:

„1. Без да се засягат които и да било други административни или несъдебни средства за защита, всяко физическо и юридическо лице има право на ефективна съдебна защита срещу отнасящо се до него решение със задължителен характер на надзорен орган.

2. Без да се засягат които и да било други административни или несъдебни средства за защита, всеки субект на данни има право на ефективна съдебна защита, когато надзорният орган, който е компетентен съгласно членове 55 и 56[,] не е разгледал жалбата или не е информирал субекта на данните в срок от три месеца за напредъка в разглеждането на жалбата, подадена съгласно член 77, или за резултата от нея“.

24 Член 94 от ОРЗД гласи:

„1. Директива [95/46] се отменя, считано от 25 май 2018 г.

2. Позоваванията на отменената директива се тълкуват като позовавания на настоящия регламент. Позоваванията на Работната група за защита на лицата при обработването на лични данни, създадена по силата на член 29 от Директива [95/46], се тълкуват като позовавания на Европейския комитет по защита на личните данни, създаден с настоящия регламент“.

25 Съгласно член 99 от този регламент:

„1. Настоящият регламент влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

2. Прилага се от 25 май 2018 г.“.

Решението СК

26 Съображение 11 от решението СК гласи следното:

„Надзорните органи на държавите членки играят ключова роля в този договорен механизъм, като осигуряват достатъчна степен на защита на личните данни след предаването им. В изключителни случаи, когато износителите на данни откажат или не са в състояние да инструктират по подходящ начин вносителя на данни и съществува непосредствен риск от тежка вреда за заинтересованите физически лица, стандартните договорни клаузи трябва да позволяват на надзорните органи да подложат вносителите на данни и подизпълнителите на проверка и ако е необходимо, да вземат решения, които са задължителни за вносителите на данни и подизпълнителите. Надзорните органи следва да имат правомощието да забраняват или да спират предаването на данни или набора от предавания на данни въз основа на стандартните договорни клаузи в такива изключителни случаи, в които е установено, че предаването въз основа на договор може да има съществени неблагоприятни последици върху гаранциите и задълженията, предоставящи достатъчна степен на защита на заинтересованото физическо лице“.

27 Член 1 от това решение гласи:

„Счита се, че стандартните договорни клаузи, съдържащи се в приложението, предоставят достатъчни гаранции за защитата на личния живот и основните права и свободи на физическите лица, както и по отношение на упражняването на съответните права, както се изисква от член 26, параграф 2 от Директива [95/46]“.

28 Съгласно член 2, втора алинея от посоченото решение то „се прилага за предаването на лични данни от администраторите на данни, установени в Европейския съюз, към получатели, установени извън територията на Европейския съюз, които действат изключително като лица, обработващи данните“.

29 Член 3 от същото решение посочва:

„За целите на настоящото решение се прилагат следните определения:

[…]

в) „износител на данни“ означава администраторът, който предава личните данни;

г) „вносител на данни“ означава лицето, обработващо данните, установено в трета страна, което приема да получава от износителя на данни лични данни, предназначени за обработване от името на износителя на данни след предаване съгласно неговите инструкции и при условията на настоящото решение, и което не е част от системата на трета страна, осигуряваща достатъчна степен на защита по смисъла на член 25, параграф 1 от Директива [95/46];

[…]

е) „приложимо право за защита на данните“ означава законодателството, защитаващо основните права и свободи на лицата, и по-специално правото на личен живот при обработването на лични данни, приложимо към администратор на данни в държавата членка, в която е установен износителят на данни;

[…]“.

30 В първоначалната си редакция, предхождаща влизането в сила на Решение за изпълнение 2016/2297, член 4 от Решение 2010/87 е предвиждал:

„1. Без да се накърняват правомощията им да предприемат мерки за осигуряване на спазването на националните разпоредби, приети съгласно глави II, III, V и VI от Директива [95/46], компетентните органи на държавите членки могат да упражняват правомощията, с които разполагат, за да забраняват или да спират потоците от данни към трети страни с цел защитата на физически лица при обработването на техните лични данни, в случай че:

а) е установено, че правото, което се прилага спрямо вносителя на данни или подизпълнител, му налага задължения за дерогиране от приложимото право за защита на данните, които се простират извън ограниченията, необходими в едно демократично общество, предвидени в член 13 от Директива [95/46], когато тези задължения могат да има[т] съществени неблагоприятни последици за гаранциите, предоставени от приложимото право за защита на данните и стандартните договорни клаузи;

б) компетентен орган е установил, че вносителят на данни или подизпълнител не е спазил стандартните договорни клаузи от приложението; или

в) е много вероятно стандартните договорни клаузи от приложението да не са или да не бъдат спазени и продължаването на предаването да създаде непосредствен риск от тежка вреда за заинтересованите физически лица.

2. Забраната или спирането съгласно параграф 1 се отменя веднага след като причините за забраната или спирането престанат да съществуват.

3. Когато държавите членки приемат мерки съгласно параграфи 1 и 2, те незабавно информират Комисията, която предоставя информацията на другите държави членки“.

31 Съображение 5 от Решение за изпълнение 2016/2297, прието след обявяването на решение от 6 октомври 2015 г., Schrems (C-362/14, EU:C:2015:650), гласи следното:

„Mutatis mutandis, решение на Комисията, прието на основание член 26, параграф 4 от Директива [95/46], е задължително за всички органи на държавите членки, към които е адресирано, включително независимите надзорни органи на държавите членки, доколкото такова решение има за последица признаването, че предаване, осъществяващо се въз основа на стандартни договорни клаузи, фигуриращи в него, предлага достатъчни гаранции, както изисква член 26, параграф 2 от Директивата. Това не възпрепятства даден национален надзорен орган да упражни своите правомощия за надзор върху потоците от данни, включително правомощието да спира или забранява предаването на лични данни, когато прецени, че то се извършва в нарушение на правото на ЕС или на националното право за защита на данните, като например в случаите, когато вносителят на данни не спазва стандартните договорни клаузи“.

32 В настоящата си редакция, произтичаща от Решение за изпълнение 2016/2297, член 4 от решение СК посочва:

„Когато компетентните органи в държавите членки упражняват своите правомощия съгласно член 28, параграф 3 от Директива [95/46], в резултат на което спират или окончателно забраняват потоци данни към трети страни с цел да защитят лицата във връзка с обработката на техните лични данни, въпросната държава членка следва незабавно да информира Комисията, която от своя страна ще предаде информацията на останалите държави членки“.

33 Приложението към решение СК, озаглавено „Стандартни договорни клаузи (лица, обработващи данните)“, съдържа дванадесет стандартни клаузи. Клауза 3 от приложението, озаглавена „Клауза в полза на трето лице“, предвижда:

„1. Заинтересованото физическо лице може да иска прилагането спрямо износителя на данни на настоящата клауза, клауза 4, букви б)—и), клауза 5, букви а)—д) и букви ж)—й), клауза 6, параграфи 1 и 2, клауза 7, клауза 8, параграф 2 и клаузи 9—12, като трето лице бенефициер.

2. Заинтересованото физическо лице може да иска прилагането спрямо вносителя на данни на настоящата клауза, клауза 5, букви а)—д) и буква ж), клауза 6, клауза 7, клауза 8, параграф 2 и клаузи 9—12, в случай че износителят на данни е изчезнал фактически или е престанал да съществува юридически, освен ако правоприемник не е поел всички правни задължения на износителя на данни чрез договор или по закон, в резултат на което правата и задълженията на износителя на данни преминават върху правоприемника, в който случай физическото лице може да иска прилагането им спрямо правоприемника.

[…]“.

34 Съгласно клауза 4 от това приложение, озаглавена „Задължения на износителя на данни“:

„Износителят на данни приема и гарантира, че:

а) обработването, включително самото предаване, на лични данни се извършва и ще продължава да се извършва съгласно съответните разпоредби на приложимото право за защита на данните (и ако е приложимо, съответните компетентни органи на държавата членка, в която е установен износителят на данни, са били уведомени за обработването) и не нарушава съответните разпоредби на тази държава;

б) е инструктирал и по време на периода на услугите по обработване на личните данни ще инструктира вносителя на данни да обработва предаваните лични данни единствено от името на износителя на данни и в съответствие с приложимото право за защита на данните и клаузите;

[…]

е) ако предаването включва специални категории от данни, заинтересованото физическо лице е било информирано или ще бъде информирано преди или непосредствено след предаването, че неговите данни могат да бъдат предадени на трета страна, която не осигурява достатъчна степен на защита по смисъла на Директива [95/46];

ж) ще изпрати всяко уведомление, получено от вносителя на данни или от подизпълнител съгласно клауза 5, буква б) и клауза 8, параграф 3, на надзорния орган за защита на данните, ако износителят на данни реши да продължи предаването или да отмени спирането;

[…]“.

35 Клауза 5 от посоченото приложение, озаглавена „Задължения на вносителя на данни […]“, предвижда:

„Вносителят на данни приема и гарантира, че:

а) ще обработва личните данни единствено от името на износителя на данни и в съответствие с неговите инструкции и клаузите; ако не може да осигури такова съответствие по каквито и да е причини, той приема да информира своевременно износителя на данни за невъзможността да осигури съответствие, като в такъв случай износителят на данни може да спре предаването на данни и/или да прекрати договора;

б) няма причини да се смята, че приложимото за него законодателство го възпрепятства да изпълнява инструкциите, получени от износителя на данни, и задълженията си по договора и че в случай на промяна на това законодателство, която може да има съществени неблагоприятни последици върху гаранциите и задълженията, предвидени от клаузите, той своевременно ще уведоми износителя на данни за промяната[, щом узнае за нея], като в такъв случай износителят на данни може да спре предаването на данни и/или да прекрати договора;

[…]

г) своевременно ще уведомява износителя на данни за:
   i) всяко правнообвързващо искане за разкриване на личните данни от правоприлагащ орган, освен ако в закона не е предвидено друго, като например наказателноправна забрана за разкриване на информация с цел запазване на тайната на разследване от страна на правоприлагащ орган,
   ii) всеки случай на неволен или неразрешен достъп, и
   iii) всяко искане, получено пряко от заинтересованите физически лица, без да отговаря на такова искане, освен ако не му е било разрешено;

[…]“.

36 Бележката под линия, към която препраща заглавието на тази клауза 5, посочва:

„Императивните изисквания на националното законодателство, прилагащи се за вносителя на данни, които не се простират извън необходимото в едно демократично общество, въз основа на един от интересите, изброени в член 13, параграф 1 от Директива [95/46], т.е. ако те представляват необходима мярка за гарантиране на националната сигурност, отбраната, обществената сигурност, предотвратяването, разследването, разкриването и преследването на престъпления или на нарушения на етичните кодекси при регламентираните професии, важни икономически и финансови интереси на държавата или защитата на заинтересованото физическо лице или на правата и свободите на други лица, не са в противоречие със стандартните договорни клаузи. […]“.

37 Клауза 6 от приложението към решението СК, озаглавена „Отговорност“, предвижда:

„1. Страните се споразумяват, че всяко физическо лице, което претърпи вреда в резултат на нарушаване на задълженията, посочени в клауза 3 или в клауза 11 от страна на една от страните или на подизпълнител, има право да получи обезщетение от износителя на данни за претърпяната вреда.

2. Ако заинтересованото физическо лице не може да подаде иск за обезщетение в съответствие с параграф 1, произтичащ от нарушение от страна на вносителя на данни или негов подизпълнител на техните задължения, посочени в клауза 3 или в клауза 11, поради това че износителят на данни е изчезнал фактически или е престанал да съществува юридически или е изпаднал в несъстоятелност, вносителят на данни приема, че заинтересованото физическо лице може да подаде иск срещу него, както ако той би бил износителя на данни […].

[…]“.

38 Клауза 8 от това приложение, озаглавена „Сътрудничество с надзорните органи“, предвижда в параграф 2:

„Страните се споразумяват, че надзорният орган има право да извършва проверка на вносителя на данни и на всеки подизпълнител със същия обхват и при същите условия, които биха се прилагали за проверка на износителя на данни съгласно приложимото право за защита на данните“.

39 В клауза 9 от посоченото приложение, озаглавена „Приложимо право“, се уточнява, че клаузите трябва да бъдат съобразени с правото на държавата членка, в която е установен износителят на данни.

40 Съгласно клауза 11 от същото приложение, озаглавена „Предаване за подизпълнение“:

„1. Вносителят на данни няма да предава за подизпълнение операциите по обработване, извършвани от името на износителя на данни съгласно клаузите, без предварителното писмено съгласие на износителя на данни. Вносителят на данни предава за подизпълнение задълженията си съгласно клаузите със съгласието на износителя на данни само посредством писмено споразумение с подизпълнителя, което налага на подизпълнителя същите задължения като тези, наложени на вносителя на данни съгласно клаузите […].

2. Предварителният писмен договор между вносителя на данни и подизпълнителя предвижда също така клауза в полза на трето лице, като тази от клауза 3, за случаи, в които заинтересованото физическо лице не може да подаде иска за обезщетение, посочен в клауза 6, параграф 1, срещу износителя на данни или срещу вносителя на данни поради това че те са изчезнали фактически или са престанали да съществуват юридически или са изпаднали в

несъстоятелност, и няма правоприемник, който да е поел всички правни задължения на износителя на данни или на вносителя на данни чрез договор или по закон. Такава гражданска отговорност на подизпълнителя е ограничена до собствените му операции по обработване съгласно клаузите.

[…]“.

41 Клауза 12 от приложението към решението СК, озаглавена „Задължение след приключване на услугите по обработване на лични данни“, предвижда в параграф 1:

„Страните се споразумяват, че при приключване на предоставянето на услуги по обработване на лични данни вносителят на данни и подизпълнителят, по избор на износителя на данни, връщат всички предадени лични данни и направените копия на износителя на данни или унищожават всички лични данни и удостоверяват този факт на износителя на данни, освен ако приложимото спрямо вносителя на данни законодателство го възпрепятства да върне или да унищожи всички или част от предадените лични данни. […]“.

Решението ЩЛД

42 С решение от 6 октомври 2015 г., Schrems (C-362/14, EU:C:2015:650) Съдът обявява за невалидно Решение 2000/520/ЕО на Комисията от 26 юли 2000 година съгласно Директива 95/46 относно адекватността на защитата, гарантирана от принципите за „сфера на неприкосновеност на личния живот“ и свързаните с това често задавани въпроси, публикувани от Департамента по търговия на САЩ (ОВ L 215, 2000 г., стр. 7; Специално издание на български език, 2007 г., глава 16, том 1, стр. 64), в което Комисията констатира, че тази трета страна гарантира адекватно ниво на защита.

