РЕГЛАМЕНТ (ЕС) 2018/1725 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 23 октомври 2018 година

относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО

(Текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 16, параграф 2 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет ([1]),

в съответствие с обикновената законодателна процедура ([2]),

като имат предвид, че:

(1) Защитата на физическите лица във връзка с обработването на лични данни е основно право. Член 8, параграф 1 от Хартата на основните права на Европейския съюз („Хартата“) и член 16, параграф 1 от Договора за функционирането на Европейския съюз (ДФЕС) предвиждат, че всеки има право на защита на своите лични данни. Това право е гарантирано също така от член 8 от Европейската конвенция за защита правата на човека и основните свободи.

(2) Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета ([3]) осигурява на физическите лица гарантирани от закона права, определя свързаните с обработването на данни задължения на администраторите в рамките на институциите и органите на Общността и създава независим надзорен орган, Европейския надзорен орган по защита на данните, който отговаря за наблюдението на обработването на лични данни от институциите и органите на Съюза. Той не се прилага обаче за обработването на лични данни при извършването на дейност на институциите и органите на Съюза, попадаща извън обхвата на правото на Съюза.

(3) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета ([4]) и Директива (ЕС) 2016/680 на Европейския парламент и на Съвета ([5]) бяха приети на 27 април 2016 г. Докато в регламента се установяват общи правила за защита на физическите лица във връзка с обработването на лични данни и за гарантиране на свободното движение на лични данни в рамките на Съюза, с директивата се установяват специални правила за защита на физическите лица във връзка с обработването на лични данни и за гарантиране на свободното движение на лични данни в рамките на Съюза в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество.

(4) В Регламент (ЕС) 2016/679 се предвижда адаптирането на Регламент (ЕО) № 45/2001, за да се осигури силна и съгласувана рамка за защита на данните в Съюза и да се даде възможност за едновременното му прилагането с Регламент (ЕС) 2016/679.

(5) Привеждането, доколкото е възможно, на правилата относно защитата на данните от страна на институциите, органите, службите и агенциите на Съюза в съответствие с правилата относно защита на данните, приети за публичния сектор в държавите членки, е в интерес както на постигането на съгласуван подход към защитата на личните данни навсякъде в Съюза, така и на свободното движение на лични данни навсякъде в Съюза. Когато разпоредбите на настоящия регламент следват същите принципи като разпоредбите на Регламент (ЕС) 2016/679,

([1]) ОВ C 288, 31.8.2017 г., стр. 107.

([2]) Позиция на Европейския парламент от 13 септември 2018 г. (все още непубликувана в Официален вестник) и решение на Съвета от 11 октомври 2018 г.

([3]) Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1).

([4]) Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

([5]) 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 (ОВ L 119, 4.5.2016 г., стр. 89).

тълкуването на тези две групи от разпоредби, съгласно практиката на Съда на Европейския съюз („Съда“), следва да бъде еднообразно, по-специално защото структурата на настоящия регламент следва да се разбира като еквивалентна на структурата на Регламент (ЕС) 2016/679.

(6) Лицата, чиито лични данни се обработват от институциите и органите на Съюза в някаква връзка, например поради това, че са служители на тези институции и органи, следва да бъдат защитени. Настоящият регламент не следва да се прилага за обработването на лични данни на починали лица. Настоящият регламент не обхваща обработването на лични данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и данните за връзка на юридическото лице.

(7) За да се избегне създаването на сериозен риск от заобикаляне на закона, защитата на физическите лица следва да бъде технологично неутрална и следва да не зависи от използваната техника.

(8) Настоящият регламент следва да се прилага за обработването на лични данни от всички институции, органи, служби и агенции на Съюза. Той следва да 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 са предназначени да съставляват част от регистър с лични данни. Досиетата или групите от досиета, както и заглавните им страници, които не са структурирани съгласно специфични критерии, не следва да попадат в обхвата на настоящия регламент.

