
# Препоръки 01/2021 относно разпоредбите, регламентиращи адекватното ниво на защита на данните съгласно Директивата относно правоприлагането

**Приети на 2 февруари 2021 г.**

# Съдържание

**Европейският комитет по защита на данните,**

като взе предвид член 51, параграф 1, буква б) от Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета[1],

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

**ПРИЕ НАСТОЯЩИТЕ ПРЕПОРЪКИ**

# 1. УВОД

1. Работната група по член 29 (РГ29) публикува Работен документ[2] относно разпоредбите, регламентиращи адекватното ниво на защита на данните съгласно Общия регламент относно защитата на данните (ОРЗД)[3]. Работният документ бе приет от Европейския комитет по защита на данните (ЕКЗД) на първото си пленарно заседание.

2. Както е посочено в Декларация № 21, приложена към Договора от Лисабон, в областта на съдебното сътрудничество по наказателноправни въпроси и на полицейското сътрудничество въз основа на член 16 от Договора за функционирането на Европейския съюз (ДФЕС) могат да се окаже необходимо приемането на специфични правила за защита на личните данни и за тяхното свободно движение поради естеството на тези области.

3. На това основание, законодателят на Съюза прие Директива (ЕС) 2016/680 (Директива относно правоприлагането, наричана по-долу „ДП“), с която се установяват специалните правила във връзка с обработването на лични данни от компетентните органи за целите на **предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване**.

4. ДП определя основанията, при които се позволява предаването на лични данни на трета държава или международна организация. Един от инструментите за такова предаване е решението на Европейската комисия, че въпросната трета държава или международна организация осигурява адекватно ниво на защита.

[1] ОВ L 119, 4.5.2016 г., стр. 89.
[2] РД254.ред.01, приет от РГ 29 на 28 ноември 2017 г., последно преразгледан и приет на 6 февруари 2018 г. С него се актуализира глава I от работния документ „Предаване на лични данни на трети държави: прилагане на членове 25 и 26 от Директивата на ЕС относно защитата на данните“, РГ12, приет от РГ29 на 24 юли 1998 г.
[3] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 26 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016 г., стр. 1.

5. Докато чрез Работния документ (РД254.ред.01) относно разпоредбите, регламентиращи адекватното ниво на защита на данните се цели да се предоставят насоки на Европейската комисия за нивото на защита на данните в трети държави и международни организации съгласно ОРЗД, чрез настоящия документ се цели да се предоставят подобни насоки съгласно ДП. В тази връзка той установява основните принципи за защита на личните данни, които трябва да присъстват в правната уредба на трета държава или на международна организация, за да се осигури съществено съответствие с правната уредба на ЕС в рамките на ДП (т.е. за обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или преследването за престъпления или налагането на наказателни санкции). Освен това документът може да предостави насоки и на трети държави, и международни организации, които са заинтересовани от получаването на статут на трета държава или международна организация с адекватно ниво на защита.

6. Акцентът на настоящия документ е единствено върху решенията за адекватно ниво на защита. Това са актове за изпълнение на Европейската комисия в съответствие с член 36, параграф 3 от ДП.

## 2. ПОНЯТИЕ ЗА АДЕКВАТНО НИВО НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

7. ДП определя правилата за предаване на лични данни на трети държави и международни организации дотолкова, доколкото подобно предаване попада в нейния обхват. Правилата за международно предаване на лични данни са изложени в глава V от ДП, и по-конкретно в членове 35—39.

8. Съгласно член 36 от ДП предаването на данни на трети държави или международни организации може да бъде осъществено, ако дадена трета държава, територия или един или повече конкретни сектори в трета държава или дадена международна организация осигуряват адекватно ниво на защита. От съдебната практика на Съда на Европейския съюз (Съда на ЕС)[4] следва, че тази разпоредба трябва да се тълкува в светлината на член 35 от ДП, озаглавен „Общи принципи за предаване на лични данни“, който предвижда, че „всички разпоредби [в глава V на ДП] се прилагат, за да се гарантира, че нивото на защита на физическите лица, гарантирано от настоящата директива, не се излага на риск.“

9. Когато Европейската комисия реши, че е осигурено подобно адекватно ниво на защита, предаването на лични данни до съответната трета държава, територия, сектор или международна организация може да бъде осъществено, без да е необходимо специално разрешение, освен ако друга държава членка, от която са получени данни, не трябва да даде разрешение за предаването, както е предвидено в членове 35 и 36 и съображение 66 от ДП. Това не засяга необходимостта обработването на данни от съответните органи на държавата членка да се извършва в съответствие с приетите национални разпоредби съгласно Директива (ЕС) 2016/680.

[4] Решение от 16 юли 2020 г., Data Protection Commissioner срещу Facebook Ireland Ltd и Maximillian Schrems, C-311/18, ECLI:EU:C:2020:559, точка 92 (Schrems II).

10. Понятието за „адекватно ниво на защита“, което вече съществуваше съгласно Директива 95/46/ЕО[5] и Рамково решение 2008/977/ПВР на Съвета[6], бе доразвито от Съда на ЕС и наскоро в рамките на ОРЗД.