43 След обявяването на това съдебно решение Комисията приема решението ЩЛД, след като за целите на приемането му извършва оценка на правната уредба на Съединените щати, както се уточнява в съображение 65 от посоченото решение:

„Комисията направи оценка на ограниченията и гаранциите, които са предвидени в правото на САЩ във връзка с достъпа и използването на лични данни, предавани съгласно Щита за личните данни в отношенията между [Европейския съюз] и САЩ, от публичните органи на САЩ за целите на националната сигурност, правоприлагането и за други цели от обществен интерес. Освен това правителството на САЩ, чрез Службата на директора на Националното разузнаване (Office of the Director of National Intelligence (ODNI) […], предостави на Комисията подробни писмени изявления и ангажименти, които са поместени в приложение VI към настоящото решение. С писмо, подписано от Държавния секретар и приложено като приложение III към настоящото решение, правителството на САЩ се ангажира също така да създаде нов механизъм за надзор относно намесата за целите на националната сигурност — омбудсман към Щита за личните данни, който е независим от разузнавателните структури. И накрая, в писмено изявление на Министерството на правосъдието на САЩ, поместено в приложение VII към настоящото решение, са разгледани ограниченията и гаранциите, които се прилагат спрямо достъпа и използването на данни от страна на публичните органи за целите на правоприлагането и за други цели от обществен интерес. За да се повиши прозрачността и да се отрази правният характер на тези ангажименти, всеки от посочените и приложени към настоящото решение документи ще бъде публикуван във Федералния регистър на САЩ“.

44 Анализът на Комисията относно тези ограничения и гаранции е обобщен в съображения 67—135 от решението ЩЛД, докато изводите на тази институция относно адекватната степен на защита съгласно Щита за личните данни в отношенията между Европейския съюз и Съединените щати се съдържат в съображения 136—141 от него.

45 По-специално съображения 68, 69, 76, 77, 109, 112—116, 120, 136 и 140 от това решение посочват:

„(68) Съгласно конституцията на САЩ гарантирането на националната сигурност е в правомощията на Президента, в качеството му на върховен главнокомандващ, върховен изпълнителен орган, а по отношение на външното разузнаване — и ръководител на външната политика на САЩ […]. Докато Конгресът има правомощията да налага ограничения и е правил това по различни въпроси, в обхвата на така наложените граници Президентът може да направлява дейността на разузнавателните структури на САЩ, по-специално чрез издаване на изпълнителни декрети и президентски директиви. […] Понастоящем двата главни правни инструмента в тази връзка са Изпълнителен декрет 12333 [Executive Order 12333, наричан по-нататък „EO 12333“] […] и Президентска изпълнителна директива 28 [Presidential Policy Directive 28, наричана по-нататък „PPD-28“].

(69) [PPD-28], издадена на 17 януари 2014 г., налага редица ограничения за операциите по „радиоелектронно разузнаване“ […]. Президентските директиви имат задължителна сила за разузнавателните органи на САЩ […] и остават в сила и след промени в администрацията на САЩ […]. [PPD-28] е особено важна за лицата, които не са американски граждани, включително за субектите на данни от ЕС. […]

[…]

(76) Въпреки че не са формулирани със същата правна терминология, тези принципи [на PPD-28] отразяват същността на принципите на необходимост и пропорционалност. […]

(77) В качеството на директива[,] издадена от Президента като главен изпълнителен орган, тези изисквания са обвързващи за всички разузнавателни структури и са въведени с допълнителни правила и процедури на агенциите, с които общите принципи са транспонирани в конкретни указания за всекидневната работа. […]

[…]

(109) И обратно, съгласно [член] 702 от [Foreign Intelligence Surveillance Act (Закон за упражняване на надзор върху външното разузнаване, наричан по-нататък „FISA“)], [United States Foreign Intelligence Surveillance Court (FISC) (Съд по надзора върху външното разузнаване на Съединените щати)] не дава разрешение за отделни мерки за наблюдение, а за програми за наблюдение (като PRISM, UPSTREAM) въз основа на годишни сертифицирания, изготвени от [United States Attorney General (главен прокурор)] и от [Director of National Intelligence (DNI) (директор на националното разузнаване)]. […] Както е посочено, в сертифицираният, подлежащи на одобрение от [FISA], не се съдържа информация относно отделните лица, които ще бъдат обект на разследване, а се посочват категориите външноразузнавателна информация […]. [FISA] не прави преценка дали — по определена вероятна причина или според някакво друго изискване — лицата са определени правилно за обект на разследване с цел придобиване на разузнавателни данни […], а неговите контролни функции се простират до проверка на условието, че „значима цел на придобиването е получаването на външноразузнавателна информация“ […].

[…]

(112) Първо, в [FISA] са предвидени редица средства за правна защита, с които разполагат също и лицата, които не са граждани на САЩ, за оспорване на неправомерно електронно наблюдение […]. Това включва възможността физическите лица да предявят срещу

Съединените американски щати граждански иск за обезщетяване на финансови вреди, когато информацията за тях е била неправомерно и умишлено използвана или разкрита […]; да заведат дело срещу длъжностни лица от правителството на САЩ в лично качество („престъпление при изпълнение на служебните задължения“ — under colour of law) за финансови вреди […]); и да оспорват законността на наблюдението (и да искат заличаване на събраната информация), в случай че правителството на САЩ възнамерява да използва или разкрива информация, получена или производна от електронно наблюдение срещу лицето, в съдебни или административни производства в Съединените американски щати […].

(113) Второ, правителството на САЩ насочи вниманието на Комисията към редица допълнителни възможности, които субектите на данни от ЕС могат да използват, за да търсят правна защита срещу длъжностни лица при неправомерен достъп или използване на лични данни от страна на правителството, включително за възнамеряваните цели на националната сигурност […].

(114) И накрая, правителството на САЩ посочи [Freedom of information Act (FOIA) (Закон за свободата на информацията)] като средство, чрез което лица, които не са граждани на САЩ[,] могат да поискат достъп до съществуващи записи на федерални агенции, включително когато в тях се съдържат лични данни на лицето […]. Предвид насочеността му, този закон не осигурява възможност за индивидуална правна защита срещу намесата в лични данни като такава, въпреки че по принцип би могъл да позволява на физически лица да получат достъп до съответна информация, с която разполагат агенциите на националното разузнаване. […]

(115) Макар от това да следва, че лицата, включително субектите на данни от ЕС, имат редица възможности за правна защита, когато са станали обект на неправомерно (електронно) наблюдение за целите на националната сигурност, също така е ясно, че не са обхванати най-малкото някои от правните основания, които могат да се използват от разузнавателните органи на САЩ (напр. [EO 12333]). Освен това, дори когато по принцип са налице възможности за съдебна правна защита за лицата, които не са граждани на САЩ, например при наблюдение съгласно [FISA], възможните начини на действие са ограничени […] и предявените от лицата (включително граждани на САЩ) искове ще бъдат обявени за недопустими, ако [не могат да докажат процесуалната си легитимация], а това ограничава достъпа до обикновените съдилища […].

(116) С цел да осигури за всички субекти на данни от ЕС достъп до допълнителни [способи за защита], правителството на САЩ реши да създаде нов механизъм, омбудсмана към Щита за личните данни, както това е изложено в писмото на държавния секретар на САЩ до Комисията, съдържащо се в приложение III към настоящото решение. Механизмът е изграден, като се изхожда от определянето съгласно [PPD-28] на старши координатор (на ниво заместник-министър) в Държавния департамент за лице за контакт, пред което чуждите правителства могат да изразяват загриженост във връзка с дейности на радиоелектронното разузнаване на САЩ, но далеч надхвърля тази първоначална идея.

[…]

(120) [П]равителството на САЩ се ангажира да гарантира, че при изпълнението на функциите си, омбудсманът към Щита за личните данни ще може да разчита на надзора и сътрудничеството на други съществуващи механизми за разглеждане на спазването на законите на САЩ. […] Когато някой от тези надзорни органи установи несъответствие, съответната разузнавателна структура (напр. разузнавателна агенция) ще трябва да

отстрани несъответствието, тъй като само въз основа на това омбудсманът ще може да даде „положителен“ отговор на физическото лице (т.е. че установеното нарушение е отстранено), за което правителството на САЩ е поело ангажимент. […]

[…]

(136) С оглед на тези констатации Комисията счита, че Съединените американски щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към самосертифицирани дружества в Съединените американски щати съгласно Щита за личните данни в отношенията между [Европейския съюз] и САЩ.

[…]

(140) И накрая, въз основа на наличната информация за правния ред на САЩ, включително съгласно писмените изявления и ангажименти на правителството на САЩ, Комисията счита, че всяка намеса на публичните органи на Съединените американски щати за целите на националната сигурност, правоприлагането или за други цели от обществен интерес в основните права на физическите лица, чиито данни се предават от Съюза към Съединените щати съгласно Щита за личните данни, и произтичащите от това ограничения, налагани на самосертифицираните организации във връзка със спазването от тяхна страна на Принципите, ще бъде ограничена до строго необходимото за постигането на набелязаната легитимна цел, и че е налице ефективна правна защита срещу подобна намеса“.

46 Съгласно член 1 от решението ЩЛД:

„1. По смисъла на член 25, параграф 2 от Директива [95/46] Съединените американски щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към организации в Съединените щати съгласно Щита за личните данни в отношенията между [Европейския съюз] и САЩ.

2. Щитът за личните данни в отношенията между [Европейския съюз] и САЩ се състои от Принципите, публикувани от Министерството на търговията на САЩ на 7 юли 2016 г., както те са установени в приложение II, и официалните писмени изявления и ангажиментите, съдържащи се в документите, поместени в приложения I и III—VII.

3. За целите на параграф 1 личните данни се предават съгласно Щита за личните данни в отношенията между [Европейския съюз] и САЩ, когато предаването се извършва от Съюза към организации в Съединените американски щати, които са включени в „списъка към Щита за личните данни“, който се поддържа и се предоставя за публичен достъп от Министерството на търговията на САЩ, в съответствие с точки I и III от Принципите, установени в приложение II“.

47 В точка I.5. от приложение II към решението ЩЛД, озаглавено „Принципи на рамката на Щита за личните данни в отношенията между [Европейския съюз] и САЩ, публикувани от Министерството на търговията на САЩ“, се предвижда, че придържането към принципите може да бъде ограничено по-специално „до необходимата степен, с оглед спазване изискванията[, свързани с] националната сигурност, [с] обществения интерес или [с] правоприлагането“.

48 Приложение III към това решение съдържа писмо от г-н John Kerry, тогавашен Secretary of State (държавен секретар, Съединени щати), до комисаря по въпросите на правосъдието, потребителите и равнопоставеността между половете от 7 юли 2016 г., към което в

приложение A е включен меморандум, озаглавен „Механизъм на омбудсмана на щита за личните данни в отношенията между [Европейския съюз] и САЩ по отношение на радиоелектронното разузнаване“, който съдържа следния пасаж:

„Като признава значението на рамката на Щита за личните данни в отношенията между [Европейския съюз] и САЩ, настоящият меморандум определя процеса за прилагането на нов механизъм във връзка с радиоелектронното разузнаване в съответствие с [PPD-28].

[…] Президентът Обама обяви издаването на нов президентски указ — [PPD-28] — „за определяне по ясен начин какво правим и какво не правим, когато се отнася за нашите наблюдения зад граница“.

В [член] 4, буква d) от [PPD-28] се дават указания на държавния секретар да определи „старши координатор на международната дипломация в областта на информационните технологии“ (старши координатор), „който […] да изпълнява функциите на лице за връзка с чуждите правителства, които желаят да изразят безпокойство във връзка с дейностите на радиоелектронното разузнаване, провеждани от Съединените щати“.

[…]

1) Старшият координатор ще изпълнява функциите на омбудсман към Щита за личните данни и […] ще работи в тясно сътрудничество със съответните длъжностни лица от други министерства и агенции, които отговарят за обработването на искания съгласно приложимото законодателство и политиката на Съединените щати. Омбудсманът е независим от разузнавателната общност. Омбудсманът е пряко подчинен на държавния секретар, който ще гарантира, че Омбудсманът изпълнява функциите си обективно и без неправомерно влияние, което може да има отражение върху отговорите, които следва да се предоставят.

[…]“.

49 Приложение VI към решението ЩЛД съдържа писмо от Службата на директора на Националното разузнаване (Office of the Director of National Intelligence) до американското Министерство на търговията и до Администрацията по международна търговия от 21 юни 2016 г., в което се уточнява, че PPD-28 позволява „събирането на „масиви от данни“ […] на относително голям обем радиоелектронна разузнавателна информация или данни при обстоятелства, при които разузнавателните структури не могат да използват идентификатор, свързан с конкретния обект на разузнаване […], за да концентрират събирането на данни“.

Спорът в главното производство и преюдициалните въпроси

50 Г-н Schrems, пребиваващ в Австрия гражданин на тази държава, е потребител на социалната мрежа Facebook (наричана по-нататък „Facebook“) от 2008 г.

51 Всяко пребиваващо на територията на Съюза лице, което иска да използва Facebook, при регистрацията си е длъжно да сключи договор с Facebook Ireland, дъщерно дружество на Facebook Inc., чието седалище е в Съединените щати. Личните данни на пребиваващите на територията на Съюза потребители на Facebook Ireland изцяло или частично се предават към разположени на територията на Съединените щати сървъри на Facebook Inc., където се обработват.

52 На 25 юни 2013 г. г-н Schrems сезира комисаря с жалба, с която по същество иска от него да забрани на Facebook Ireland да предава личните му данни към Съединените щати, като твърди, че действащото право и практики в тази страна не гарантират достатъчна защита на съхраняваните на територията ѝ лични данни срещу извършваните в страната дейности по наблюдение от публичните органи. Тази жалба е отхвърлена по-специално с мотива че в Решение 2000/520 Комисията е констатирала, че Съединените щати гарантират достатъчна степен на защита.

53 High Court (Висш съд, Ирландия), пред който г-н Schrems обжалва отхвърлянето на жалбата му, сезира Съда с преюдициално запитване относно тълкуването и валидността на Решение 2000/520. С решение от 6 октомври 2015 г., Schrems (C-362/14, EU:C:2015:650) Съдът обявява това решение за невалидно.

54 Вследствие на това съдебно решение запитващата юрисдикция отменя отхвърлянето на жалбата на г-н Schrems и я връща на комисаря. В рамките на започнатото от последния разследване Facebook Ireland обяснява, че голяма част от личните данни е предадена на Facebook Inc. въз основа на стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК. Предвид тези обстоятелства комисарят приканва г-н Schrems да преформулира жалбата си.

55 В така преформулираната си жалба, подадена на 1 декември 2015 г., г-н Schrems изтъква по-специално, че американското право задължава Facebook Inc. да предостави предаваните му лични данни на американски органи като National Security Agency (NSA) (Агенция за национална сигурност, Съединени щати) и Federal Bureau of Investigation (FBI) (Федерално бюро за разследване, Съединени щати). Той поддържа, че тъй като тези данни са използвани в рамките на различни програми за наблюдение по несъвместим с членове 7, 8 и 47 от Хартата начин, решението СК не може да обоснове предаването на посочените данни на Съединените щати. При тези условия г-н Schrems иска от комисаря да забрани или да спре предаването на личните му данни на Facebook Inc.

56 На 24 май 2016 г. комисарят публикува „проект на решение“, в което обобщава предварителните изводи от своето разследване. В този проект той временно приема, че има опасност личните данни на гражданите на Съюза, предадени на Съединените щати, да бъдат консултирани и обработвани от американските органи по начин, който е несъвместим с членове 7 и 8 от Хартата, и че правото на Съединените щати не предоставя на тези граждани съвместими с член 47 от Хартата способи за защита. Комисарят счита, че стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК, не могат да преодолеят този недостатък, доколкото те предоставят на субектите на данни само договорни права срещу износителя и вносителя на данни, без обаче да обвързват американските органи.