(9) В Декларация № 21 относно защитата на личните данни в областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество, приложена към заключителния акт на Междуправителствената конференция, която прие Договора от Лисабон, конференцията признава, че биха могли да са необходими специални правила относно защитата на личните данни и относно свободното движение на лични данни в областите на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество въз основа на член 16 от ДФЕС поради специфичното естество на тези области. Ето защо отделна глава от настоящия регламент, съдържаща общи правила, следва да се прилага за обработването на лични данни от оперативен характер, като например лични данни, обработвани за целите на наказателното разследване от органи, служби или агенции на Съюза при извършването на дейности в областите на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество.

(10) С Директива (ЕС) 2016/680 се установяват хармонизирани правила за защитата и свободното движение на личните данни, обработвани за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или на изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване. С цел да се осигури еднакво ниво на защита на физическите лица чрез гарантирани от закона права навсякъде в Съюза и да се предотвратят различията, възпрепятстващи обмена на лични данни между органите, службите или агенциите на Съюза при извършването на дейности, попадащи в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС, и компетентните органи, правилата за защитата и свободното движение на лични данни от оперативен характер, обработвани от тези органи, служби или агенции на Съюза, следва да бъдат в съответствие с Директива (ЕС) 2016/680.

(11) Общите правила на главата от настоящия регламент, отнасяща се до обработването на лични данни от оперативен характер, следва да се прилагат, без да се засягат специалните правила относно обработването на лични данни от оперативен характер от органите, службите или агенциите на Съюза при извършването на дейности, попадащи в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС. Тези специални правила следва да се разглеждат като lex specialis по отношение на разпоредбите в главата от настоящия регламент, отнасяща се до обработването на лични данни от оперативен характер (lex specialis derogat legi generali). С цел да се намали правната разпокъсаност, специалните правила относно обработването на лични данни от оперативен характер от органите, службите или агенциите на Съюза при извършването на дейности, попадащи в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС, следва да бъдат съгласувани с принципите, залегнали в основата на главата от настоящия регламент, отнасяща се до обработването на лични данни от оперативен характер, както и с разпоредбите на настоящия регламент, отнасящи се до независимия надзор, средствата за правна защита, отговорността за причинени вреди и санкциите.

(12) Главата от настоящия регламент, отнасяща се до обработването на лични данни от оперативен характер, следва да се прилага към органите, службите и агенциите на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС, независимо дали те упражняват тези дейност като свои основни или допълнителни задачи за целите на предотвратяването, разкриването, разследването или наказателното преследване на престъпления. Тя обаче не следва да се прилага за Европол или за Европейската прокуратура, докато правните актове за създаване на Европол и Европейската прокуратура не бъдат изменени с оглед въвеждането, със съответните адаптации, на глава в настоящия регламент, отнасяща се до обработването на лични данни от оперативен характер„ приложима по отношение на тях.

(13) Комисията следва да извърши преглед на настоящия регламент, по-специално на главата от настоящия регламент, отнасяща се до обработването на лични данни от оперативен характер. Комисията следва да извърши преглед и на други правни актове, приети въз основа на Договорите, които уреждат обработването на лични данни от оперативен

характер от органите, службите или агенциите на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС. След такъв преглед, с цел да се гарантира единна и съгласувана защита на физическите лица във връзка с обработването на лични данни, Комисията следва да може да прави всякакви подходящи законодателни предложения, включително необходимите адаптации на главата от настоящия регламент, отнасяща се до обработването на личните данни от оперативен характер, с оглед нейното прилагане по отношение на Европол и Европейската прокуратура. Адаптациите следва да бъдат съобразени с разпоредбите относно независимия надзор, средствата за правна защита, отговорността за причинени вреди и санкциите.

(14) Настоящият регламент следва да обхваща обработването на лични данни от административен характер, като например данни за персонала, обработвани от органите, службите или агенциите на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС.