11. Както е посочено от Съда на ЕС, докато степента на защита в третата държава трябва да бъде по същество равностойна на гарантираната в ЕС, „средствата, до които третата държава прибягва в това отношение, за да гарантира такава степен на защита, може да са различни от прилаганите вътре в Европейския съюз“, но „все пак е необходимо на практика тези средства да се окажат ефективни“[7]. Ето защо за постигане на определения стандарт за адекватно ниво на защита не е необходимо законодателството на ЕС да се отрази точка по точка, а да се установят съществените, основните изисквания на това законодателство.

12. В тази връзка Съдът също така уточни, че решението на Комисията относно адекватното ниво на защита следва да съдържа заключение относно наличието в третата държава на правила, приети от нея, предназначени за ограничаване на евентуалната намеса на публичноправните субекти, които *биха имали право* да обработват лични данни с оглед преследване на законосъобразни цели, като например осигуряване на националната сигурност и които засягат основните права на лицата, чиито данни се предават от Европейския съюз към тази трета държава[8].

13. Целта на решенията относно адекватното ниво на защита, които се вземат от Европейската комисия, е официално да се потвърди с обвързващи последици за държавите членки,[9] включително за техните компетентни органи за защита на личните данни[10], че нивото на защита на данните в дадена трета държава или международна организация е по същество равностойно на нивото на защита на данните в Европейския съюз. Третата държава следва да предостави гаранции, които да осигуряват адекватно ниво на защита, по същество равностойно на гарантираното в рамките на Съюза, по-специално, когато данните се обработват в един или повече конкретни сектори[11].

14. Адекватно ниво на защита може да се постигне чрез комбинация от права за субектите на данни и задължения за лицата, които обработват данните или които упражняват контрол върху това обработване и надзор от страна на независими органи. Правилата за защита на данните обаче са ефективни само ако се прилагат и се спазват на практика. Поради това е необходимо да се разгледат не само съдържанието на правилата, които са приложими за предаването на лични данни на трета държава или международна организация, но също така въведената система за гарантиране на ефективността на тези правила. Ефикасните

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

[6] Рамково решение 2008/977/ПВР на Съвета от 27 ноември 2008 г. относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, ОВ L 350, 30.12.2008 г., стр. 60.

[7] Решение от 6 октомври 2015 г., Maximillian Schrems срещу Data Protection Commissioner, C−362/14, ECLI:EU:C:2015:650, точки 73 и 74 (Schrems I).

[8] Schrems I, точка 88.

[9] Член 288, параграф 2 от ДФЕС.

[10] Schrems I, точка 52.

[11] Съображение 67 от ДП.

механизми за правоприлагане са от съществена важност за ефективността на правилата за защита на данните.[12].

## 3. ПРОЦЕДУРНИ АСПЕКТИ НА ЗАКЛЮЧЕНИЯТА, ОТНАСЯЩИ СЕ ДО АДЕКВАТНОТО НИВО НА ЗАЩИТА СЪГЛАСНО ДП

15. За да може да изпълни задачата си за даване на консултации на Европейската комисия в съответствие с член 51, параграф 1, буква ж) от ДП, на ЕКЗД следва да се предостави съответната документация, включително свързаната кореспонденция и заключенията, направени от Европейската комисия. Абсолютно наложително е съответните документи да бъдат предадени достатъчно рано и преведени на английски език, за да се даде възможност на ЕКЗД да проведе информирани и полезни дискусии преди окончателното приемане на решения относно адекватното ниво на защита. Когато правната уредба е сложна, предоставената документация следва да включва всеки един изготвен доклад относно нивото на защита на данните в третата държава или международната организация. Във всеки случай предоставената от Европейската комисия информация трябва да бъде изчерпателна и да дава възможност на ЕКЗД да оцени анализа, извършен от Комисията , по отношение на нивото на защита на данните в третата държава или международната организация.

16. Комитетът ще представи своевременно своето становище по заключенията на Европейската комисия, посочвайки недостатъците в рамката за осигуряване на адекватно ниво на защита, ако има такива, и предоставяйки възможни препоръки, когато е необходимо.

17. Според член 36, параграф 4 от ДП, Европейската комисия осъществява постоянно наблюдение на развитието, което би могло да повлияе на действието на решение относно адекватното ниво на защита.

18. В член 36, параграф 3 от ДП се предвижда, че трябва да се извършва периодичен преглед най-малко веднъж на четири години. Това обаче е общ срок, който следва да се адаптира за всяка трета държава или международна организация, за която е прието решение относно адекватното ниво на защита. В зависимост от конкретните обстоятелства в дадения случай, може да е обосновано прилагането на по-кратък период за извършване на прегледа. Освен това, възникването на извънредни обстоятелства или предоставяне на друга информация, или настъпили промени в правната уредба в дадената трета държава или международна организация, биха могли да породят необходимост от предсрочен преглед. Също така изглежда целесъобразно първият преглед на напълно ново решение относно адекватното ниво на защита да се извършва по-рано от заложеното и периода за извършване на прегледите да се коригира постепенно в зависимост от резултата.