57 Тъй като счита, че при тези условия преформулираната жалба на г-н Schrems повдига въпроса за валидността на решението СК, на 31 май 2016 г. комисарят сезира High Court (Висш съд), като се позовава на съдебната практика, произтичаща от решение от 6 октомври 2015 г., Schrems (C-362/14, EU:C:2015:650, т. 65), за да отправи запитване до Съда по този въпрос. С акт от 4 май 2018 г. High Court (Висш съд) сезира Съда с настоящото преюдициално запитване.

58 High Court (Висш съд) прилага към това преюдициално запитване решение, постановено на 3 октомври 2017 г., в което отразява резултата от разглеждането на представените пред него доказателства в рамките на националното производство, в което е участвало американското правителство.

59 В това решение, към което многократно препраща преюдициалното запитване, запитващата юрисдикция отбелязва, че по принцип има не само правото, но и задължението да разгледа всички изложени пред нея факти и доводи, за да реши въз основа на тях дали се изисква

преюдициално запитване. Във всеки случай тя счита, че е длъжна да вземе предвид евентуалните изменения на правото, настъпили между подаването на жалбата и организираното от нея съдебно заседание. Тази юрисдикция уточнява, че в рамките на главното производство собствената ѝ преценка не се ограничава до основанията за невалидност, изтъкнати от комисаря, така че и тя може да изтъкне служебно други основания за невалидност и въз основа на тях да отправи преюдициално запитване.

60 Съгласно констатациите, съдържащи се в посоченото съдебно решение, разузнавателните дейности на американските органи във връзка с предаваните на Съединените щати лични данни се основават по-специално на член 702 от FISA и на EO 12333.

61 Що се отнася до член 702 от FISA, запитващата юрисдикция уточнява в същото съдебно решение, че този член позволява на главния прокурор и на директора на националното разузнаване да разрешават съвместно, след одобрение от FISC, с цел получаване на „външноразузнавателна информация“, наблюдението на лица, които не са американски граждани, намиращи се извън територията на Съединените щати, и служи по-специално за основание на програмите за наблюдение PRISM и UPSTREAM. Съгласно констатациите на тази юрисдикция, в рамките на програмата PRISM доставчиците на интернет услуги са длъжни да предоставят на NSA всички съобщения, изпратени и получени съгласно „критерий за подбор“, като част от тях също се предават на FBI и на Central Intelligence Agency (CIA) (Централно разузнавателно управление, Съединени щати).

62 Що се отнася до програмата UPSTREAM, посочената юрисдикция констатира, че в рамките на тази програма далекосъобщителните предприятия, които управляват „опорната мрежа“ — тоест кабелната мрежа, комутаторите и рутерите — са принудени да позволят на NSA да копира и да филтрира потоците интернет трафик, за да събира изпратени съобщения от, към или относно лице, което не е американски гражданин, обхванато от „критерий за подбор“. В рамките на посочената програма NSA има достъп, съгласно констатациите на същата юрисдикция, както до метаданните, така и до съдържанието на съответните съобщения.

63 Що се отнася до EO 12333, запитващата юрисдикция констатира, че той позволява на NSA да получи достъп до данни, които се „пренасят“ към Съединените щати чрез достъп до подводните кабели, разположени на дъното на Атлантическия океан, както и да събира и съхранява тези данни, преди те да пристигнат в Съединените щати и за тях да бъдат приложени разпоредбите на FISA. Тя пояснява, че основаните на EO 12333 дейности не са уредени от закона.

64 Що се отнася до ограниченията на разузнавателните дейности, запитващата юрисдикция подчертава факта, че лицата, които не са американски граждани, попадат единствено в обхвата на PPD-28 и че този акт само посочва, че разузнавателните дейности трябва да бъдат „съобразени с конкретния случай, доколкото това е практически възможно“ („as tailored as feasible“). Въз основа на констатациите си посочената юрисдикция счита, че Съединените щати обработват масиви от данни, без да осигурят защита, която по същество е равностойна на гарантираната с членове 7 и 8 от Хартата.

65 Що се отнася до съдебната защита, същата юрисдикция посочва, че гражданите на Съюза нямат достъп до същите правни средства за защита като тези, с които разполагат американските граждани срещу обработването на лични данни от американските органи, тъй като четвъртата поправка на Constitution of the United States (Конституцията на Съединените щати), която съгласно американското право е най-важната защита срещу незаконното наблюдение, е неприложима за гражданите на Съюза. В това отношение запитващата юрисдикция уточнява, че оставащите на разположение на последните правни средства за защита се сблъскват със значителни препятствия, по-специално задължението — според нея изключително трудно за изпълнение — да обосноват процесуалната си легитимация. Освен това съгласно констатациите на тази юрисдикция дейностите на NSA, основаващи се на EO 12333, не са предмет на съдебен

надзор и не могат да бъдат обжалвани по съдебен ред. Накрая, посочената юрисдикция счита, че доколкото според нея омбудсманът към Щита за личните данни не е съд по смисъла на член 47 от Хартата, американското право не осигурява на гражданите на Съюза ниво на защита, което по същество е равностойно на това, което е гарантирано от основното право, закрепено в този член.

66 В преюдициалното си запитване запитващата юрисдикция уточнява още, че страните в главното производство спорят по-специално по въпроса за приложимостта на правото на Съюза към предаването на трета държава на лични данни, които могат да бъдат обработвани от органите на тази държава по-специално за целите на националната сигурност, както и относно обстоятелствата, които следва да се вземат предвид при преценката на осигуряваната от тази държава достатъчна степен на защита. По-специално тази юрисдикция отбелязва, че според Facebook Ireland констатации на Комисията относно адекватността на осигурената от трета държава защита, каквито са съдържащите се в решението ЩЛД, обвързват надзорните органи и в контекста на предаване на лични данни, основано на стандартните клаузи за защита на данните, съдържащи се в приложението към решението СДК.

67 Що се отнася до тези стандартни клаузи за защита на данните, посочената юрисдикция иска да се установи дали решението СК може да се счита за валидно, въпреки че според същата юрисдикция посочените клаузи не са задължителни за държавните органи на съответната трета страна и следователно не могат да отстранят евентуална липса на достатъчна степен на защита в тази страна. В това отношение тя счита, че възможността, призната на компетентните органи на държавите членки с член 4, параграф 1, буква а) от Решение 2010/87, в редакцията му преди влизането в сила на Решение за изпълнение 2016/2297, да забранят предаването на лични данни към трета страна, налагаща на вносителя задължения, несъвместими с гаранциите, съдържащи се в същите тези клаузи, показва, че състоянието на правото на третата страна може да обоснове забраната за предаване на данни дори когато е извършено на основание на стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК, и следователно показва, че те могат да са недостатъчни, за да се осигури подходяща защита. При това положение запитващата юрисдикция иска да се установи обхватът на правомощието на комисаря да забрани предаване на данни въз основа на тези клаузи, като същевременно счита, че правото на преценка не е достатъчно, за да се гарантира адекватна защита.

68 При тези условия High Court (Висш съд) решава да спре производството и да постави на Съда следните преюдициални въпроси:

„1) В случай че от частно дружество от държава членка на [Съюза] се предават лични данни към частно дружество в трета държава за търговски цели съгласно [решение СК] и тези данни могат да се обработват допълнително в третата държава от нейните органи за цели, свързани с националната сигурност, но също така и за целите на поддържането на обществения ред и провеждането на външната политика на третата държава, прилага ли се правото на Съюза (включително Хартата) по отношение на предаването на данните, независимо от разпоредбите на член 4, параграф 2 ДЕС във връзка с националната сигурност и разпоредбите на член 3, параграф 2, първо тире от Директива [95/46] във връзка с обществената сигурност, отбраната и държавната сигурност?

2) а) За да се определи дали е извършено нарушение на правата на дадено физическо лице чрез предаването на данни от [Съюза] към трета държава съгласно Решение [СК], когато данните могат да се обработват допълнително за цели, свързани с националната сигурност, кой е релевантният критерий за сравнение за целите на Директива [95/46]:

i) Хартата, Договора за ЕС, Договора за функционирането на ЕС, Директива [95/46], [Европейската конвенция за защита на правата на човека и основните свободи, подписана в Рим на 4 ноември 1950 г.,] (или друга разпоредба на правото на Съюза); или

ii) законодателството на една или повече държави членки?

б) Ако релевантният критерий за сравнение е посоченият в [подточка ii)], следва ли практиките в контекста на националната сигурност в една или повече държави членки също да бъдат включени в критерия за сравнение?

3) Когато се преценява дали дадена трета държава осигурява изискваната от правото на Съюза степен на защита на предадените към тази държава лични данни за целите на член 26 от Директива [95/46], следва ли степента на защита в третата държава да се оценява с оглед на:

а) приложимите правила в третата държава, произтичащи от вътрешно ѝ законодателство или от сключените от нея международни споразумения, както и практиката по осигуряване на спазването на тези правила, включително професионалните правила и мерките за сигурност, които се спазват в тази трета държава;

или

б) правилата, посочени в буква а), заедно с всички административни, регулаторни практики и практики за осигуряване на съответствие, политически гаранции, процедури, протоколи, надзорни механизми и извънсъдебни средства за защита, които съществуват в третата държава?

4) Предвид обстоятелствата, установени от High Court [(Висш съд)] във връзка с правото на Съединените щати, ако личните данни се предават от [Съюза] към Съединените щати съгласно решението [СК], това нарушава ли правата на физическите лица по член 7 и/или член 8 от Хартата?

5) Предвид обстоятелствата, установени от High Court [(Висш съд)] във връзка с правото на Съединените щати, ако се предават лични данни от [Съюза] към Съединените щати съгласно решението [СК]:

а) Степента на защита, предоставена от Съединените щати, зачита ли основното съдържание на гарантираното с член 47 от Хартата право на физическите лица на правни средства за защита пред съд в случай на нарушение на техните права във връзка със защита на личните им данни?

При утвърдителен отговор на пети въпрос, буква а):

б) Дали ограниченията, наложени от законодателството на Съединените щати спрямо правото на физическите лица на правни средства за защита пред съд в контекста на националната сигурност на Съединените щати, са пропорционални по смисъла на член 52 от Хартата и не надхвърлят рамките на необходимото в едно демократично общество за цели, свързани с националната сигурност?

6) а) Каква е степента на защита, която следва да се осигури по отношение на личните данни, които се предават на трета държава съгласно стандартни договорни клаузи, приети в съответствие с решение на Комисията съгласно член 26, параграф 4 от Директива [95/46], в светлината на разпоредбите [на тази директива], и по-специално членове 25 и 26, разглеждани във връзка с Хартата?

б) Кои са въпросите, които трябва да бъдат взети предвид, когато се преценява дали степента на защита на данните, прехвърлени към трета държава съгласно решението [СК], отговаря на изискванията на Директива [95/46] и на Хартата?

7) От обстоятелството, че стандартните клаузи за защита се прилагат само между износителя и вносителя на данни и не обвързват националните органи на трета държава, които могат да изискват от вносителя на данни да предоставя на службите за сигурност за

допълнителна обработка личните данни, предавани съгласно предвидените в решението [СК] клаузи, следва ли, че тези клаузи не предоставят достатъчно гаранции, както се изисква от член 26, параграф 2 от Директива [95/46]?

8) Ако вносител на данни от трета държава е обект на надзорни норми, които според орган за защита на данните са в противоречие със стандартните клаузи за защита или с членове 25 и 26 от Директива [95/46] и/или с Хартата, длъжен ли е органът за защита на данните да използва своите изпълнителни правомощия съгласно член 28, параграф 3 от Директива [95/46], за да спре потока от данни, или упражняването на тези правомощия е ограничено единствено до изключителни случаи в светлината на съображение 11 от решението [СК], или органът за защита на данните може да използва правото си на преценка, за да не спира потока от данни?

9) а) За целите на член 25, параграф 6 от Директива [95/46] представлява ли решение [ЩЛД] задължителна за органите за защита на данните и съдилищата на държавите членки констатация от общ характер, че Съединените щати осигуряват достатъчна степен на защита по смисъла на член 25, параграф 2 от Директива [95/46] по силата на вътрешното си законодателство или на международните споразумения, по които са страна?
   б) Ако това не е така, какво значение има решението [ЩЛД], ако изобщо има някакво значение, когато се преценява дали гаранциите, осигурени по отношение на данни, предавани в Съединените щати в съответствие с решението [СК], са достатъчни?

10) Предвид обстоятелствата, установени от High Court [(Висш съд)] във връзка с правото на Съединените щати, дали създаването на омбудсмана към Щита за личните данни съгласно приложение A към приложение III към решението [ЩЛД], разгледано във връзка със съществуващия в Съединените щати режим, гарантира, че Съединените щати осигуряват правни средства за защита на заинтересованите физически лица, чиито лични данни се предават към Съединените щати съгласно решението [СК], които са съвместими с член 47 от Хартата?

11) Решение [СК] нарушава ли членове 7, 8 и/или 47 от Хартата?“.

По допустимостта на преюдициалното запитване

69 Facebook Ireland, германското правителство и правителството на Обединеното кралство твърдят, че преюдициалното запитване е недопустимо.

70 Що се отнася до повдигнатото от Facebook Ireland възражение, това дружество отбелязва, че разпоредбите на Директива 95/46, на които се основават преюдициалните въпроси, са отменени от ОРЗД.

71 В това отношение, макар да е вярно, че по силата на член 94, параграф 1 от ОРЗД Директива 95/46 е отменена, считано от 25 май 2018 г., тази директива още е била в сила при формулирането на 4 май 2018 г. на настоящото преюдициално запитване, постъпило в Съда на 9 май 2018 г. Освен това член 3, параграф 2, първо тире, членове 25 и 26, както и член 28, параграф 3 от Директива 95/46, които са посочени в преюдициалните въпроси, по същество са възпроизведени съответно в член 2, параграф 2, както и в членове 45, 46 и 58 от ОРЗД. Впрочем следва да се припомни, че задача на Съда е да тълкува всички разпоредби от правото на Съюза, които са необходими на националните юрисдикции, за да се произнасят по споровете, с които са сезирани, дори тези разпоредби да не са изрично посочени във въпросите, отправени от тези юрисдикции до Съда (решение от 2 април 2020 г., Ruska Federacija, C-897/19 PPU, EU:C:2020:262, т. 43 и цитираната съдебна практика). Поради тези

различни съображения обстоятелството, че запитващата юрисдикция е формулирала преюдициалните въпроси, като се е позовала единствено на разпоредбите на Директива 95/46, не може да доведе до недопустимост на настоящото преюдициално запитване.

72 От своя страна германското правителство основава възражението си за недопустимост на обстоятелството, от една страна, че комисарят е изразил само съмнения, а не окончателно становище по въпроса за валидността на решението СК и от друга страна, че запитващата юрисдикция не е проверила дали г-н Schrems несъмнено е дал съгласието си за разглежданото в главното производство предаване на данни, което, ако беше така, би обезсмислило отговора на този въпрос. Накрая, според правителството на Обединеното кралство преюдициалните въпроси имат хипотетичен характер, тъй като тази юрисдикция не е установила, че тези данни действително са били предадени на основание на посоченото решение.