(15) Настоящият регламент следва да се прилага за обработването на лични данни от институциите, органите, службите или агенциите на Съюза при извършването на дейности, които попадат в обхвата на дял V, глава 2 от Договора за Европейския съюз (ДЕС). Настоящият регламент не следва да се прилага за обработването на лични данни от мисиите, посочени в член 42, параграф 1 и членове 43 и 44 от ДЕС, които осъществяват общата политика за сигурност и отбрана. Когато е целесъобразно, следва да се представят подходящи предложения за по-нататъшно регламентиране на обработването на личните данни в областта на общата политика за сигурност и отбрана.

(16) Принципите за защита на данните следва да се прилагат по отношение на всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано. Личните данни, които са били подложени на псевдонимизация, които могат да бъдат свързани с дадено физическо лице чрез използването на допълнителна информация, следва да се считат за информация, отнасяща се до физическо лице, което може да бъде идентифицирано. За да се определи дали дадено физическо лице може да бъде идентифицирано, следва да се вземат предвид всички средства, като например подбирането на лица за извършване на проверка, с които е най-вероятно да си послужи администраторът или друго лице, за да идентифицира пряко или непряко даденото физическо лице. За да се уточни дали има разумна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като например разходите и времето, необходими за идентифицирането, като се отчитат както наличните към момента на обработване на данните технологии, така и тяхното развитие. Поради това принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, а именно информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на лични данни, които са анонимизирани по такъв начин, че субектът на данните вече не може да бъде идентифициран. Ето защо настоящият регламент не се отнася до обработването на такава анонимна информация, включително за статистически или изследователски цели.

(17) Прилагането на псевдонимизация на личните данни може да намали рисковете за съответните субекти на данни и да помогне на администраторите и на обработващите лични данни да изпълняват своите задължения за защита на данните. Изричното въвеждане на псевдонимизация в настоящия регламент не е предназначено да изключи други мерки за защита на данните.

(18) Физическите лица могат да бъдат свързани с онлайн идентификатори, предоставени от техните устройства, приложения, инструменти и протоколи, като адресите по интернет протокол (IP адреси) или идентификаторите, наричани „бисквитки“, или други идентификатори, например етикетите за радиочестотна идентификация. По този начин може да бъдат оставени следи, които в съчетание по-специално с уникални идентификатори и с друга информация, получена от сървърите, може да се използват за създаването на профили на физическите лица и за тяхното идентифициране.

(19) Съгласие следва да се дава чрез ясно утвърдителен акт, с който да се изразява свободно дадено, конкретно, информирано и недвусмислено заявление за съгласие от страна на субекта на данни за обработване на свързани с него лични данни, например чрез писмена декларация, включително по електронен път, или устна декларация. Това може да включва отбелязване с отметка в поле при посещението на уебсайт в интернет, избиране на технически настройки за услуги на информационното общество или друго заявление или поведение, което ясно показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Поради това мълчанието, предварително отметнатите полета или липсата на действие не следва да представляват съгласие. Съгласието следва да обхваща всички дейности по обработване, извършени за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях следва да бъде дадено съгласие. Ако съгласието на субекта на данни трябва да се даде след искане по електронен път, искането трябва да е ясно, сбито и да не нарушава излишно използването на услугата, за която се предвижда. Същевременно субектът на данните следва да има правото да оттегли съгласието си по всяко време, без това да засяга законосъобразността на обработката на данните, основаваща се на съгласие преди неговото оттегляне. За да се гарантира, че е дадено свободно, съгласието не следва да представлява валидно правно основание за обработването на лични данни в конкретна ситуация, когато е налице очевидна неравнопоставеност между субекта на данните и администратора и поради това изглежда малко вероятно съгласието да е дадено свободно предвид всички

обстоятелства на конкретната ситуация. Често в момента на събиране на данните целта на обработването на лични данни за научноизследователски цели не може да бъде напълно установена. Поради това на субектите на данни следва да бъде дадена възможност да дадат съгласието си за определени области на научни изследвания, когато те са в съответствие с признатите етични норми, отнасящи се за научните изследвания. Субектите на данни следва да имат възможност да дадат съгласието си само за определени области на научни изследвания или части от научноизследователски проекти, доколкото позволява набелязаната цел.