[12] Schrems I, точки 72—74 и Становище 1/15 на Съда на ЕС относно проекта на споразумение между Канада и Европейския съюз, 26 юли 2017 г., ECLI:EU:C:2017:592 (Становище 1/15), точка 134: „Посоченото право на защита на личните данни изисква по-специално да се осигури непрекъснатост на предоставеното от правото на Съюза високо ниво на защита на основните права и свободи при прехвърляне на лични данни от Съюза към трета държава. Макар да е възможно средствата, които целят да гарантират такава степен на защита, да са различни от прилаганите вътре в Съюза, за да се гарантира спазването на изискванията, произтичащи от правото на Съюза, все пак е необходимо на практика тези средства да се окажат ефективни с цел да се осигури защита, която по същество е равностойна на гарантираната в Съюза.“

19. Предвид задачата на Европейския комитет по защита на данните да предостави на Европейската комисия становище дали третата държава, територия или един или повече конкретни сектори в третата държава или дадена международна организация са престанали да осигуряват адекватно ниво на защита, Комитетът трябва своевременно да получи важната информация от извършения мониторинг от Европейската комисия на съответното развитие в дадената трета държава или международна организация. Съответно Комитетът следва да бъде информиран за всички процедури за преглед на правната уредба или за всички възложени задачи за такъв преглед в третата държава или международната организация. Комитетът препоръчва да бъде поканен за участие в тези процедури за преглед и задачи, както бе предвидено в решението за Щита за личните данни в отношенията между ЕС и САЩ и в решението относно адекватното ниво на защита на данните по отношение на Япония.

20. Следва също така да се отбележи, че съгласно член 36, параграф 5 от ДП Европейската комисия има правомощието, когато третата държава или международната организация вече не осигурява адекватно ниво на защита, да отменя, изменя или спира прилагането на съществуващи решения относно адекватното ниво на защита. ЕКЗД е включен в процедурата за отмяна, изменение или спиране, като се иска неговото становище в съответствие с член 51, параграф 1, буква ж от ДП.

21. Освен това, без да се засягат правомощията на прокуратурата, надзорните органи следва също да имат правомощието да сезират съдебните органи за нарушения на тази директива или да участват в съдебни производства[13]. По-конкретно, от решението на Съда на ЕС по делото Schrems I следва, че органите за защита на данните трябва да имат възможност да участват в съдебни производства пред националните съдилища, ако считат, че искът, предявен от дадено лице срещу решение относно адекватното ниво на защита, е основателен[14]. Решението по делото Schrems II потвърди тази оценка[15].

# 4. СТАНДАРТИ НА ЕС ЗА АДЕКВАТНОТО НИВО НА ЗАЩИТА ПРИ ПОЛИЦЕЙСКОТО И СЪДЕБНО СЪТРУДНИЧЕСТВО ПО НАКАЗАТЕЛНОПРАВНИ ВЪПРОСИ

22. По същество, при решенията относно адекватното ниво на защита следва да се постави акцент върху оценката на съществуващото законодателство на съответната трета държава като цяло, на теория и практика, като се вземат предвид критериите за оценка, посочени в член 36 от ДП. Системата на третата държава или на международната организация трябва

[13] Вж. член 47, параграф 5 от ДП и съображение 82 от нея.

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

[15] Вж. Schrems II, точка 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.“

да включва следните основни общи принципи и механизми, отнасящи се до процедурите и прилагането в областта на защитата на данните.

23. В член 36, параграф 2 от ДП са установени елементите, които Европейската комисия взема предвид при оценяването на адекватността на нивото на защита в трета държава или международна организация.

24. По-конкретно, Комисията взема предвид върховенството на закона, спазването на правата на човека и основните свободи[16], съответното законодателство, както и прилагането на това законодателство, наличието на действителни и приложими права на субектите на данни и ефективни средства за административна и съдебна защита за физическите лица, чиито лични данни се предават, наличието и ефективното функциониране на един или повече независими надзорни органи, и международните ангажименти, които съответната трета държава или международна организация е поела.

25. Затова е ясно, че всеки значим анализ на адекватната защита трябва да включва два основни елемента: съдържанието на приложимите правила и средствата за осигуряване на тяхното ефективно практическо прилагане. Европейската комисия следва редовно да проверява дали въведените правила са ефективни на практика.

26. Основната част от общите принципи за защита на данните и от изискванията за процедурите, и правоприлагането, които може да се разглеждат като минимално изискване за адекватна защита, произтичат от Хартата на основните права на ЕС (Хартата) и от ДП. Не е достатъчно да са налице общи разпоредби за защита на данните и неприкосновеността на личния живот в третата държава. Напротив, в правната уредба на третата държава или международната организация трябва да бъдат включени специфични разпоредби, конкретно насочени към правото на защита на данните в областта на правоприлагането. Третата държава следва да предостави гаранции, които осигуряват адекватно ниво на защита, по същество равностойно на гарантираното в рамките на Съюза. Изпълнението на тези разпоредби трябва да може да бъде осигурявано.

27. Освен това, що се отнася до принципа на пропорционалност[17], Съдът на ЕС е приел, че по отношение на законодателствата на държавите членки преценката, дали ограничението на правата на неприкосновеност на личния живот и на защита на личните данни може да бъде оправдано, следва да се извърши, като се измери, от една страна, **тежестта на намесата,** която е вследствие от такова ограничение,[18] а от друга страна, като се провери дали

[16] При оценката на правната уредба на третата държава следва да се вземе под внимание възможността за налагане на смъртно наказание или каквато и да е форма на жестоко и нечовешко отношение въз основа на данни, предадени от ЕС. Ако в действителност такова наказание или отношение е предвидено в законодателството на третата държава, следва да се открият допълнителни гаранции в правната уредба на третата държава, които да гарантират, че предадените от ЕС данни няма да бъдат използвани за искане, постановяване или изпълнение на смъртно наказание или каквато и да е форма на жестоко и нечовешко отношение (например- международно споразумение, налагащо условия за предаването на данните, ангажимент от страна на третата държава да не налага смъртно наказание или каквато и да е форма на жестоко и нечовешко отношение въз основа на данните, предадени от ЕС, или мораториум на смъртното наказание).