73 Видно от постоянната съдебна практика, само националният съд, който е сезиран със спора и трябва да поеме отговорността за последващото му съдебно решаване, може да прецени — предвид особеностите на делото — както необходимостта от преюдициално решение, за да може да се произнесе, така и релевантността на въпросите, които поставя на Съда. Следователно, след като тези въпроси се отнасят до тълкуването или валидността на норма от правото на Съюза, Съдът по принцип е длъжен да се произнесе. Оттук следва, че поставените от националните юрисдикции въпроси се ползват с презумпция за релевантност. Съдът може да откаже да се произнесе по отправеното от национална юрисдикция преюдициално запитване само ако е видно, че исканото тълкуване няма никаква връзка с действителността или с предмета на спора в главното производство, ако проблемът е от хипотетично естество или още ако Съдът не разполага с необходимите данни от фактическа и правна страна, за да бъде полезен с отговора на посочените въпроси (решения от 16 юни 2015 г., Gauweiler и др., C-62/14, EU:C:2015:400, т. 24 и 25, от 2 октомври 2018 г., Ministerio Fiscal, C-207/16, EU:C:2018:788, т. 45 и от 19 декември 2019 г., Dobersberger, C-16/18, EU:C:2019:1110, т. 18 и 19).

74 В случая преюдициалното запитване съдържа достатъчно данни от фактическа и правна страна, за да се разбере обхватът на преюдициалните въпроси. Освен това и преди всичко нищо в преписката, с която разполага Съдът, не позволява да се приеме, че исканото тълкуване на правото на Съюза няма връзка с действителността или с предмета на спора в главното производство или е от хипотетично естество, по-специално поради факта че разглежданото в главното производство предаване на лични данни се основава на изричното съгласие на съответното физическо лице за това предаване, а не на решението СК. Всъщност съгласно съдържащата се в това запитване информация Facebook Ireland признава, че предава на Facebook Inc. личните данни на своите пребиваващи в Съюза абонати и че голяма част от това предаване, чиято законосъобразност г-н Schrems оспорва, се извършва въз основа на стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК.

75 Освен това за допустимостта на настоящото преюдициално запитване е без значение обстоятелството, че комисарят не е изразил окончателно становище относно валидността на това решение, щом запитващата юрисдикция счита, че отговорът на преюдициалните въпроси относно тълкуването и валидността на норми от правото на Съюза е необходим за разрешаването на спора в главното производство.

76 Следователно преюдициалното запитване е допустимо.

По преюдициалните въпроси

77 В самото начало следва да се припомни, че настоящото преюдициално запитване е отправено във връзка с жалба на г-н Schrems, с която се цели комисарят да разпореди спирането или забраната за в бъдеще на предаването на личните му данни от Facebook Ireland на Facebook Inc.

Макар преюдициалните въпроси да се отнасят до разпоредбите на Директива 95/46, все пак е безспорно, че комисарят още не е приел окончателно решение по тази жалба, когато посочената директива е отменена и заменена с ОРЗД, считано от 25 май 2018 г.

78 Тази липса на национално решение разграничава разглеждания в главното производство случай от делата, по които са постановени решения от 24 септември 2019 г., Google (Териториален обхват на премахването от резултатите при търсене) (C-507/17, EU:C:2019:772) и от 1 октомври 2019 г., Planet49 (C-673/17, EU:C:2019:801), в които се оспорват решения, приети преди отмяната на посочената директива.

79 При това положение на преюдициалните въпроси следва да се отговори с оглед на разпоредбите на ОРЗД, а не на разпоредбите на Директива 95/46.

По първия въпрос

80 С първия си въпрос запитващата юрисдикция по същество иска да се установи дали член 2, параграф 1 и член 2, параграф 2, букви а), б) и г) от ОРЗД, разглеждани във връзка с член 4, параграф 2 ДЕС, трябва да се тълкуват в смисъл, че предаване на лични данни от икономически оператор, установен в държава членка, към друг икономически оператор, установен в трета държава, попада в приложното поле на този регламент, когато по време на предаването или след него тези данни могат да се обработват от органите на тази трета държава за целите на обществената сигурност, отбраната и държавната сигурност.

81 В това отношение в самото начало следва да се отбележи, че разпоредбата на член 4, параграф 2 ДЕС, съгласно която в Съюза националната сигурност остава единствено в рамките на отговорността на всяка държава членка, се отнася изключително до държавите — членки на Съюза. Следователно в случая тази разпоредба не е релевантна за тълкуването на член 2, параграф 1 и член 2, параграф 2, букви а), б) и г) от ОРЗД.

82 Съгласно член 2, параграф 1 от ОРЗД този регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни. Член 4, точка 2 от този регламент определя понятието „обработване“ като „всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства“ и посочва като примери „разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни“, без да прави разграничение дали тези операции се извършват в рамките на Съюза, или са свързани с трета държава. Освен това посоченият регламент обвързва предаването на лични данни на трети държави със специални правила, съдържащи се в глава V от него, озаглавена „Предаване на лични данни на трети държави или международни организации“, и дори предоставя на надзорните органи специални правомощия за тази цел, съдържащи се в член 58, параграф 2, буква й) от същия регламент.

83 Затова операцията по предаване на лични данни от държава членка към трета държава сама по себе си представлява обработване на лични данни по смисъла на член 4, точка 2 от ОРЗД, извършвано на територията на държава членка, обработване, за което този регламент се прилага по силата на член 2, параграф 1 от ОРЗД (вж. по аналогия, що се отнася до член 2, буква б) и член 3, параграф 1 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 45 и цитираната съдебна практика).

84 Относно въпроса дали такава операция може да се счита за изключена от приложното поле на ОРЗД по силата на член 2, параграф 2 от него, следва да се припомни, че тази разпоредба предвижда изключения от приложното поле на регламента, както е определено в член 2,

параграф 1 от него, и че тези изключения трябва да се тълкуват стриктно (вж. по аналогия, що се отнася до член 3, параграф 2 от Директива 95/46, решение от 10 юли 2018 г., Jehovan todistajat, C-25/17, EU:C:2018:551, т. 37 и цитираната съдебна практика).

85 В случая, тъй като разглежданото в главното производство предаване на лични данни се извършва от Facebook Ireland към Facebook Inc., а именно между две юридически лица, това предаване не попада в обхвата на член 2, параграф 2, буква в) от ОРЗД, който се отнася до обработването на данни, извършвано от физическо лице в хода на чисто лични или домашни занимания. Посоченото предаване не попада и в обхвата на изключенията, съдържащи се в член 2, параграф 2, букви а), б) и г) от този регламент, тъй като дейностите, посочени като пример там, във всички случаи са присъщи на държавите или на държавните органи дейности, които са извън областите на дейност на частноправните субекти (вж. по аналогия, що се отнася до член 3, параграф 2 от Директива 95/46, решение от 10 юли 2018 г., Jehovan todistajat, C-25/17, EU:C:2018:551, т. 38 и цитираната съдебна практика).

86 Впрочем възможността личните данни, предавани между двама икономически оператори за търговски цели, да претърпят по време на предаването или след него обработване за целите на обществената сигурност, отбраната и държавната сигурност от органите на съответната трета държава, не може да изключи посоченото предаване от приложното поле на ОРЗД.

87 Като предвижда изрично задължение за Комисията, когато оценява адекватността на нивото на защита от дадена трета държава, да отчита по-специално „съответното законодателство — както общо, така и секторно, включително в областта на обществената сигурност, отбраната, националната сигурност и наказателното право и достъпа на публичните органи до лични данни, а също и прилагането на такова законодателство“, самият текст на член 45, параграф 2, буква а) от този регламент всъщност подчертава обстоятелството, че евентуалното обработване от трета държава на съответните данни за целите на обществената сигурност, отбраната и държавната сигурност не поставя под въпрос приложимостта на посочения регламент към съответното предаване.

88 Следователно подобно прехвърляне не може да остане извън приложното поле на ОРЗД, с мотива че разглежданите данни могат да се обработват по време на това предаване или след него от органите на съответната трета държава за целите на обществената сигурност, отбраната и държавната сигурност.

89 Ето защо на първия въпрос следва да се отговори, че член 2, параграфи 1 и 2 от ОРЗД трябва да се тълкува в смисъл, че предаване на лични данни за търговски цели от икономически оператор, установен в държава членка, към друг икономически оператор, установен в трета държава, попада в приложното поле на този регламент, независимо че по време на предаването или след него тези данни могат да се обработват от органите на съответната трета държава за целите на обществената сигурност, отбраната и държавната сигурност.

По втория, третия и шестия въпрос

90 С втория, третия и шестия си въпрос запитващата юрисдикция по същество иска от Съда да установи изискването от член 46, параграф 1 и член 46, параграф 2, буква в) от ОРЗД ниво на защита в рамките на предаване на лични данни на трета държава, основаващо се на стандартни клаузи за защита на данните. По-специално тази юрисдикция иска от Съда да уточни елементите, които следва да се вземат предвид, за да се определи дали това ниво на защита е осигурено в контекста на такова предаване.

91 Що се отнася до изискваното ниво на защита, от съвместния прочит на тези разпоредби следва, че при липсата на решение относно адекватното ниво на защита, прието съгласно член 45, параграф 3 от този регламент, администраторът или обработващият лични данни може да предава лични данни на трета държава само ако е предвидил „подходящи гаранции“ и при условие че са налице „приложими права на субектите на данни и ефективни правни средства за защита“, като тези подходящи гаранции могат да се предвидят по-специално посредством стандартни клаузи за защита на данните, приети от Комисията.

92 Макар член 46 от ОРЗД да не уточнява естеството на изискванията, които произтичат от това посочване на „подходящи гаранции“, „приложими права“ и „ефективни правни средства за защита“, следва да се отбележи, че този член се съдържа в глава V от този регламент и следователно трябва да се тълкува в светлината на член 44 от посочения регламент, озаглавен „Общ принцип на предаването на данни“, който гласи, че „[в]сички разпоредби на [посочената глава] се прилагат, за да се направи необходимото нивото на защита на физическите лица, осигурено от [същия] регламент, да не се излага на риск“. Следователно това ниво на защита трябва да се гарантира без значение коя е разпоредбата на посочената глава, въз основа на която се извършва предаване на лични данни на трета държава.

93 Всъщност, както отбелязва генералният адвокат в точка 117 от заключението си, разпоредбите на глава V от ОРЗД имат за цел да осигурят непрекъснатостта на високото ниво на тази защита при предаване на лични данни на трета държава, в съответствие с целта, посочена в съображение 6 от този регламент.

94 Член 45, параграф 1, първо изречение от ОРЗД предвижда, че предаване на лични данни на трета държава може да се разреши с прието от Комисията решение, съгласно което тази трета държава, територия или един или повече конкретни нейни сектори осигуряват адекватно ниво на защита. В това отношение, без да се изисква съответната трета държава да гарантира ниво на защита, което е идентично на гарантираното в правния ред на Съюза, изразът „адекватно ниво на защита“ трябва да се разбира, както потвърждава съображение 104 от този регламент, в смисъл, че от тази трета държава се изисква действително да гарантира, по силата на вътрешното си законодателство или на международните си ангажименти, ниво на защита на основните права и свободи, което по същество е равностойно на гарантираното в Съюза по силата на посочения регламент, разглеждан в светлината на Хартата. Всъщност, ако това изискване не е изпълнено, посочената в предходната точка цел би се оказала пренебрегната (вж. по аналогия, що се отнася до член 25, параграф 6 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 73).

95 В този контекст съображение 107 от ОРЗД посочва, че когато „дадена трета държава, територия или конкретен сектор в трета държава […] вече не осигурява адекватно ниво на защита на данните […], предаването на лични данни на тази трета държава […] следва да бъде забранено, докато не бъдат изпълнени изискванията по [този регламент] относно предаването на данни с подходящи гаранции […]“. В това отношение в съображение 108 от посочения регламент се уточнява, че при липсата на решение относно адекватното ниво на защита, подходящите гаранции, които администраторът или обработващият лични данни следва да предвиди в съответствие с член 46, параграф 1 от същия регламент, трябва „да компенсира[т] липсата на защита на данни в дадена трета държава“, за да „осигуряват спазването на изискванията относно защитата на данните и на правата на субектите на данни, подходящи при обработване в рамките на Съюза“.

96 От това следва, както отбелязва генералният адвокат в точка 115 от заключението си, че тези подходящи гаранции трябва да са от естество да гарантират, че лицата, чиито лични данни са предадени на трета държава въз основа на стандартни клаузи за защита на данните, се ползват, както при предаване, основано на решение относно адекватното ниво на защита, от ниво на защита, което по същество е равностойно на гарантираното в Съюза.

97 Запитващата юрисдикция иска да се установи и дали това по същество равностойно на гарантираното в рамките на Съюза ниво на защита трябва да се определи с оглед на правото на Съюза, по-специално на правата, гарантирани от Хартата, и/или с оглед на основните права, закрепени в Европейската конвенция за защита на правата на човека и основните свободи (наричана по-нататък „ЕКПЧ“), или пък на националното право на държавите членки.

98 В това отношение следва да се припомни, че макар закрепените в ЕКПЧ основни права да са част от правото на Съюза като общи принципи, както потвърждава член 6, параграф 3 ДЕС, и макар член 52, параграф 3 от Хартата да предвижда, че съдържащите се в тази харта права, съответстващи на права, гарантирани от ЕКПЧ, имат същия смисъл и обхват като дадените им в посочената конвенция, докато Съюзът не се присъедини към тази конвенция, тя не представлява юридически акт, формално интегриран в правния ред на Съюза (решения от 26 февруари 2013 г., Åkerberg Fransson, C-617/10, EU:C:2013:105, т. 44 и цитираната съдебна практика и от 20 март 2018 г., Menci, C-524/15, EU:C:2018:197, т. 22).

99 При тези обстоятелства Съдът приема, че правото на Съюза следва да се тълкува и валидността на актовете на Съюза следва да се разглежда в светлината на гарантираните от Хартата основни права (вж. по аналогия решение от 20 март 2018 г., Menci, C-524/15, EU:C:2018:197, т. 24).

100 Освен това от постоянната съдебна практика следва, че валидността на разпоредбите от правото на Съюза и при липса на изрично препращане към националното право на държавите членки, тяхното тълкуване, не могат да се преценяват в светлината на това национално право, дори с конституционен ранг, и по-специално на основните права, както са предвидени в националната им конституция (вж. в този смисъл решения от 17 декември 1970 г., Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, т. 3, от 13 декември 1979 г., Hauer, 44/79, EU:C:1979:290, т. 14 и от 18 октомври 2016 г., Nikiforidis, C-135/15, EU:C:2016:774, т. 28 и цитираната съдебна практика).

101 Ето защо щом, от една страна, предаване на лични данни като разглежданото в главното производство, извършено за търговски цели от икономически оператор, установен в държава членка, към друг икономически оператор, установен в трета държава, попада в приложното поле на ОРЗД, както следва от отговора на първия въпрос, и щом, от друга страна, този регламент има за цел по-специално, както личи от съображение 10 от него, да гарантира последователно и високо ниво на защита на физическите лица в Съюза и за целта да гарантира последователно и еднородно прилагане в рамките на Съюза на правилата за защита на основните права и свободи на тези лица във връзка с обработването на лични данни, изискването от член 46, параграф 1 от посочения регламент ниво на защита на основните права трябва да се определи въз основа на разпоредбите на същия регламент, разглеждани в светлината на основните права, гарантирани от Хартата.

102 Запитващата юрисдикция иска да се установи и какви елементи следва да се вземат предвид, за да се определи адекватното ниво на защита в контекста на предаване на лични данни на трета държава въз основа на стандартни клаузи за защита на данните, приети на основание член 46, параграф 2, буква в) от ОРЗД.