(20) Всяко обработване на лични данни следва да бъде законосъобразно и добросъвестно. За физическите лица следва да е прозрачно по какъв начин отнасящи се до тях лични данни се събират, използват, консултират или обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данните. Принципът на прозрачност изисква всяка информация и комуникация във връзка с обработването на тези лични данни да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки. Този принцип се отнася в особена степен за информацията, която получават субектите на данни за самоличността на администратора и целите на обработването, и за допълнителната информация, гарантираща добросъвестно и прозрачно обработване на данните по отношение на засегнатите физически лица и тяхното право да получат потвърждение и уведомление за съдържанието на свързани с тях лични данни, които се обработват. Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни, и за начините, по които да упражняват правата си по отношение на обработването. По-специално конкретните цели, за които се обработват лични данни, следва да бъдат ясни и законни и определени към момента на събирането на личните данни. Личните данни следва да са адекватни, релевантни и ограничени до необходимото за целите, за които се обработват. Това налага по-специално да се гарантира, че срокът, за който личните данни се съхраняват, е ограничен до строг минимум. Личните данни следва да се обработват, единствено ако целта на обработването не може да бъде постигната в достатъчна степен с други средства. С цел да се гарантира, че срокът на съхранение на личните данни не е по-дълъг от необходимия, администраторът следва да установи срокове за тяхното изтриване или периодичен преглед. Следва да бъдат предприети всички разумни мерки, за да се гарантира, че неточните лични данни се коригират или заличават. Личните данни следва да се обработват по начин, който гарантира подходяща степен на сигурност и поверителност на личните данни, включително за предотвратяване на непозволен достъп до лични данни или на тяхното използване и на оборудването за тяхното обработване, и за предотвратяване на неразрешеното им разкриване, когато те бъдат предавани.

(21) В съответствие с принципа на отчетност, когато институциите и органите на Съюза предават лични данни в рамките на същата институция или орган на Съюза и получателят не е част от администратора, или на други институции или органи на Съюза, те следва да проверяват дали тези лични данни са необходими за законосъобразното изпълнение на задачи в рамките на компетентността на получателя. По-специално, след искане на получател за предаване на лични данни, администраторът следва да удостовери наличието на съответно основание за законосъобразно обработване на лични данни от получателя, както и неговата компетентност. Администраторът следва също да извърши предварителна оценка на необходимостта от предаването на данните. В случай на възникнали съмнения относно тази необходимост администраторът следва да изисква допълнителна информация от получателя. Получателят следва да гарантира, че необходимостта от предаване на данните може да бъде впоследствие проверена.

(22) За да бъде обработването законосъобразно, личните данни следва да бъдат обработвани въз основа на необходимостта от изпълнение на задача от обществен интерес от страна на институции и органи на Съюза или при упражняването на техните официални правомощия, необходимостта от спазване на правно задължение, наложено на администратора на лични данни, или на друго законно основание съгласно настоящия регламент, включително съгласието на субекта на данни, необходимостта от изпълнение на договор, по който субектът на данни е страна, или с оглед предприемане на стъпки по искане на субекта на данни преди встъпване в договорни отношения. Обработването на лични данни за изпълнението на задачи от обществен интерес от страна на институции и органи на Съюза включва обработването на лични данни, които са необходими за управлението и функционирането на тези институции и органи. Обработването на лични данни следва да се счита за законосъобразно и когато е необходимо, за да се защити интерес от първостепенно значение за живота на субекта на данните или на друго физическо лице. Обработването на лични данни единствено въз основа на жизненоважен интерес на друго физическо лице следва да се състои по принцип само когато обработването не може явно да се базира на друго правно основание. Някои видове обработване могат да обслужват както важни области от обществен интерес, така и жизненоважните интереси на субекта на данните, например когато обработването е необходимо за хуманитарни цели, включително за наблюдение на епидемии и тяхното разпространение, или при спешни хуманитарни ситуации, по-специално в случай на природни или причинени от човека бедствия.