[17] Член 52, параграф 1 от Хартата.

[18] Съдът отбеляза например, че „намесата, състояща се в събирането на данни в реално време, което позволява локализирането на крайно оборудване, изглежда особено сериозна, тъй като тези данни предоставят на компетентните национални органи средства за точно и постоянно проследяване на движението на потребителите на мобилни телефони (...)“ (решение от 6 октомври 2020 г. по съединени

**важността на целта от обществен интерес,** преследвана от това ограничение, е пропорционална на съответната тежест[19].

28. Според съдебната практика на Съда на ЕС при правно основание, позволяващо намеса в основните права, трябва да се определи обхватът на ограничението при упражняване на съответното право, за да се удовлетворят изискванията на принципа на пропорционалност[20]. Дерогациите и ограниченията на защитата на личните данни трябва да се въвеждат в границите на строго необходимото[21]. За да се изпълни това изискване, освен установяването на ясни и точни правила, регулиращи обхвата и прилагането на въпросната мярка, съответната правна уредба трябва да наложи минимални гаранции, така че лицата, чиито данни са били предадени, да имат достатъчни мерки за ефективната защита на личните си данни при възникване на риск от злоупотреба. „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[22].“

29. ЕКЗД прие Препоръки за определяне на основните гаранции в областта на надзора, които следва да са включени в законодателството на третата държава; тези препоръки отразяват съдебната практика на Съда на ЕС и на Европейския съд по правата на човека (ЕСПЧ) и могат да се използват при оценка на намесата на мерките за наблюдение на трети държави в правата на субектите на данни, в случай че данните се предават на третата държава съгласно ОРЗД[23]. За да се оцени дали са изпълнени условията на член 36, параграф 2, буква а) от ДП, ЕКЗД счита, че гаранциите, посочени в тези Препоръки, трябва да бъдат взети под внимание при оценката на адекватното ниво на защита на трета държава съгласно ДП по отношение на наблюдението, като се имат предвид наличието на допълнителни специфични условия.

30. Във връзка с изискването в член 36, параграф 2, буква б) третата държава следва не само да осигури ефективен независим надзор в областта на защитата на данните, но и да предвиди механизми за сътрудничество с органите за защита на данните на държавите членки [24].

31. Във връзка с изискването в член 36, параграф 2, буква в), освен международните ангажименти, които съответната трета държава или международна организация е поела, следва да се вземат под внимание и задълженията, произтичащи от участието на третата държава или международната организация в многостранни или регионални системи, по-конкретно по отношение на защитата на личните данни, както и изпълнението на такива задължения, по-специално присъединяването на третата държава към други международни споразумения за защита на данните; като например- Конвенцията на Съвета на Европа от 28 януари 1981 г. за защита на физическите лица по отношение на автоматичната обработка на лични данни и Допълнителният протокол към нея (Конвенция 108[25] и нейната осъвременена версия – Конвенция 108+). Съответствието на

дела C-511/18, C-512/18 и C-520/18, La Quadrature du Net и други, ECLI:EU:C:2020:791, точка 187, включително цитираната съдебна практика).

[19] La Quadrature du Net и други, точка 131.

[20] Schrems II, точка 180.

[21] Schrems II, точка 176, включително цитираната съдебна практика.

[22] Schrems II, точка 176, включително цитираната съдебна практика.

[23] Препоръки 02/2020 на ЕКЗД относно европейските основни гаранции при прилагане на мерки за наблюдение, приети на 10 ноември 2020 г.

[24] Съображение 67 от ДП.

[25] Съображение 68 от ДП.

третата държава с принципите, залегнали в международни документи, като Практическото ръководство на Съвета на Европа относно използването на лични данни в полицейския сектор: как да защитим личните данни при борба с престъпността, също може да бъде взето под внимание.

32. Решението за адекватно ниво на защита следва да гарантира, че чуждата система като цяло предоставя необходимото ниво на защита, включително по отношение на данните които се предоставят транзитно на третата държава чрез ефективното въвеждане, надзор и прилагане на правата за неприкосновеност на личния живот и защитата на данните. Както е подчертано от Съда на ЕС в решението по делото Schrems II, предоставяната висока степен на защита следва също да бъде гарантирана, докато данните се предават в трета държава.[26].

33. Накрая, при приемане на решение относно адекватното ниво на защита на личните данни само за територия или конкретен сектор в трета държава, Европейската комисия следва да вземе под внимание ясни и обективни критерии, като например позоваване на специфични дейности по обработване или обхвата на приложимите правни стандарти и на действащото законодателство в третата държава[27].

## A. Общи принципи и гаранции

**а) Понятия**

34. Следва да съществуват основни понятия за защита на данните. Не е необходимо те да съвпадат с терминологията според ДП, но трябва да отразяват понятията, заложени в европейското право в областта на защитата на данните, и да съответстват на тях. Например ДП включва следните важни дефиниции: „лични данни“, „обработване на лични данни“, „компетентни органи“, „администратор на лични данни“, „обработващ лични данни“, „получател“, „чувствителни данни“, „точност“, „профилиране“, „защита на данните на етапа на проектирането и по подразбиране“, „надзорен орган“ и „псевдонимизация“.