103 В това отношение, макар тази разпоредба да не изброява различните елементи, които следва да се вземат предвид, за да се прецени адекватното ниво на защита, което да се спазва при такова предаване, член 46, параграф 1 от този регламент уточнява, че субектите на данни трябва да се ползват от подходящи гаранции и да разполагат с приложими права и ефективни правни средства за защита.

104 При необходимата за тази цел оценка в контекста на такова предаване трябва по-специално да се вземат предвид както договорните клаузи между администратора или обработващия лични данни, установени в Съюза, и получателя на предаването, установен в съответната трета

държава, така и — що се отнася до евентуалния достъп на публичните органи на тази трета държава до прехвърлените лични данни — релевантните елементи на нейната правна система. В това отношение елементите, които следва да се вземат предвид в контекста на член 46 от посочения регламент, съответстват на тези, които са изброени неизчерпателно в член 45, параграф 2 от същия.

105 Затова на втория, третия и шестия въпрос следва да се отговори, че член 46, параграф 1 и член 46, параграф 2, буква в) от ОРЗД трябва да се тълкуват в смисъл, че изискваните от тези разпоредби подходящи гаранции, приложими права и ефективни правни средства за защита трябва да гарантират, че правата на лицата, чиито лични данни са предадени на трета държава въз основа на стандартни клаузи за защита на данните, се ползват с ниво на защита, което по същество е равностойно на гарантираното в Съюза с този регламент, разглеждан в светлината на Хартата. За тази цел при оценката на гарантираното в контекста на такова предаване ниво на защита трябва по-специално да се вземат предвид както договорните клаузи, уговорени между администратора или обработващия лични данни, установени в Съюза, и получателя на предаването, установен в съответната трета държава, така и, що се отнася до евентуалния достъп на публичните органи на тази трета държава до така предадените лични данни, релевантните елементи на нейната правна система, и по-специално посочените в член 45, параграф 2 от този регламент.

По осмия въпрос

106 С осмия си въпрос запитващата юрисдикция иска по същество да се установи дали член 58, параграф 2, букви е) и й) от ОРЗД трябва да се тълкува в смисъл, че компетентният надзорен орган е длъжен да спре или да забрани предаването на лични данни на трета държава, основаващо се на приети от Комисията стандартни клаузи за защита на данните, когато този надзорен орган счита, че тези клаузи не са или не могат да бъдат спазени в тази трета държава, и когато защитата на предаваните данни, изисквана от правото на Съюза, по-специално от членове 45 и 46 ОРЗД и от Хартата, не може да бъде осигурена, или в смисъл, че упражняването на тези правомощия е ограничено до изключителни случаи.

107 В съответствие с член 8, параграф 3 от Хартата, член 51, параграф 1 и член 57, параграф 1, буква а) от ОРЗД националните надзорни органи отговарят за контрола за спазването на нормите на Съюза относно защитата на физическите лица във връзка с обработването на лични данни. Затова всеки от тях разполага с правомощия да проверява дали дадено предаване на лични данни от държавата членка, към която спада съответният орган, на трета държава отговаря на въведените с този регламент изисквания (вж. по аналогия, що се отнася до член 28 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 47).

108 От тези разпоредби следва, че основната задача на надзорните органи е да наблюдават прилагането на ОРЗД и да следят за спазването му. Упражняването на тази задача е от особено значение в контекста на предаването на лични данни на трета държава, тъй като, както следва от самия текст на съображение 116 от този регламент, „[т]рансграничното движение на лични данни извън Съюза може да увеличи риска физическите лица да не могат да упражнят правата на защита на данните, по-специално да се защитят срещу неправомерна употреба или разкриване на тези данни“. В тази хипотеза, както се уточнява в същото съображение, „надзорните органи могат да бъдат изправени пред невъзможността да разглеждат жалби или да провеждат разследвания, свързани с дейности, извършвани извън техните граници“.

109 Освен това по силата на член 57, параграф 1, буква е) от ОРЗД всеки надзорен орган е длъжен на своята територия да разглежда жалбите, които всяко лице има право да подаде в съответствие с член 77, параграф 1 от този регламент, когато счита, че обработване на свързани с него лични данни представлява нарушение на посочения регламент, и да разглежда предмета

им, доколкото това е необходимо. Надзорният орган трябва да разгледа такава жалба с цялата дължима грижа (вж. по аналогия, що се отнася до член 25, параграф 6 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 63).

110 Член 78, параграфи 1 и 2 от ОРЗД признава на всяко лице правото на ефективна съдебна защита по-специално когато надзорният орган не разгледа неговата жалба. В съображение 141 от този регламент също се посочва това „право на ефективни правни средства за защита в съответствие с член 47 от Хартата“, когато този надзорен орган „не предприема действия, когато такива са необходими, за да се защитят правата на субекта на данни“.

111 За целите на обработването на подадените жалби член 58, параграф 1 от ОРЗД предоставя на всеки надзорен орган важни правомощия за разследване. Когато в края на разследването си такъв орган счита, че субектът на данните, чиито лични данни са били предадени на трета държава, не се ползва от адекватно ниво на защита, той е длъжен в съответствие с правото на Съюза да реагира по подходящ начин, за да отстрани констатирания недостатък, и то независимо от произхода или естеството на този недостатък. За тази цел член 58, параграф 2 от регламента изброява различните корективни правомощия, които има надзорният орган.

112 Въпреки че изборът на подходящото и необходимо средство е от компетентността на надзорния орган и той трябва да направи този избор предвид всички обстоятелства по съответното предаване на лични данни, този орган все пак трябва да изпълни с цялата дължима грижа своята задача да следи за пълното спазване на ОРЗД.

113 В това отношение и както отбелязва и генералният адвокат в точка 148 от заключението си, посоченият орган е длъжен по силата на член 58, параграф 2, букви е) и й) от този регламент да спре или да забрани предаването на лични данни на трета държава, когато с оглед на всички обстоятелства във връзка с това предаване счита, че стандартните клаузи за защита на данните не са или не могат да бъдат спазени в тази трета държава и че изискваната от правото на Съюза защита на предаваните данни не може да бъде осигурена с други средства, в случай че самият установен в Съюза администратор или обработващ лични данни не е спрял или прекратил предаването.

114 Съдържащото се в предходната точка тълкуване не се поставя под съмнение от доводите на комисаря, че член 4 от Решение 2010/87 в редакцията му преди влизането в сила на Решение за изпълнение 2016/2297, разглеждан във връзка със съображение 11 от това решение, ограничава до някои изключителни хипотези правомощието на надзорните органи да спрат или да забранят предаване на лични данни на трета държава. Всъщност в редакцията на член 4 от решението СК, произтичаща от Решение за изпълнение 2016/2297, се посочва правомощието, с което разполагат тези органи — понастоящем по силата на член 58, параграф 2, букви е) и й) от ОРЗД — да спират или да забраняват такова предаване, без изобщо да се ограничава упражняването на това правомощие до изключителни обстоятелства.

115 Във всеки случай изпълнителните правомощия, които член 46, параграф 2, буква в) ОРЗД признава на Комисията, за да приема стандартни клаузи за защита на данните, не ѝ дават право да ограничава правомощията, с които разполагат надзорните органи съгласно член 58, параграф 2 от този регламент (вж. по аналогия, що се отнася до член 25, параграф 6 и член 28 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 102 и 103). Впрочем съображение 5 от Решение за изпълнение 2016/2297 потвърждава, че решението СК „не възпрепятства даден [надзорен орган] да упражни своите правомощия за надзор върху потоците от данни, включително правомощието да спира или забранява предаването на лични данни, когато прецени, че то се извършва в нарушение на правото на ЕС или на националното право за защита на данните“.

116 Важно е обаче да се уточни, че правомощията на компетентния надзорен орган са обвързани с пълното спазване на решението, с което Комисията евентуално констатира съгласно член 45, параграф 1, първо изречение от ОРЗД, че определена трета държава осигурява адекватно ниво на защита. Всъщност в подобна хипотеза от член 45, параграф 1, второ изречение във връзка със съображение 103 от този регламент следва, че предаването на лични данни на съответната трета държава може да се осъществи, без да е необходимо получаването на специално разрешение.

117 По силата на член 288, четвърта алинея ДФЕС решението на Комисията относно адекватното ниво на защита е обвързващо в своята цялост за всички държави членки адресати и следователно е задължително за всичките им органи, доколкото с него се установява, че съответната трета държава гарантира адекватно ниво на защита и се разрешава това предаване на данни (вж. по аналогия, що се отнася до член 25, параграф 6 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 51 и цитираната съдебна практика).

118 Така, докато решението относно адекватното ниво на защита не бъде обявено за невалидно от Съда, държавите членки и техните органи, включително независимите им надзорни органи, не могат да приемат мерки, които противоречат на въпросното решение, като например да приемат актове със задължителна сила, с които се цели да се констатира, че посочената в решението трета държава не гарантира адекватно ниво на защита (решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 52 и цитираната съдебна практика), и вследствие на това да спират или да забраняват предаването на лични данни на тази трета държава.

119 Същевременно решение на Комисията относно адекватното ниво на защита, прието въз основа на член 45, параграф 3 от ОРЗД, не може да възпрепятства лицата, чиито лични данни са били или биха могли да бъдат предадени на трета държава, да сезират съгласно член 77, параграф 1 от ОРЗД компетентния национален надзорен орган с жалба за защита на техните права и свободи при обработването на тези данни. Освен това решение от такова естество не може нито да отнеме, нито дори да намали правомощията, които изрично са признати на националните надзорни органи с член 8, параграф 3 от Хартата и с член 51, параграф 1 и член 57, параграф 1, буква а) от посочения регламент (вж. по аналогия, що се отнася до член 25, параграф 6 и член 28 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 53).

120 Така, дори при наличие на решение на Комисията относно адекватното ниво на защита компетентният национален надзорен орган, сезиран от лице с жалба за защитата на неговите права и свободи при обработването на свързаните с него лични данни, трябва да може да провери напълно независимо дали предаването на тези данни отговаря на въведените с ОРЗД изисквания, и ако е необходимо, да подаде жалба пред националните юрисдикции, така че ако последните споделят съмненията на този орган относно валидността на решението относно адекватното ниво на защита, да отправят преюдициално запитване с цел проверка на тази валидност (вж. по аналогия, що се отнася до член 25, параграф 6 и член 28 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 57 и 65).

121 С оглед на гореизложените съображения на осмия въпрос следва да се отговори, че член 58, параграф 2, букви е) и й) от ОРЗД трябва да се тълкува в смисъл, че освен ако съществува надлежно прието от Комисията решение относно адекватното ниво на защита, компетентният надзорен орган е длъжен да спре или да забрани предаването на данни на трета държава, основаващо се на приети от Комисията стандартни клаузи за защита на данните, когато с оглед на всички обстоятелства във връзка с това предаване надзорният орган счита, че тези клаузи не са или не могат да бъдат спазени в тази трета държава и че защитата на предаваните данни, изисквана от правото на Съюза, по-специално от членове 45 и 46 от ОРЗД и от Хартата, не може да бъде осигурена с други средства, в случай че самият установен в Съюза администратор или обработващ лични данни не е спрял или прекратил предаването.

По седмия и единадесетия въпрос

122 Със седмия и единадесетия въпрос, които следва да се разгледат заедно, запитващата юрисдикция по същество иска от Съда да установи валидността на решението СК с оглед на членове 7, 8 и 47 от Хартата.

123 По-специално, както следва от самия текст на седми въпрос и от разясненията във връзка с него, съдържащи се в акта за преюдициално запитване, запитващата юрисдикция иска да се установи дали решението СК може да гарантира адекватна защита на предадените на трети държави лични данни, доколкото предвидените в него стандартни клаузи за защита на данните не обвързват органите на тези трети държави.

124 Член 1 от решението СК предвижда, че съдържащите се в приложението към него стандартни клаузи за защита на данните предоставят подходящи гаранции за защитата на личния живот и основните права и свободи на физическите лица в съответствие с изискванията на член 26, параграф 2 от Директива 95/46. Последната разпоредба по същество е възпроизведена в член 46, параграф 1 и в член 46, параграф 2, буква в) от ОРЗД.

125 Все пак, макар тези клаузи да са обвързващи за установения в Съюза администратор и за установения в трета държава получател на лични данни, в случай че са сключили договор с оглед на тези клаузи, безспорно е, че посочените клаузи не могат да обвържат органите на тази трета държава, тъй като последните не са страни по договора.

126 Макар следователно да съществуват случаи, при които в зависимост от действащото право и практики в съответната трета държава получателят на такова предаване е в състояние да гарантира необходимата защита на данните само въз основа на стандартните клаузи за защита на данните, съществуват и други случаи, при които съдържащата се в тези клаузи уредба може да не представлява достатъчно средство, позволяващо на практика да се осигури ефективна защита на предадените в съответната трета държава лични данни. Такъв е случаят по-специално когато правото на тази трета държава позволява на нейните публични органи намеса в правата на субектите на данни във връзка с тези данни.

127 Така се поставя въпросът дали решение на Комисията относно стандартни клаузи за защита на данните, прието на основание член 46, параграф 2, буква в) от ОРЗД, е невалидно, ако в него липсват гаранции, приложими спрямо публичните органи на трети държави, на които са или могат да бъдат предадени лични данни въз основа на тези клаузи.

128 Член 46, параграф 1 от ОРЗД предвижда, че при липса на решение относно адекватното ниво на защита администраторът или обработващият лични данни може да предава лични данни на трета държава само ако е предвидил подходящи гаранции и при условие че са налице приложими права на субектите на данни и ефективни правни средства за защита. Съгласно член 46, параграф 2, буква в) от регламента тези гаранции могат да бъдат предвидени посредством стандартни клаузи за защита на данните, приети от Комисията. Тези разпоредби обаче не предвиждат, че съвкупността от посочените гаранции трябва непременно да бъде предвидена с решение на Комисията, каквото е решението СК.

129 В това отношение е важно да се отбележи, че подобно решение се различава от решение относно адекватното ниво на защита, прието на основание член 45, параграф 3 от ОРЗД, с което се цели след проверка на правната уредба на съответната трета държава, отчитаща по-специално релевантното законодателство в областта на националната сигурност и достъпа на публичните органи до личните данни, да се констатира със задължителна сила, че трета държава, територия или един или повече конкретни сектори в тази трета държава осигурява адекватно ниво на защита и че следователно достъпът на публичните органи на тази трета държава до такива данни не пречи на предаването им на същата трета държава. Поради това Комисията може да

приеме такова решение относно адекватното ниво на защита само при условие че е констатирала, че релевантното законодателство на третата държава в тази област действително съдържа всички необходими гаранции, които позволяват да се приеме, че тя гарантира адекватно ниво на защита.

130 Напротив, що се отнася до решение на Комисията, с което се приемат стандартни клаузи за защита на данните, каквото е решението СК, доколкото такова решение не се отнася до трета държава, територия или един или повече конкретни сектори в тази държава, от член 46, параграф 1 и от член 46, параграф 2, буква в) от ОРЗД не може да се направи извод, че преди да приеме такова решение, Комисията е длъжна да извърши оценка на адекватността на нивото на защита, гарантирано в третите държави, на които биха могли да бъдат предадени лични данни въз основа на такива клаузи.