(23) Правото на Съюза, посочено в настоящия регламент, следва да бъде ясно и точно и прилагането му следва да бъде предвидимо за лицата, за които се прилага, в съответствие с изискванията, определени в Хартата и в Европейската конвенция за защита на правата на човека и основните свободи.

(24) Вътрешните правила, посочени в настоящия регламент, следва да бъдат ясни и точни актове с обща приложимост, които са предназначени да породят правни последици по отношение на субектите на данни. Те следва да бъдат приети на най-високото равнище на управление на институциите и органите на Съюза в рамките на тяхната компетентност и да се отнасят до въпроси, свързани с тяхното функциониране. Те следва да бъдат публикувани в *Официален вестник на Европейския съюз*. Прилагането на тези правила следва да бъде предвидимо за лицата, които са техни адресати, в съответствие с изискванията, определени в Хартата и в Европейската конвенция за защита на правата на човека и основните свободи. Вътрешните правила могат да бъдат под формата на решения, по-специално когато се приемат от институции на Съюза.

(25) Обработването на лични данни за цели, различни от тези, за които първоначално са събрани личните данни, следва да бъде разрешено единствено когато обработването е съвместимо с целите, за които първоначално са събрани личните данни. В такъв случай не се изисква отделно правно основание, различно от това, с което е било разрешено събирането на личните данни. Ако обработването е необходимо за изпълнението на задача от обществен интерес или свързана с упражняването на официални правомощия, които са предоставени на администратора, в правото на Съюза могат да бъдат определени и уточнени задачите и целите, за които по-нататъшното обработване следва да се счита за съвместимо и законосъобразно. По-нататъшното обработване за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели следва да се разглежда като съвместима законосъобразна операция по обработване. Правното основание, предвидено от правото на Съюза за обработване на лични данни, може да предостави и правно основание за по-нататъшно обработване. За да установи дали дадена цел на по-нататъшно обработване е съвместима с целта, за която първоначално са събрани личните данни, администраторът на лични данни, след като е спазил всички изисквания относно законосъобразността на първоначалното обработване, следва да отчете, *inter alia*: всички връзки между тези цели и целите на предвиденото по-нататъшно обработване; в какъв контекст са събрани личните данни, по-специално основателните очаквания на субектите на данните въз основа на техните взаимоотношения с администратора по отношение на по-нататъшно използване на личните данни; естеството на личните данни; последствията от предвиденото по-нататъшно обработване на данни за субектите на данни; и наличието на подходящи гаранции при операциите по първоначалното и предвиденото по-нататъшно обработване.

(26) Когато обработването се извършва въз основа на съгласието на субекта на данните, администраторът следва да може да докаже, че субектът на данните е дал съгласието си за операцията по обработване. По-специално, в случай на писмена декларация по друг въпрос, с гаранциите следва да се обезпечи, че субектът на данни е информиран за това, че дава съгласието си, и в каква степен го дава. В съответствие с Директива 93/13/ЕИО на Съвета ([1]) следва да бъде осигурена предварително съставена от администратора декларация за съгласие в разбираема и лесно достъпна форма, на ясен и прост език, която не следва да съдържа неравноправни клаузи. За да бъде съгласието информирано, субектът на данни следва да знае поне самоличността на администратора и целите на обработването, за което са предназначени личните данни. Съгласието не следва да се разглежда като свободно дадено, ако субектът на данни няма истински и свободен избор и не е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

(27) На децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на лични данни. Тази специална защита следва да се прилага по-специално за създаването на личностни профили и за събирането на лични данни по отношение на деца при пряко предлагане на услуги на деца на уебсайтове на институции и органи на Съюза, като например междуличностни съобщителни услуги или онлайн продажба на билети, и обработването на лични данни се основава на съгласие.