**б) Законосъобразност и добросъвестност на обработването на лични данни** (член 4 — съображение 26)

35. Съгласно член 8, параграф 2 от Хартата личните данни следва между другото 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“.[28] При правоприлагането обаче следва да се отбележи, че изпълнението на задачите по предотвратяване, разследване, разкриване или наказателно преследване на престъпления, институционално възложено със закон на компетентните органи, им позволява да изискват или нареждат на физическите лица да се съобразяват с направените искания. В този случай съгласието на субекта на данните не следва да предоставя правно основание за обработването на личните данни от компетентните органи[29].

[26] Вж. точка 93.
[27] Съображение 67 от ДП.
[28] Вж. Schrems II, точка 173.
[29] Съображение 35 от ДП също посочва, че „когато от субекта на данните се изисква да се съобрази с правно задължение, субектът на данните не разполага с истински и свободен избор, така че реакцията на субекта на данните не би могла да се счита за свободно изразяване на неговите желания. Това не следва да възпрепятства държавите членки да предвидят в националното си право, че субектът на данните може да даде съгласието си за обработване на неговите лични данни за целите на настоящата директива, като

36. Това правно основание трябва да определя ясни и точни правила, регулиращи обхвата и прилагането на съответните дейности по обработването на данни и налагащи минимални гаранции[30]. В допълнение Съдът на ЕС напомня, че „правната уредба трябва да бъде правно обвързваща съгласно вътрешното законодателство“[31].

37. За да бъде законосъобразно, обработването на лични данни[32] следва да бъде необходимо за изпълнението на задача от компетентен орган за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване.[33] Тези цели трябва да бъдат предвидени в националното законодателство.

38. Личните данни да се обработват добросъвестно. Принципът за добросъвестно обработване във връзка със защитата на данните е различно понятие от правото на справедлив съдебен процес, както е предвидено в член 47 от Хартата и в член 6 от Европейската конвенция за защита на правата на човека и основните свободи (ЕКПЧ)[34].

**в) Принцип на ограничаване в рамките на целта** (член 4)

39. Конкретните цели, за които се обработват личните данни, следва да бъдат изрично указани и легитимни, и определени към момента на събирането на личните данни[35].

40. Данните следва да се обработват за конкретна, изрично указана и легитимна цел в рамките на целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания[36], включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване в третата държава, както и последващото използване за някоя от тези цели, стига това да не е

например данни от ДНК тестове в рамките на наказателни разследвания или наблюдение на местоположението на субекта на данни посредством електронен уред при изпълнението на наказания.“

[30] Вж. Schrems II, точка 175 и точка 180 и Становище 1/15, точка 139, както и цитираната съдебна практика.

[31] Вж. решение от 6 октомври 2020 г., Privacy International срещу Secretary of State for Foreign and Commonwealth Affairs and Others, C-623/17, ECLI:EU:C:2020:790, точка 68. Следва също да е ясно, че във френската версия на решението Съдът на ЕС използва думата „*réglementation*“ чийто смисъл е по-широк от просто „актове на Парламента“.

[32] Обработване на лични данни изцяло или частично с автоматични средства, както и обработване с други средства за лични данни, които са част от регистър с лични данни или са предназначени да съставляват част от такъв регистър.

[33] Компетентен орган е всеки публичен орган, който е компетентен за такива цели, или всеки друг орган или образувание, което по силата на правото упражнява публична власт и публични правомощия за такива целите.

[34] Съображение 26 от ДП.

[35] Съображение 26 от ДП.

[36] Включва „полицейски дейности, без предварително да е известно дали даден инцидент съставлява престъпление или не. Тези дейности могат да включват упражняване на правомощия чрез предприемане на принудителни мерки, като полицейски дейности по време на демонстрации, големи спортни събития и безредици. Те включват и поддържането на законността и реда като задача, възложена на полицията или други правоприлагащи органи, когато е необходимо да се вземат предпазни мерки и да се предотвратят заплахи за обществената сигурност и основните интереси на обществото, защитени от закона, които могат да доведат до извършването на престъпление“ (съображение 12 от ДП). Трябва да се разграничи от целите на националната сигурност или от дейности, които попадат в обхвата на глава 2 от дял V от Договора за Европейския съюз (ДЕС) (съображение 14 от ДП).

несъвместимо с първоначалната цел на обработването (например за паралелни производства за принудително изпълнение или архивиране в обществен интерес, използване за научни, статистически или исторически цели), и при прилагането на подходящи гаранции за правата и свободите на субектите на данните. Ако лични данни се обработват от същия или друг администратор (компетентен орган[37]) с цел предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, като целта е различна от тази, за която данните са били събрани, това обработване следва да е допустимо, при условие че е разрешено в съответствие с приложимите правни разпоредби и е необходимо и пропорционално на тази друга цел[38]. Наличието на механизъм за информиране на компетентните органи на съответните държави членки за последващо обработване на данни следва също да бъде взето под внимание[39]. Освен това, във всички случаи нивото на защита на физическите лица, предвидено в Съюза с ДП, не следва да бъде застрашено, включително в случаите на предаване на лични данни от третата държава на администратори или обработващи лични данни в същата трета държава.[40].