131 В това отношение следва да се припомни, че съгласно член 46, параграф 1 от този регламент при липса на решение на Комисията относно адекватното ниво на защита установеният в Съюза администратор или обработващ лични данни трябва да предвиди по-специално подходящи гаранции. Съображения 108 и 114 от посочения регламент потвърждават, че когато Комисията не е взела решение относно адекватното ниво на защита на данните в трета държава, администраторът или евентуално обработващият лични данни „следва да предприеме мерки, за да компенсира липсата на защита на данни в дадена третата държава чрез подходящи гаранции за субекта на данните“, и че „[т]ези гаранции следва да осигуряват спазването на изискванията относно защитата на данните и на правата на субектите на данни, подходящи при обработване в рамките на Съюза, включително наличието на приложими права на субектите на данни и на ефективни средства за правна защита [...] в Съюза или в трета държава“.

132 След като, както следва от точка 125 от настоящото съдебно решение, поради присъщия си договорен характер стандартните клаузи за защита на данните не могат да обвържат публичните органи на трети държави, а член 44, член 46, параграф 1 и член 46, параграф 2, буква в) от ОРЗД, тълкувани в светлината на членове 7, 8 и 47 от Хартата, изискват гарантираното с този регламент ниво на защита на физическите лица да не бъде нарушено, може да се окаже необходимо да се допълнят гаранциите, съдържащи се в тези стандартни клаузи за защита на данните. В това отношение в съображение 109 от този регламент се посочва, че „[в]ъзможността администраторът [...] да използва стандартни клаузи за защита на данните, приети от Комисията [...], не следва да възпрепятства администраторите [...] да добавят други клаузи или допълнителни гаранции“ и по-специално се уточнява, че тези лица „следва да бъдат насърчавани да предоставят допълнителни гаранции [...], които допълват стандартните клаузи за защита [на данните]“.

133 Така става ясно, че целта на приетите от Комисията на основание член 46, параграф 2, буква в) от същия регламент стандартни клаузи за защита на данните е единствено да предоставят на установените в Съюза администратори или обработващи лични данни договорни гаранции, които се прилагат еднакво във всички трети държави и следователно независимо от гарантираното във всяка от тях ниво на защита. Доколкото с оглед на естеството си тези стандартни клаузи за защита на данните не могат да предоставят гаранции извън договорното задължение за спазване на изискваното от правото на Съюза ниво на защита, те могат да изискват, в зависимост от съществуващото положение в една или друга трета държава, приемането на допълнителни мерки от администратора, за да се осигури спазването на това ниво на защита.

134 В това отношение, както отбелязва генералният адвокат в точка 126 от заключението си, предвиденият в член 46, параграф 2, буква в) от ОРЗД договорен механизъм се основава на овластяването на администратора или на обработващия лични данни, установени в Съюза, както и, при условията на евентуалност, на компетентния надзорен орган. Следователно този администратор или обработващият лични данни трябва преди всичко да провери поотделно и

евентуално в сътрудничество с получателя на предаването дали правото на третата държава на местоназначение осигурява подходяща от гледна точка на правото на Съюза защита на личните данни, предадени въз основа на стандартни клаузи за защита на данните, като при необходимост предостави допълнителни спрямо предоставените от тези клаузи гаранции.

135 Ако администраторът или обработващият лични данни, установени в Съюза, не могат да предприемат достатъчни допълнителни мерки, за да гарантират такава защита, те или, при условията на евентуалност, компетентният надзорен орган са длъжни да спрат или да прекратят предаването на лични данни на съответната трета държава. Такъв по-специално е случаят, когато правото на тази трета държава налага на получателя на лични данни от Съюза задължения, които противоречат на посочените клаузи и следователно могат да поставят под въпрос договорната гаранция за адекватно ниво на защита срещу достъпа на публичните органи на посочената трета държава до тези данни.

136 Следователно самият факт, че стандартни клаузи за защита на данните, съдържащи се в решение на Комисията, прието съгласно член 46, параграф 2, буква в) от ОРЗД, като съдържащите се в приложението към решението СК, не обвързват органите на третите държави, на които могат да се предават лични данни, не засяга валидността на това решение.

137 Тази валидност обаче зависи от това дали в съответствие с изискването, произтичащо от член 46, параграф 1 и от член 46, параграф 2, буква в) от ОРЗД, тълкувани в светлината на членове 7, 8 и 47 от Хартата, подобно решение съдържа ефективни механизми, позволяващи на практика да се осигури спазването на изискваното от правото на Съюза ниво на защита и предаването на лични данни, основаващо се на такива клаузи, да бъде спряно или забранено в случай на нарушение на тези клаузи или при невъзможност за спазването им.

138 Що се отнася до гаранциите, съдържащи се в стандартните клаузи за защита на данните, включени в приложението към решението СК, видно от клауза 4, букви а) и б), клауза 5, буква а), клауза 9, както и от клауза 11, параграф 1 от това решение администраторът, установен в Съюза, получателят на лични данни и евентуално обработващият такива данни взаимно се ангажират, че обработването на тези данни, включително предаването им, е било извършено и ще продължи да се извършва в съответствие с „приложимото право за защита на данните“, а именно съгласно определението, съдържащо се в член 3, буква е) от посоченото решение, „законодателството, защитаващо основните права и свободи на лицата, и по-специално правото на личен живот при обработването на лични данни, приложимо към администратор на данни в държавата членка, в която е установен износителят на данни“. Впрочем разпоредбите на ОРЗД, разглеждани в светлината на Хартата, са част от това законодателство.

139 Освен това по силата на тази клауза 5, буква а) получателят на лични данни, установен в трета държава, се ангажира да информира своевременно установения в Съюза администратор за евентуалната си невъзможност да изпълни своите задължения по сключения договор. По-специално съгласно посочената клауза 5, буква б) този получател удостоверява, че няма причини да се смята, че приложимото за него законодателство го възпрепятства да изпълнява задълженията си по сключения договор и се ангажира да уведоми своевременно администратора за всяка промяна, щом узнае за нея, в отнасящото се до него национално законодателство, която може да има съществени неблагоприятни последици върху гаранциите и задълженията, предвидени от стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК. Освен това, макар същата клауза 5, буква г), подточка i) да позволява на получателя на лични данни в случай на законодателство, което му налага забрана, като например наказателноправна забрана за разкриване на информация с цел запазване на тайната на разследване от страна на правоприлагащ орган, да не съобщава на установения в Съюза администратор правнообвързващо искане за разкриване на личните данни от

правоприлагащ орган, той все пак е длъжен в съответствие с клауза 5, буква а) от приложението към решението СК да информира администратора за невъзможността си да осигури съответствие със стандартните клаузи за защита на данните.

140 И в двете предвидени от тази клауза 5, букви а) и б) хипотези на установения в Съюза администратор се предоставя правото да спре предаването на данни и/или да прекрати договора. С оглед на изискванията, произтичащи от член 46, параграф 1 и параграф 2, буква в) от ОРЗД, разглеждани в светлината на членове 7 и 8 от Хартата, спирането на предаването на данни и/или прекратяването на договора са задължителни за администратора, когато получателят на предаването не е или вече не е в състояние да спазва стандартните клаузи за защита на данните. Ако не направи това, администраторът ще наруши задълженията си по клауза 4, буква а) от приложението към решението СК, тълкувана в светлината на разпоредбите на ОРЗД и на Хартата.

141 Така изглежда, че клауза 4, буква а) и клауза 5, букви а) и б) от същото приложение задължават администратора, установен в Съюза, и получателят на лични данни да се уверят, че законодателството на третата държава на местоназначение позволява на посочения получател да се съобрази със стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК, преди предаването на личните данни на тази трета държава. Що се отнася до тази проверка, в бележка под линия относно посочената клауза 5 се уточнява, че императивните изисквания на това законодателство, които не се простират извън необходимото в едно демократично общество за гарантиране по-специално на националната сигурност, отбраната и обществената сигурност, не са в противоречие с тези стандартни клаузи за защита на данните. Обратно, както подчертава генералният адвокат в точка 131 от заключението си, изпълнението на задължение, диктувано от правото на третата държава на местоназначение, което надхвърля необходимото за постигането на тези цели, трябва да се счита за нарушение на посочените клаузи. Преценката от страна на тези оператори на необходимостта на подобно задължение трябва евентуално да отчита констатацията за осигуряваното от съответната трета държава адекватно ниво на защита на данните, съдържаща се в решение на Комисията относно адекватното ниво на защита, прието съгласно член 45, параграф 3 от ОРЗД.

142 От това следва, че администраторът, установен в Съюза, и получателят на лични данни са длъжни предварително да проверят спазването в съответната трета държава на изискваното от правото на Съюза ниво на защита. Получателят на тези данни е длъжен при необходимост, по силата на същата клауза 5, буква б), да информира администратора за евентуалната си невъзможност да осигури съответствие с тези клаузи, като тогава последният може да спре предаването на данни и/или да прекрати договора.

143 Ако получателят на предадени на трета страна лични данни е уведомил администратора на основание клауза 5, буква б) от приложението към решението СК, че законодателството на съответната трета държава не му позволява да осигури съответствие със стандартните клаузи за защита на данните, съдържащи се в това приложение, видно от клауза 12 от същото приложение, данните, които вече са били предадени на тази трета държава, и направените копия трябва да бъдат изцяло върнати или унищожени. При всички положения клауза 6 от същото приложение санкционира неспазването на тези стандартни клаузи, като предоставя на заинтересованото физическо лице правото да получи обезщетение за претърпяната вреда.

144 Следва да се добави, че съгласно клауза 4, буква е) от приложението към решението СК, когато специални категории от данни могат да бъдат предадени на трета страна, която не осигурява достатъчна степен на защита, администраторът, установен в Съюза, се задължава да информира за това заинтересованото физическо лице преди или непосредствено след предаването. Тази информация може да даде възможност на посоченото лице да упражни признатото му от клауза 3, параграф 1 от това приложение право на правни средства за защита срещу

администратора, за да може последният да спре планираното предаване, да прекрати договора, сключен с получателя на лични данни, или евентуално да иска от последния да върне или унищожи предадените данни.

145 Накрая, по силата на клауза 4, буква ж) от посоченото приложение администраторът, установен в Съюза, е длъжен — когато съгласно клауза 5, буква б) от приложението получателят на лични данни го уведоми, че в приложимото за него законодателство има промяна, която може да има съществени неблагоприятни последици върху предложените гаранции и задълженията, наложени от стандартните клаузи за защита на данните — да предаде това уведомление на компетентния надзорен орган, ако въпреки посоченото уведомление реши да продължи предаването или да отмени спирането. Предаването на такова уведомление на този надзорен орган и правото му да извършва проверки на получателя на лични данни съгласно клауза 8, параграф 2 от същото приложение позволяват на посочения надзорен орган да проверява дали следва да спре или да забрани планираното предаване, за да се осигури адекватно ниво на защита.

146 В този контекст член 4 от решението СК, тълкуван в светлината на съображение 5 от Решение за изпълнение 2016/2297, потвърждава, че решението СК не възпрепятства компетентния надзорен орган при необходимост да спира или да забранява предаване на лични данни на трета държава, основано на стандартните клаузи за защита на данните, съдържащи се в приложението към това решение. В това отношение, както следва от отговора на осмия въпрос, освен ако съществува надлежно прието от Комисията решение относно адекватното ниво на защита, компетентният надзорен орган е длъжен по силата на член 58, параграф 2, букви е) и й) от ОРЗД да спре или да забрани такова предаване, когато счита с оглед на всички обстоятелства във връзка с това предаване, че тези клаузи не са или не могат да бъдат спазени в тази трета държава и че изискваната от правото на Съюза защита на предаваните данни не може да бъде осигурена с други средства, в случай че самият установен в Съюза администратор или обработващ лични данни не е спрял или прекратил предаването.

147 Що се отнася до изтъкнатото от комисаря обстоятелство, че предаването на лични данни на такава трета държава би могло евентуално да бъде предмет на различаващи се решения на надзорните органи в различни държави членки, трябва да се добави, че както следва от член 55, параграф 1 и член 57, параграф 1, буква а) от ОРЗД, задачата да следи за спазването на този регламент, по принцип е възложена на всеки надзорен орган на територията на собствената му държава членка. Освен това, за да се избегнат различаващи се решения, член 64, параграф 2 от посочения регламент предвижда възможността надзорен орган, който счита, че предаването на данни на трета държава като цяло трябва да бъде забранено, да поиска становище от Европейския комитет по защита на данните (ЕКЗД), който съгласно член 65, параграф 1, буква в) от същия регламент може да приеме решение със задължителен характер по-специално когато надзорен орган не се е съобразил с даденото становище.

148 От това следва, че решението СК предвижда ефективни механизми, които на практика позволяват да се гарантира, че предаването на лични данни на трета държава въз основа на стандартни клаузи за защита на данните, съдържащи се в приложението към това решение, се спира или забранява, когато получателят на данните не спазва посочените клаузи или е в невъзможност да ги спази.

149 Предвид гореизложените съображения на седмия и единадесетия въпрос следва да се отговори, че при разглеждането на решението СК с оглед на членове 7, 8 и 47 от Хартата не се установяват обстоятелства, които могат да засегнат валидността на това решение.

По четвърти, пети, девети и десети въпрос

150 С деветия си въпрос запитващата юрисдикция иска по същество да се установи дали и в каква степен даден надзорен орган на държава членка е обвързан от констатациите в решението ЩЛД, че Съединените щати гарантират достатъчна степен на защита. С четвъртия, петия и десетия си въпрос тази юрисдикция иска по същество да се установи дали с оглед на собствените ѝ констатации относно правото на Съединените щати предаването на тази трета държава на лични данни въз основа на стандартни клаузи за защита на данните, съдържащи се в приложението към решението СК, нарушава правата, гарантирани с членове 7, 8 и 47 от Хартата, и в частност иска от Съда да установи дали въвеждането на споменатия в приложение III към решението ЩЛД омбудсман е съвместимо с този член 47.

151 В самото начало е важно да се отбележи, че макар подадената от комисаря в главното производство жалба да поставя под съмнение валидността само на решението СК, тази жалба е подадена пред запитващата юрисдикция преди приемането на решението ЩЛД. Доколкото с четвъртия и петия си въпрос тази юрисдикция отправя питане по общ начин до Съда относно защитата, която трябва да се осигури по силата на членове 7, 8 и 47 от Хартата при такова предаване, проверката на Съда трябва да вземе предвид последиците от междувременното приемане на решението ЩЛД. Това важи в още по-голяма степен, тъй като с десетия си въпрос посочената юрисдикция изрично иска да се установи дали защитата, изисквана от този член 47, е осигурена посредством споменатия в последното решение омбудсман.

152 Освен това от данните, съдържащи се в акта за преюдициално запитване, е видно, че в рамките на главното производство Facebook Ireland твърди, че решението ЩЛД има обвързващо действие за комисаря по отношение на констатацията за адекватността на гарантираното от Съединените щати ниво на защита и следователно относно законосъобразността на предаване на тази трета държава на лични данни, основано на стандартните клаузи за защита на данните, съдържащи се в приложението към решението СК.

153 Както обаче следва от точка 59 от настоящото съдебно решение, в приложеното към преюдициалното запитване решение от 3 октомври 2017 г. запитващата юрисдикция подчертава, че е длъжна да вземе предвид измененията на правото, настъпили между подаването на жалбата и организираното от нея съдебно заседание. Така тази юрисдикция, изглежда, е длъжна да вземе предвид промяната в обстоятелствата вследствие приемането на решението ЩЛД, както и евентуалното му обвързващо действие, за да разреши спора в главното производство.

154 По-конкретно, наличието на обвързващо действие във връзка с констатацията в решението ЩЛД за адекватна степен на защита в Съединените щати е релевантно за целите на преценката както на задълженията, припомнени в точки 141 и 142 от настоящото решение, на администратора и на получателя на лични данни, предадени на трета държава въз основа на стандартни клаузи за защита на данните, съдържащи се в приложението към решението СК, така и на задълженията, които има надзорният орган евентуално да спре или да забрани такова предаване.

155 Всъщност, що се отнася до обвързващото действие на решението ЩЛД, член 1, параграф 1 от това решение предвижда, че за целите на член 45, параграф 1 от ОРЗД „Съединените американски щати гарантират адекватна степен на защита на личните данни, които се предават от Съюза към организации в Съединените щати съгласно щита за личните данни в отношенията между [Европейския съюз] и САЩ“. Съгласно член 1, параграф 3 от посоченото решение личните данни се считат за предадени съгласно този щит, когато предаването се извършва от Съюза към организации, установени в Съединените щати, които са включени в

списъка към посочения щит, който се поддържа и се предоставя за публичен достъп от Министерството на търговията на САЩ, в съответствие с точки I и III от принципите, установени в приложение II към същото решение.

156 Както следва от съдебната практика, припомнена в точки 117 и 118 от настоящото съдебно решение, решението ЩЛД е обвързващо за надзорните органи, доколкото с него се установява, че Съединените щати гарантират адекватно ниво на защита и следователно се разрешава предаване на лични данни, извършвано съгласно Щита за личните данни в отношенията между Европейския съюз и Съединените щати. Ето защо, докато това решение не бъде обявено за невалидно от Съда, компетентният надзорен орган не може да спре или да забрани предаване на лични данни на организация, включена в списъка към този щит, с мотива че противно на преценката на Комисията в посоченото решение, счита, че законодателството на Съединените щати, което урежда достъпа до предадените съгласно посочения щит лични данни, и използването на тези данни от публичните органи на тази трета държава за целите на националната сигурност, правоприлагането или обществения интерес, не осигурява адекватно ниво на защита.

157 Това не променя факта, че съгласно припомнената в точки 119 и 120 от настоящото решение съдебна практика, когато е сезиран от лице с жалба, компетентният надзорен орган трябва да провери напълно независимо дали разглежданото предаване на лични данни отговаря на въведените с ОРЗД изисквания, и ако счита за основателни оплакванията на това лице за оспорване на валидността на решение относно адекватното ниво на защита, да подаде жалба пред националните юрисдикции, така че последните да отправят до Съда преюдициално запитване за преценка на валидността на това решение.

158 Всъщност жалба, подадена на основание на член 77, параграф 1 от ОРЗД, с която лице, чиито лични данни са били или биха могли да бъдат предадени на трета държава, твърди, че въпреки констатацията на Комисията в прието въз основа на член 45, параграф 3 от този регламент решение правото и практиките на третата държава не гарантират адекватно ниво на защита, трябва да се разглежда като жалба, отнасяща се по същество до съвместимостта на това решение със защитата на личния живот и на основните права и свободи на лицата (вж. по аналогия, що се отнася до член 25, параграф 6 и член 28, параграф 4 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 59).

159 В случая г-н Schrems по същество е поискал от комисаря да забрани или да спре предаването от Facebook Ireland на личните му данни на установеното в Съединените щати Facebook Inc., с довода че тази трета държава не осигурява адекватно ниво на защита. Тъй като след разследване на твърденията на г-н Schrems комисарят е сезирал запитващата юрисдикция, последната, изглежда, предвид представените доказателства и проведените пред нея устни състезания си задава въпроси относно основателността на съмненията на г-н Schrems за адекватността на нивото на защита, осигурено в посочената трета държава, въпреки това, което Комисията междувременно е констатирала в решението ЩЛД, поради което тази юрисдикция поставя на Съда четвърти, пети и десети преюдициален въпрос.

160 Както отбелязва генералният адвокат в точка 175 от заключението си, тези преюдициални въпроси трябва да се разбират в смисъл, че по същество поставят под въпрос съдържащата се в решението ЩЛД констатация на Комисията, че Съединените щати осигуряват адекватно ниво на защита на личните данни, предавани от Съюза на тази трета държава, и следователно — валидността на това решение.

161 С оглед на съображенията, изтъкнати в точки 121 и 157—160 от настоящото съдебно решение, и за да е пълен отговорът, който ще бъде даден на запитващата юрисдикция, следва съответно да се провери дали решението ЩЛД съответства на изискванията, произтичащи от ОРЗД, разглеждан във връзка със Хартата (вж. по аналогия решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 67).

162 За приемането от Комисията на решение относно адекватното ниво на защита съгласно член 45, параграф 3 от ОРЗД е необходимо тази институция да направи надлежно мотивирана констатация, че по силата на вътрешното си законодателство или на международните си ангажименти съответната трета държава ефективно гарантира ниво на защита на основните права, което по същество е равностойно на гарантираното в правния ред на Съюза (вж. по аналогия, що се отнася до член 25, параграф 6 от Директива 95/46, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 96).

По съдържанието на решението ЩЛД

163 В член 1, параграф 1 от решение ЩЛД Комисията констатира, че Съединените щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към организации в Съединените щати съгласно Щита за личните данни в отношенията между Европейския съюз и Съединените щати, който съгласно член 1, параграф 2 от това решение се състои по-специално от принципите, публикувани от Министерството на търговията на САЩ на 7 юли 2016 г. и съдържащи се в приложение II към посоченото решение, както и от официалните писмени изявления и ангажиментите, съдържащи се в документите, поместени в приложения I, III—VII към същото решение.

164 Все пак в решението ЩЛД също се пояснява по-конкретно в точка I.5. от приложение II, озаглавено „Принципи на рамката на Щита за личните данни в отношенията между [Европейски съюз] и САЩ“, че придържането към тези принципи може да бъде ограничено по-специално „с оглед спазване изискванията[, свързани с] националната сигурност, [с] обществения интерес или [с] правоприлагането“. Така това решение дава предимство, подобно на Решение 2000/520, на тези изисквания пред посочените принципи, по силата на което предимство американските самосертифицирани организации, получаващи лични данни от Съюза, са длъжни без ограничения да се отклоняват от същите принципи, когато последните влизат в противоречие с посочените изисквания и съответно се оказват несъвместими с тях (вж. по аналогия, що се отнася до Решение 2000/520, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 86).

165 Предвид общия ѝ характер, дерогацията, съдържаща се в точка I.5. от приложение II към решението ЩЛД, съответно прави възможна намесата — въз основа на изисквания, свързани с националната сигурност и с обществения интерес, или въз основа на вътрешното законодателство на Съединените щати — в упражняването на основните права на лицата, чиито лични данни се предават или биха могли да се предадат от Съюза на Съединените щати (вж. по аналогия, що се отнася до Решение 2000/520, решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 87). По-специално, и както е констатирано в решението ЩЛД, такава намеса може да произтича от достъпа и използването от страна на американските публични органи на личните данни, предавани от Съюза на Съединените щати в рамките на програмите за наблюдение PRISM и UPSTREAM на основание на член 702 от FISA, както и на основание на EO 12333.

166 В този контекст Комисията оценява в съображения 67—135 от решението ЩЛД ограниченията и гаранциите, предвидени от правната уредба на Съединените щати, по-специално в член 702 от FISA, в EO 12333 и в PPD-28, във връзка с достъпа и използването от страна на американските

публични органи на личните данни, предавани съгласно Щита за личните данни в отношенията между Европейския съюз и Съединените щати, за целите на националната сигурност, правоприлагането и за други цели от обществен интерес.

167 В края на тази оценка Комисията констатира в съображение 136 от това решение, че „Съединените американски щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към самосертифицирани дружества в Съединените американски щати“, и приема в съображение 140 от посоченото решение, че „въз основа на наличната информация за правния ред на САЩ, […] всяка намеса на публичните органи на Съединените американски щати за целите на националната сигурност, правоприлагането или за други цели от обществен интерес в основните права на физическите лица, чиито данни се предават от Съюза към Съединените щати съгласно Щита за личните данни, и произтичащите от това ограничения, налагани на самосертифицираните организации във връзка със спазването от тяхна страна на Принципите, ще бъде ограничена до строго необходимото за постигането на набелязаната легитимна цел, и че е налице ефективна правна защита срещу подобна намеса“.

По констатацията за адекватното ниво на защита

168 С оглед на обстоятелствата, посочени от Комисията в решението ЩЛД, както и на тези, които запитващата юрисдикция е установила в рамките на главното производство, тази юрисдикция има съмнения дали правото на Съединените щати действително осигурява адекватното ниво на защита, изисквано в член 45 от ОРЗД, разглеждан в светлината на основните права, гарантирани в членове 7, 8 и 47 от Хартата. Посочената юрисдикция счита по-специално, че правото на тази трета държава не предвижда необходимите ограничения и гаранции с оглед разрешената от националната ѝ правна уредба намеса, нито осигурява ефективна съдебна защита срещу такава намеса. Във връзка с последното тя добавя, че според нея въвеждането на омбудсмана към Щита за личните данни не може да отстрани тези пропуски, тъй като този омбудсман не може да бъде приравнен на съд по смисъла на член 47 от Хартата.

169 Що се отнася, на първо място, до членове 7 и 8 от Хартата, които са част от нивото на защита, изисквана в рамките на Съюза и чието спазване трябва да бъде констатирано от Комисията, преди тя да приеме решение относно адекватното ниво на защита съгласно член 45, параграф 1 от ОРЗД, следва да се припомни, че член 7 от Хартата гарантира на всеки правото на зачитане на неговия личен и семеен живот, на неговото жилище и тайната на неговите съобщения. Що се отнася до член 8, параграф 1 от Хартата, той изрично признава на всеки правото на защита на неговите лични данни.

170 Така достъпът до лични данни на физическо лице с оглед на тяхното съхранение или използване засяга основното право на това лице на зачитане на неговия личен живот, гарантирано в член 7 от Хартата, като това право се отнася до всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано. Посоченото обработване на данни попада и в обхвата на член 8 от Хартата, поради това че представлява обработка на лични данни по смисъла на посочения член, и следователно задължително трябва да отговаря на изискванията за защита на данните, произтичащи от него (вж. в този смисъл решения от 9 ноември 2010 г., Volker und Markus Schecke и Eifert, C-92/09 и C-93/09, EU:C:2010:662, т. 49 и 52, от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 29 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 122 и 123).

171 Съдът вече е постановил, че съобщаването на лични данни на трето лице, например публичен орган, представлява намеса в основните права, закрепени в членове 7 и 8 от Хартата, независимо от последващото използване на съобщената информация. Същото се отнася за запазването на лични данни, както и за достъпа до тях с оглед на използването им от

публичните органи, независимо дали съответните данни за личния живот имат чувствителен характер и дали заинтересованите лица са претърпели евентуални неудобства поради тази намеса (вж. в този смисъл решения от 20 май 2003 г., Österreichischer Rundfunk и др., C-465/00, C-138/01 и C-139/01, EU:C:2003:294, т. 74 и 75, от 8 април 2014 г., Digital Rights Ireland и др., C-293/12 и C-594/12, EU:C:2014:238, т. 33—36 и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 124 и 126).

172 При все това правата, признати в членове 7 и 8 от Хартата, не са абсолютни, а трябва да се разглеждат във връзка с тяхната социална функция (вж. в този смисъл решения от 9 ноември 2010 г., Volker und Markus Schecke и Eifert, C-92/09 и C-93/09, EU:C:2010:662, т. 48 и цитираната съдебна практика, от 17 октомври 2013 г., Schwarz, C-291/12, EU:C:2013:670, т. 33 и цитираната съдебна практика и становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 136).

173 В това отношение следва също да се отбележи, че съгласно член 8, параграф 2 от Хартата личните данни трябва по-специално да бъдат обработвани „за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание“.

174 Съгласно член 52, параграф 1, първо изречение от Хартата всяко ограничаване на упражняването на признатите от нея права и свободи трябва да бъде предвидено в закон и да зачита основното съдържание на посочените права и свободи. Съгласно член 52, параграф 1, второ изречение от Хартата при спазване на принципа на пропорционалност ограничения на тези права и свободи могат да бъдат налагани само ако са необходими и ако действително отговарят на признати от Съюза цели от общ интерес или на необходимостта да се защитят правата и свободите на други хора.

175 Във връзка с предходното следва да се добави, че изискването всяко ограничение на упражняването на основни права да бъде предвидено в закон, означава, че самото правно основание, позволяващо намеса в тези права, трябва да определя обхвата на ограничението при упражняване на съответното право (становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 139 и цитираната съдебна практика).

176 Накрая, за да удовлетвори изискването за пропорционалност, съгласно което дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото, разглежданата правна уредба, включваща намесата, трябва да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да налагат минимални изисквания, така че лицата, чиито данни са били предадени, да разполагат с достатъчно гаранции, позволяващи ефикасна защита на техните лични данни срещу рискове от злоупотреби. Тя трябва в частност да посочва обстоятелствата и условията, при които може да се приложи мярка за обработване на такива данни, като по този начин гарантира ограничаване на намесата до строго необходимото. Необходимостта от такива гаранции е още по-голяма, когато личните данни са подложени на автоматична обработка (вж. в този смисъл становище 1/15 (Споразумение PNR между ЕС и Канада) от 26 юли 2017 г., EU:C:2017:592, т. 140 и 141 и цитираната съдебна практика).

177 За тази цел член 45, параграф 2, буква а) от ОРЗД уточнява, че в рамките на своята оценка на адекватността на нивото на защита, гарантирана от трета държава, Комисията отчита по-специално „[д]ействителните и приложими права на субектите на данни“, чиито лични данни се предават.

178 В случая констатацията на Комисията в решението ЩЛД, че Съединените щати осигуряват ниво на защита, което по същество е равностойно на гарантираното в Съюза с ОРЗД, разглеждан в светлината на членове 7 и 8 от Хартата, е поставена под съмнение, с мотива по специално че за

намесата, произтичаща от програмите за наблюдение, основани на член 702 от FISA и на ЕО 12333, не се прилагат изисквания, които осигуряват, при спазване на принципа на пропорционалност, ниво на защита, което по същество е равностойно на гарантираното от член 52, параграф 1, второ изречение от Хартата. Ето защо следва да се разгледа дали тези програми за наблюдение се прилагат при спазване на подобни изисквания, без да е необходимо предварително да се проверява дали тази трета държава е спазила условия, които по същество са равностойни на предвидените в член 52, параграф 1, първо изречение от Хартата.

179 В тази връзка, що се отнася до програмите за наблюдение, основани на член 702 от FISA, в съображение 109 от решението ЩЛД Комисията констатира, че съгласно посочения член „[FISC] не дава разрешение за отделни мерки за наблюдение, а за програми за наблюдение (като PRISM, UPSTREAM) въз основа на годишни сертифицирания, изготвени от [главния прокурор] и от директора на Националното разузнаване“. Както следва от същото съображение, упражняваният от FISC контрол има за цел да се провери дали тези програми за наблюдение отговарят на целта за получаване на външноразузнавателна информация, но не се отнася до това „дали […] лицата са определени правилно за обект на разследване с цел придобиване на разузнавателни данни“.