**г) Специфични условия за последващо обработване за други цели** (член 9)

41. По отношение на последващото обработване или разкриване на данни, предавани от ЕС за цели, различни от тези на правоприлагането, например целите на националната сигурност, то също следва да бъде предвидено в закона като необходимо и пропорционално. Наличието на механизъм за информиране на компетентните органи на съответните държави членки за последващо обработване на данни следва също да бъде взето под внимание[41]. И тук след последващо обработване или разкриване данните трябва да се ползват от същото ниво на защита, както при първоначалното обработване от получаващия компетентен орган.

**д) Принцип за свеждане на данните до минимум**

42. Данните следва да са подходящи, относими и да не надхвърлят необходимото във връзка с целите, за които се обработват. По-конкретно, следва да се вземе под внимание прилагането на изискванията за защита на данните на етапа на проектирането и по подразбиране, като ограничени полета за въвеждане (структурирани съобщения) или автоматични и неавтоматични проверки на качеството.

**е) Принцип за точност на данните**

43. Данните следва да бъдат точни и при необходимост редовно да се актуализират. Принципът за точност на данните все пак трябва да се прилага, като се вземат предвид естеството и целта на съответното обработване. Особено в съдебни производства, изявления, съдържащи лични данни, се основават на субективното възприемане от физически лица и не могат винаги да бъдат проверени. По тази причина изискването за точност не следва да

[37] Вж. бележка под линия 33.
[38] Съображение 29 от ДП.
[39] Такъв механизъм може за бъде например взаимно съгласувани кодове за обработване, задължение за уведомяване съгласно международен инструмент, включително евентуални автоматични уведомления или други сходни мерки за прозрачност.
[40] Съображение 64 от ДП.
[41] Вж. бележка под линия 39.

се отнася за точността на изявлението, а само за факта, че е направено конкретно изявление[42].

44. Следва да се гарантира, че лични данни, които са неточни, непълни или които вече не са актуални, не се предават или предоставят[43] и че са предвидени процедури за поправяне или заличаване на неточни данни. По-конкретно, трябва да се вземе под внимание всяка система за класифициране на обработената информация по отношение на надеждността на източника и на нивото на проверка на фактите[44].

**ж) Принцип на запазване на данни**

45. Данните следва да се съхраняват не повече от необходимото за целите, за които се обработват. Следва да бъдат създадени подходящи механизми за изтриване на лични данни. Може да бъде определен период или периодичен преглед на нуждата от съхраняване на лични данни (или комбинация от двете: определен максимален период и периодичен преглед през определени интервали)[45]. Личните данни, съхранявани за по-дълги периоди за целите на архивирането в обществен интерес и за използването с научен, статистически или исторически характер, трябва да бъдат обект на подходящи гаранции (например по отношение на достъпа)[46].

**з) Принцип на сигурност и поверителност** (член 29, съображения 28 и 71)

46. Всяко юридическо лице, което обработва лични данни, следва да гарантира, че данните се обработват по начин, който гарантира степен на сигурност на личните данни, включително чрез предотвратяване на непозволен достъп или използване на лични данни и на оборудването за тяхното обработване. Това включва защита срещу и подходящи мерки за справяне с неразрешено или незаконосъобразно обработване, както и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически и организационни мерки. Когато се определя нивото на сигурност, трябва да бъдат взети предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, същността и целите на обработването, както и породеният от обработването риск с различна вероятност и тежест за правата и свободите на физическите лица.

47. Следва да се осигурят сигурни канали за комуникация между органите на държавите членки, които предават личните данни, и получаващите органи на трети държави.

**и) Принцип на прозрачността** (член 13, съображения 26, 39, 42, 43, 44, 46)

48. Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на личните им данни, и за начините, по които да упражняват правата си по отношение на обработването[47].

49. На физическите лица трябва да бъде предоставена информация относно всички основни елементи на обработването на личните им данни. Информацията следва да бъде лесно

[42] Съображение 30 от ДП.
[43] Съображение 32 от ДП.
[44] Например таблици 4x4 за оценка на надеждността и кодовете за обработване.
[45] Член 5 от ДП.
[46] Съображение 26 от ДП.
[47] Съображение 26 от ДП.

достъпна и разбираема, като се използва ясен и прост език. Тази информация следва да включва целта на обработването, идентичността на администратора на данни, правата, които са му предоставени[48], и друга информация, доколкото това е необходимо, за да се гарантира добросъвестността.

50. Възможно е да съществуват някои изключения от правото на информиране. Подобно ограничение обаче следва да бъде разрешено от законодателна мярка и да бъде необходимо и пропорционално, така че да се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури, да се избегне засягане на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, или изпълнението на наказания, да се защитят обществената или националната сигурност или правата и свободите на други лица, стига такова частично или пълно ограничение да представлява необходима или пропорционална мярка в демократично общество, което зачита надлежно основните права и законните интереси на съответното физическо лице. Подобни ограничения следва също да бъдат разглеждани и оценени, като се вземе предвид възможността за подаване на жалба до надзорен орган или търсенето на средство за правна защита. Във всеки случай всяко евентуално ограничение следва да бъде временно, а не общо и да бъде разписано, подобно на условията, гаранциите и ограниченията, изискани съгласно Хартата и ЕКПЧ, според тълкуването в съдебната практика на Съда на ЕС и съответно на ЕСПЧ, и по-конкретно да зачита същността на заложените права и свободи.