180 Така става ясно, че член 702 от FISA изобщо не разкрива наличието на ограничения на съдържащото се в него оправомощаване за прилагането на програми за наблюдение за целите на външното разузнаване, нито пък съществуването на гаранции за потенциално обхванатите от тези програми лица, които не са американски граждани. При тези условия, и както по същество отбелязва генералният адвокат в точки 291, 292 и 297 от заключението си, този член не може да осигури ниво на защита, което по същество е равностойно на нивото, гарантирано от Хартата, както е тълкувана в припомнената в точки 175 и 176 от настоящото решение съдебна практика, съгласно която, за да удовлетвори принципа на пропорционалност, самото правно основание, позволяващо намеса в основните права, трябва да определя обхвата на ограничението при упражняване на съответното право и да предвижда ясни и точни правила, които да уреждат обхвата и прилагането на разглежданата мярка и да налагат минимални изисквания.

181 Съгласно констатациите в решението ЩЛД прилагането на програмите за наблюдение, основани на член 702 от FISA, несъмнено трябва да се извършва при спазване на произтичащите от PPD-28 изисквания. Все пак, макар Комисията да подчертава в съображения 69 и 77 от решението ЩЛД, че подобни изисквания са обвързващи за американските разузнавателни структури, в отговор на въпрос на Съда американското правителство признава, че PPD-28 не предоставя на субектите на данни приложими пред съдилищата права срещу американските органи. Следователно това решение не може да гарантира ниво на защита, което по същество е равностойно на произтичащото от Хартата, противно на изискването на член 45, параграф 2, буква а) от ОРЗД, съгласно който установяването на това ниво зависи по-специално от наличието на действителни и приложими права на лицата, чиито данни са били предадени на съответната трета държава.

182 Що се отнася до програмите за наблюдение, основани на ЕО 12333, от преписката, с която разполага Съдът, е видно, че и този декрет не предоставя приложими пред съдилищата права срещу американските органи.

183 Следва да се добави, че PPD-28, която трябва да се спазва при прилагането на програмите, посочени в предходните две точки, позволява „събирането на „масиви от данни“ […] на относително голям обем радиоелектронна разузнавателна информация или данни при обстоятелства, при които разузнавателните структури не могат да използват идентификатор, свързан с конкретния обект на разузнаване […], за да концентрират събирането на данни“, както се уточнява в писмо от 21 юни 2016 г. от Службата на директора на Националното разузнаване (Office of the Director of National Intelligence) до американското Министерство на търговията и до Администрацията по международна търговия, съдържащо се в приложение VI

към решението ЩЛД. Впрочем тази възможност, която позволява достъп в рамките на програмите за наблюдение, основани на ЕО 12333, до данни, пренасяни към Съединените щати, без този достъп да подлежи на какъвто и да било съдебен контрол, при всички положения не очертава достатъчно ясно и точно обхвата на това събиране на масиви от лични данни.

184 Поради това изглежда, че нито член 702 от FISA, нито ЕО 12333, разглеждани във връзка с PPD-28, съответстват на минималните изисквания, свързани в правото на Съюза с принципа на пропорционалност, поради което не може да се приеме, че програмите за наблюдение, основани на тези разпоредби, са ограничени до строго необходимото.

185 При тези условия ограниченията на защитата на личните данни, които произтичат от вътрешноправната уредба на Съединените щати относно достъпа и използването от американските публични органи на такива данни, предадени от Съюза на Съединените щати, и които Комисията е оценила в решението ЩЛД, не са определени по начин, който да отговаря на изисквания, които по същество са равностойни на предвидените съгласно правото на Съюза в член 52, параграф 1, второ изречение от Хартата.

186 Що се отнася, на второ място, до член 47 от Хартата, който също е част от изискваното ниво на защита в Съюза и чието спазване Комисията трябва да констатира, преди да приеме решение относно адекватното ниво на защита съгласно член 45, параграф 1 от ОРЗД, следва да се припомни, че първа алинея от този член 47 изисква всеки, чиито права и свободи, гарантирани от правото на Съюза, са били нарушени, да има право на ефективни правни средства за защита пред съд в съответствие с предвидените в този член условия. Съгласно втора алинея от посочения член всеки има право неговото дело да бъде гледано от независим и безпристрастен съд.

187 Съгласно постоянната съдебна практика самото наличие на ефективен съдебен контрол, чието предназначение е да гарантира спазването на разпоредбите от правото на Съюза, е неделимо свързано със съществуването на правовата държава. Така правна уредба, в която не се предвижда никаква възможност правният субект да използва правни средства за защита, за да получи достъп до засягащи го лични данни или да поправи или заличи такива данни, не зачита съществото съдържание на основното право на ефективна съдебна защита, признато в член 47 от Хартата (решение от 6 октомври 2015 г., Schrems, C-362/14, EU:C:2015:650, т. 95 и цитираната съдебна практика).

188 За тази цел член 45, параграф 2, буква а) от ОРЗД изисква в рамките на своята оценка за осигуреното от трета държава адекватно ниво на защита Комисията да отчита по-специално „ефективната административна и съдебна защита за субектите на данни, чиито лични данни се предават“. В съображение 104 от ОРЗД се подчертава в това отношение, че третата държава „следва […] да осигури ефективен независим надзор в областта на защитата на данните и да предвиди механизми за сътрудничество с органи по защита на данните на държавите членки, а на субектите на данните следва да бъдат предоставени действителни и приложими права и ефективни средства за административна и съдебна защита“.

189 Наличието на такива ефективни средства за защита в съответната трета държава е от особено значение в контекста на предаването на лични данни на тази трета държава, доколкото, както следва от съображение 116 от ОРЗД, субектите на данни могат да счетат, че административните и съдебните органи на държавите членки имат недостатъчни правомощия и средства, за да предприемат надлежни действия по техните жалби, основани на твърдяно незаконосъобразно обработване в тази трета държава на така прехвърлените техни данни, което може да ги принуди да се обърнат към националните органи и съдилища на същата трета държава.

190 В случая констатацията на Комисията в решението ЩЛД, че Съединените щати гарантират ниво на защита, което по същество е равностойно на гарантираното в член 47 от Хартата, е поставена под въпрос по-специално с мотива че въвеждането на омбудсмана към Щита за личните данни не може да поправи установените от самата Комисия пропуски, що се отнася до съдебната защита на лицата, чиито лични данни са предадени на тази трета държава.

191 В това отношение Комисията посочва в съображение 115 от решение ЩЛД, че ако „лицата, включително субектите на данни от [Съюза], имат редица възможности за правна защита, когато са станали обект на неправомерно (електронно) наблюдение за целите на националната сигурност, също така е ясно, че не са обхванати най-малкото някои от правните основания, които могат да се използват от разузнавателните органи на САЩ (напр. [ЕО 12333])“. Така, що се отнася до ЕО 12333, тя подчертава в посоченото съображение 115 отсъствието на какъвто и да било способ за защита. Съгласно припомнената в точка 187 от настоящото решение съдебна практика от такъв пропуск в съдебната защита по отношение на намесата във връзка с програмите за разузнаване, основани на този изпълнителен декрет, обаче не може да се изведе, както прави Комисията в решението ЩЛД, че правото на Съединените щати осигурява ниво на защита, което по същество е равностойно на гарантираното в член 47 от Хартата.

192 Освен това, що се отнася както до програмите за наблюдение, основани на член 702 от FISA, така и до тези, основани на ЕО 12333, в точки 181 и 182 от настоящото съдебно решение бе отбелязано, че нито PPD-28, нито ЕО 12333 предоставят на субектите на данни приложими пред съдилищата права срещу американските органи, поради което тези лица не разполагат с право на ефективни правни средства за защита.

193 Комисията обаче констатира в съображения 115 и 116 от решението ЩЛД, че поради наличието на създадения от американските органи механизъм на омбудсмана към Щита за личните данни, както е описан в писмото, изпратено на 7 юли 2016 г. от американския държавен секретар до Европейския комисар по въпросите на правосъдието, потребителите и равнопоставеността между половете, което се съдържа в приложение III към това решение, и поради естеството на задачата, възложена на омбудсмана, в случая „старши координатор на международната дипломация в областта на информационните технологии“, може да се приеме, че Съединените щати осигуряват ниво на защита, което по същество е равностойно на гарантираното в член 47 от Хартата.

194 Разглеждането на въпроса дали механизмът на омбудсмана, посочен в решението ЩЛД, действително може да поправи установените от Комисията ограничения на правото на съдебна защита, в съответствие с изискванията, произтичащи от член 47 от Хартата и от припомнената в точка 187 от настоящото решение съдебна практика, трябва да се основе на принципа, че правните субекти трябва да разполагат с възможността да използват правни средства за защита пред независим и безпристрастен съд, за да получат достъп до отнасящи се до тях лични данни или да поправят или заличат такива данни.

195 В писмото, посочено в точка 193 от настоящото съдебно решение, омбудсманът към Щита за личните данни, макар да е описан като „независим от разузнавателната общност“, е представен като „пряко подчинен на държавния секретар, който ще гарантира, че Омбудсманът изпълнява функциите си обективно и без неправомерно влияние, което може да има отражение върху отговорите, които следва да се предоставят“. Нещо повече, освен че както констатира Комисията в съображение 116 от това решение, омбудсманът е назначен от държавния секретар и е неразделна част от държавния департамент на Съединените щати, в посоченото решение не се съдържат данни, както отбелязва генералният адвокат в точка 337 от заключението си, че освобождаването от длъжност на омбудсмана или отмяната на назначаването му са обвързани с конкретни гаранции, което може да постави под въпрос независимостта на омбудсмана от изпълнителната власт (вж. в този смисъл решение от 21 януари 2020 г., Banco de Santander, C-274/14, EU:C:2020:17, т. 60 и 63 и цитираната съдебна практика).

196 Също така, както подчертава генералният адвокат в точка 338 от заключението си, макар в съображение 120 от решението ЩЛД да се посочва, че американското правителство е поело ангажимент съответната разузнавателна структура да отстрани всяко нарушение на приложимите стандарти, установено от омбудсмана към Щита за личните данни, в посоченото решение не се указва, че този омбудсман е оправомощен да взема обвързващи решения по отношение на тези структури, и освен това не се посочват законови гаранции, които да придружават този ангажимент и на които субектите на данни да могат да се позоват.

197 Следователно механизмът на омбудсмана, посочен в решението ЩЛД, не предоставя способ за защита пред орган, който предоставя на лицата, чиито данни са предадени на Съединените щати, гаранции, които по същество са равностойни на изискваните от член 47 от Хартата.

198 Следователно, като е констатирала в член 1, параграф 1 от решението ЩЛД, че Съединените щати гарантират адекватна степен на защита за личните данни, които се предават от Съюза към организации в Съединените щати съгласно Щита за личните данни в отношенията между ЕС и САЩ, Комисията е нарушила изискванията, произтичащи от член 45, параграф 1 от ОРЗД, разглеждан в светлината на членове 7, 8 и 47 от Хартата.

199 От това следва, че член 1 от решението ЩЛД е несъвместим с член 45, параграф 1 от ОРЗД, разглеждан в светлината на членове 7, 8 и 47 от Хартата, и поради това е невалиден.

200 Тъй като член 1 от решението ЩЛД е неразделно свързан с членове 2—6 и с приложенията към това решение, неговата невалидност засяга валидността на последното в неговата цялост.

201 С оглед на изложените съображения се налага изводът, че решението ЩЛД е невалидно.

202 Що се отнася до въпроса дали следва да се запазят последиците от това решение, за да се избегне създаването на празнота в правото (вж. в този смисъл решение от 28 април 2016 г., Borealis Polyolefine и др., C-191/14, C-192/14, C-295/14, C-389/14 и C-391/14—C-393/14, EU:C:2016:311, т. 106), трябва да се отбележи, че във всеки случай, предвид член 49 от ОРЗД, отмяната на решение относно адекватното ниво на защита, каквото е решението ЩЛД, не може да създаде такава празнота в правото. Всъщност този член подробно установява условията, при които предаването на лични данни на трети държави може да се осъществи при липсата на решение относно адекватното ниво на защита съгласно член 45, параграф 3 от посочения регламент или на подходящи гаранции съгласно член 46 от същия регламент.

По съдебните разноски

203 Тъй като за страните по главното производство настоящото дело представлява отклонение от обичайния ход на производството пред запитващата юрисдикция, последната следва да се произнесе по съдебните разноски. Разходите, направени за представяне на становища пред Съда, различни от тези на посочените страни, не подлежат на възстановяване.

По изложените съображения Съдът (голям състав) реши:

1) **Член 2, параграфи 1 и 2 от Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) трябва да се тълкува в смисъл, че предаване на лични данни за търговски цели от икономически оператор, установен в държава членка, към друг икономически оператор, установен в трета държава, попада в приложното поле на този регламент,**

независимо че по време на предаването или след него тези данни могат да се обработват от органите на съответната трета държава за целите на обществената сигурност, отбраната и държавната сигурност.

2) **Член 46, параграф 1 и член 46, параграф 2, буква в) от Регламент 2016/679 трябва да се тълкуват в смисъл, че изискванията от тези разпоредби подходящи гаранции, приложими права и ефективни правни средства за защита трябва да гарантират, че правата на лицата, чиито лични данни са предадени на трета държава въз основа на стандартни клаузи за защита на данните, се ползват с ниво на защита, което по същество е равностойно на гарантираното в Европейския съюз с този регламент, разглеждан в светлината на Хартата на основните права на Европейския съюз. За тази цел при оценката на гарантираното в контекста на такова предаване ниво на защита трябва по-специално да се вземат предвид както договорните клаузи, уговорени между администратора или обработващия лични данни, установени в Европейския съюз, и получателя на предаването, установен в съответната трета държава, така и, що се отнася до евентуалния достъп на публичните органи на тази трета държава до така предадените лични данни, релевантните елементи на нейната правна система, и по-специално посочените в член 45, параграф 2 от този регламент.**

3) **Член 58, параграф 2, букви е) и й) от Регламент 2016/679 трябва да се тълкува в смисъл, че, освен ако съществува надлежно прието от Европейската комисия решение относно адекватното ниво на защита, компетентният надзорен орган е длъжен да спре или да забрани предаването на данни на трета държава, основаващо се на приети от Комисията стандартни клаузи за защита на данните, когато с оглед на всички обстоятелства във връзка с това предаване надзорният орган счита, че тези клаузи не са или не могат да бъдат спазени в тази трета държава и че защитата на предаваните данни, изисквана от правото на Съюза, по-специално от членове 45 и 46 от този регламент и от Хартата на основните права, не може да бъде осигурена с други средства, в случай че самият установен в Съюза администратор или обработващ лични данни не е спрял или прекратил предаването.**

4) **При разглеждането на Решение 2010/87/ЕС на Комисията от 5 февруари 2010 година относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета, изменено с Решение за изпълнение (ЕС) 2016/2297 на Комисията от 16 декември 2016 г., с оглед на членове 7, 8 и 47 от Хартата на основните права не се установяват обстоятелства, които могат да засегнат валидността на това решение.**

5) **Решение за изпълнение (ЕС) 2016/1250 на Комисията от 12 юли 2016 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ, е невалидно.**

Подписи