**й) Право на достъп, коригиране и изтриване** (членове 14 и 16)

51. Субектът на данни следва да има право да получи потвърждение относно това дали се обработват данни за него или не, и ако това е така, да получи достъп до тях. Това право следва да включва поне определена информация за обработването, като целите и правното основание за него, правото да се подаде жалба до надзорния орган или обработваните категории лични данни[49]. Това е изключително важно, в случай че прозрачността се постига чрез общо известие (например информация на уебсайта на органа).

52. Субектът на данни следва да има право да поиска коригиране на своите данни поради определени причини, когато се окаже например, че те са неточни или непълни. Субектът на данни също трябва да има право на изтриване на своите данни, когато например тяхната обработка вече не е необходима или законна.

53. Упражняването на тези права не следва да бъде прекалено трудно за субекта на данни.

**к) Ограничения на правата на субекта на данни**

54. Могат да съществуват евентуални ограничения на тези права, за да се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури, да се избегне засягане на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, или изпълнението на наказания, да се защитят обществената или националната сигурност или правата и свободите на други лица, стига такова частично или пълно ограничение да представлява необходима или пропорционална мярка в демократично общество, което зачита надлежно основните права и законните интереси на съответното физическо лице. Подобни ограничения следва също

[48] Както материалните права (право на достъп, коригиране и др.), така и правото на правна защита.
[49] Член 14 от ДП.

да бъдат разглеждани и оценени, като се вземе предвид възможността за подаване на жалба до надзорния орган или търсенето на средство за правна защита.

**л) Ограничение на последващо предаване** (член 35, съображения 64-65)

55. Последващото предаване на лични данни от първоначалния получател до друга трета държава или международна организация не трябва да подкопава нивото на защита на физическите лица, чиито данни се предават, предвидено в Съюза. Поради това, подобно последващо предаване на данни следва да бъде разрешено само там, където е осигурена приемственост на нивото на защита, предоставено съгласно законодателството на ЕС [50]. По-конкретно, последващият получател (т.е. получателят на последващото предаване) трябва да бъде компетентен правоприлагащ орган[51], като всяко последващо предаване на данни може да се извършва единствено за ограничени и конкретни цели, и стига да има правно основание за него.

56. Наличието на механизъм за информиране на компетентните органи на съответната държава членка и за разрешаването на такова последващо предаване на данни също трябва да бъде взето под внимание. Първоначалният получател на данните, предадени от ЕС, следва да носи отговорност и да може да докаже, че съответният компетентен орган на държавата членка е разрешил последващото предаване[52], както и че са предвидени подходящи гаранции за последващия трансфер на данни при липса на решение относно адекватното ниво на защита по отношение на третата държава, към която данните биха били предадени[53].

**м) Принцип на отчетността** (член 4, параграф 4)

57. Администраторът носи отговорност за спазването на принципите за защита на данните, установени в член 4 от ДП.

[50] Вж. също Становище 1/15.
[51] Вж. бележка под линия 33.
[52] В тази връзка трябва да се вземе под внимание наличието на задължение или ангажимент за прилагането на съответните кодове за обработване, определени от органите на предаващите държави членки.
[53] Изискванията по-горе не засягат специфичните условия за последващо предаване до държава с адекватно ниво на защита, предвидени съгласно ДП (член 35, параграф 1, букви в) и д).

## Б. Примери за допълнителни принципи, които трябва да се прилагат при специфични видове обработване

**а) Специални категории данни** (член 10 и съображение 37)

58. Когато се касае за „специални категории данни“, трябва да има специфични гаранции[54], свързани с включените специфични рискове[55]. Тези категории данни следва да отразяват категориите, заложени в член 10 от ДП. Поради това обработването на специални категории данни следва да бъде предмет на специфични гаранции и да бъде разрешено, когато това е строго необходимо, при определени условия, например за защита на жизненоважни интереси на субекта на данните.

**б) Автоматично вземане на решения и профилиране** (член 11 и съображение 38)

59. Решения, основани единствено на автоматично обработване (автоматично вземане на индивидуални решения), включително профилиране, които пораждат неблагоприятни правни последици или сериозно засягат субекта на данните, следва да се вземат само при определени условия, установени в правната уредба на третата държава[56].

60. В правната уредба на Европейския съюз такива условия включват например предоставянето на конкретна информация на субекта на данните и правото на човешка намеса от страна на администратора, по-специално, за изразяване на неговото мнение, за получаване на обяснение за решението, взето в резултат на такава оценка и за обжалване на решението.

61. Във всеки случай законодателството на третата държава следва да предвижда необходимите гаранции за правата и свободите на субекта на данните. В тази връзка следва също да бъде взето под внимание наличието на механизъм за информиране на компетентните органи на съответните държави членки за последващо обработване, като например използването на предадените данни за широкомащабно профилиране.

**в) Защита на данните на етапа на проектирането и по подразбиране** (член 20)

62. Когато се оценява адекватното ниво на защита, следва да се вземе предвид наличието на задължение на администраторите да приемат вътрешни политики и да приложат мерки, които се придържат към принципите на защитата на данните на етапа на проектирането и по подразбиране, като отчитат достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове с различна вероятност и тежест за правата и свободите както към момента на определянето на средствата за обработването на данни, така и към момента на самото обработване, а така също и да приемат подходящи технически и организационни мерки, например псевдонимизация, разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и да интегрират необходимите гаранции в процеса на обработване.

[54] Тези специални категории данни са наречени също така „чувствителни данни“ в съображение 37 от ДП.
[55] Такива допълнителни гаранции могат да бъдат например специфични мерки за сигурност, ограничени права на достъп на персонала, ограничения по отношение на последващото обработване, автоматично вземане на решения, последващо споделяне или последващо предаване.
[56] Становище 1/15, точка 173.

## B. Процедури и правоприлагащи механизми

63. Въпреки че средствата, до които третата държава има достъп, за да гарантира адекватно ниво на защита, може да се различават от използваните в рамките на Европейския съюз[57], за да отговаря системата на европейската, в нея трябва да са заложени следните елементи:

**а) Компетентен независим надзорен орган** (член 36, параграф 2, точка б) и член 36, параграф 3 и съображение 67)

64. Следва да съществуват един или повече независими надзорни органи, натоварени с гарантиране и осигуряване на спазването на разпоредбите за защита на данните и неприкосновеността на личния живот в третата държава. Надзорният орган трябва да действа изцяло независимо и безпристрастно при изпълнението на задачите и упражняването на правомощията си, като в тази връзка няма нито да търси, нито да приема инструкции. Предвид това, надзорният орган следва да разполага с всички адекватни изпълнителни правомощия, за да се гарантира спазването на правата за защита на данните и да се насърчава осведомеността. Желателно е да се обърне внимание също и на персонала, и на бюджета на надзорния орган. Надзорният орган трябва да може също така да извършва проучвания по собствена инициатива. Следва също да бъде му бъде възложена задачата да подпомага и да съветва субекти на данни при упражняването на техните права (вж. също буква в) по-долу). В решенията относно адекватното ниво на защита трябва да се определят, когато е приложимо, надзорният орган или надзорните органи и механизмите за сътрудничество с надзорните органи на държавите членки при прилагане на правилата за защита на данните.

**б) Ефективно въвеждане на правила за защита на данните**

65. Системата на третата държава следва да гарантира висока степен на осведоменост на администраторите и обработващите лични данни по отношение на техните задължения, задачи и отговорности, както и на субектите на данни относно техните права и средствата за упражняването им. Наличието на ефективни и възпиращи санкции може да има важна роля за осигуряването на спазването на правилата, като такава роля могат да имат и системите за пряка проверка от органи, одитори или независими длъжностни лица, отговарящи за защитата на данните.

66. Рамката за защита на данните на третата държава следва да задължава администраторите или обработващите лични данни да я спазват и да могат да докажат, че я спазват, по-специално, пред компетентния надзорен орган. Подобни мерки следва да включват съхраняване на записи или регистрационни файлове за дейности по обработването на данни за подходящ период от време. Те могат също да включват например оценки на въздействието на защитата на данните, назначаването на длъжностно лице по защита на данните или защитата на данните на етапа на проектирането и по подразбиране.

**в) Системата за защита на данните трябва да улеснява упражняването на правата на субектите на данни** (членове 12, 17 и 46 от ДП)

67. Правната уредба за защита на данните на третата държава следва да задължава администраторите на лични данни да улесняват упражняването на правата на субектите на

[57] Schrems I, точка 74.

данни, посочени в раздел А, буква й) по-горе, и да предвижда нейният надзорен орган да информира при поискване всеки субект на данни относно упражняването на неговите права[58].

**г) Системата за защита на данните трябва да осигурява подходящи механизми за правна защита**

68. Въпреки че понастоящем няма съдебна практика по отношение на адекватността на правната система на трета държава съгласно ДП, Съдът на ЕС тълкува основното право на ефективна съдебна защита според заложеното в член 47 от Хартата. В член 47, първа алинея от Хартата се 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[59] в съответствие с предвидените в този член условия.

69. Съгласно установената съдебна практика на Съда на ЕС 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. По този начин законодателство, което не предвижда възможността на дадено лице да използва правни средства за защита за достъп до отнасящи се до него лични данни или да му бъде осигурено коригиране или изтриване на такива данни, не зачита същността на основното право на ефективна съдебна защита според заложеното в член 47 от Хартата[60].

70. Физическото лице следва да може да използва средства за правна защита, за да упражни правата си бързо и ефективно и без възпиращи разходи, както и за да се гарантира спазване на правилата.

71. За тази цел трябва да има механизми за надзор, позволяващи независимо разследване по жалбите и установяване, и реално санкциониране на всяко нарушение на правото на защита на данните, и на зачитане на неприкосновеността на личния живот.

72. Когато правилата не се спазват, субектът на данни, чиито лични данни са предадени на трета държава, следва да разполага също така с ефективни административни и съдебни средства за защита в третата държава, включително за обезщетение за вреди в резултат на незаконосъобразно обработване на неговите лични данни. Това е ключов елемент, който трябва да включва система за независимо отсъждане или арбитраж, даваща възможност за изплащането на компенсация и, по целесъобразност, налагането на санкции.

[58] Упражняването на правата на субектите на данни може да бъде пряко или непряко.
[59] Съдът на ЕС счита, че ефективна съдебна защита може да бъде осигурена не само от съд, но и от орган, който предлага гаранции, по същество равностойни на тези, изисквани от член 47 от Хартата (вж. Schrems II, точка 197). Това може да е от значение по-специално за международните организации.
[60] Schrems II, точки 187 и 194, включително цитираната съдебна практика.