(28) Когато установени в Съюза получатели, различни от институциите и органите на Съюза, искат институции и органи на Съюза да им предадат лични данни, тези получатели следва да докажат, че предаването е необходимо за изпълнението на тяхна задача, която се осъществява в обществен интерес, или за упражняването на официалните им правомощия. Като алтернатива тези получатели следва да докажат, че предаването е необходимо за конкретна цел в обществен интерес, като администраторът следва да установи дали има основание да се предполага, че законните интереси на субекта на данните могат да бъдат накърнени. В такива случаи администраторът следва да претегли по доказуем начин различните конкуриращи се интереси, за да прецени пропорционалността на поисканото предаване

([1]) Директива 93/13/ЕИО на Съвета от 5 април 1993 г. относно неравноправните клаузи в потребителските договори (ОВ L 95, 21.4.1993 г., стр. 29).

на лични данни. Конкретните цели в обществен интерес могат да се отнасят до прозрачността на институциите и органите на Съюза. Институциите и органите на Съюза следва да докажат такава необходимост, когато те самите предприемат предаването на данни, в съответствие с принципите на прозрачност и добро управление. Определените в настоящия регламент изисквания във връзка с предаването на данни на установени в Съюза получатели, различни от институциите и органите на Съюза, следва да се разбират като допълнителни по отношение на условията за законосъобразно обработване.

(29) На личните данни, които по своето естество са особено чувствителни от гледна точка на основните права и свободи, се полага специална защита, тъй като контекстът на тяхното обработване би могъл да създаде значителни рискове за основните права и свободи. Такива лични данни не следва да бъдат обработвани, освен ако са изпълнени специфичните условия, определени в настоящия регламент. Посочените лични данни следва да включват личните данни, разкриващи расов или етнически произход, като използването на понятието „расов произход“ в настоящия регламент не означава, че Съюзът приема теориите, които се опитват да установят съществуването на отделни човешки раси. Обработването на снимки не следва систематично да се счита за обработване на специални категории лични данни, тъй като снимките се обхващат от определението за биометрични данни единствено когато се обработват чрез специални технически средства, позволяващи уникална идентификация на дадено физическо лице или удостоверяване на автентичността. В допълнение към специфичните изисквания за обработване на чувствителни данни следва да се прилагат общите принципи и другите правила, залегнали в настоящия регламент, по-специално по отношение на условията за законосъобразно обработване. Дерогации от общата забрана за обработване на такива специални категории лични данни следва изрично да бъдат предвидени, *inter alia*, когато субектът на данните даде изричното си съгласие или във връзка с конкретни нужди, по-специално когато обработването се извършва в хода на законната дейност на някои сдружения или фондации, чиято цел е да се позволи упражняването на основните свободи.

(30) Специалните категории лични данни, за които е обоснована по-голяма защита, следва да бъдат обработвани за здравни цели само когато това е необходимо за постигането на тези цели в полза на физическите лица и на обществото като цяло, по-специално в рамките на управлението на услуги и системи за здравни или социални грижи. Поради това настоящият регламент следва да предвижда хармонизирани условия за обработването на специални категории лични данни за здравословното състояние по отношение на специфични потребности, по-специално когато обработването на тези данни се извършва за определени здравни цели от лица, обвързани от правното задължение за професионална тайна. Правото на Съюза следва да предвижда конкретни и подходящи мерки за защита на основните права и личните данни на физическите лица.

(31) Обработването на специални категории лични данни може да е необходимо по съображения от обществен интерес в областта на общественото здраве без съгласието на субекта на данните. Такова обработване следва да бъде предмет на подходящи и конкретни мерки с оглед защита на правата и свободите на физическите лица. В този контекст понятието „обществено здраве“ следва да се тълкува по смисъла на Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета ([1]) и означава всички елементи, свързани със здравето, а именно здравословно състояние, включително заболеваемост и инвалидност, решаващи фактори, които оказват влияние върху това здравословно състояние, потребности от здравно обслужване, средства, отделени за здравно обслужване, предоставяне на здравни грижи и всеобщ достъп до тях, разходи и финансиране на здравното обслужване, както и причини за смъртност. Такова обработване на данни за здравето по съображения от обществен интерес не следва да води до обработването на лични данни за други цели.

(32) Ако обработваните от администратора лични данни не му позволяват да идентифицира дадено физическо лице, администраторът на данни не следва да е задължен да се сдобие с допълнителна информация, за да идентифицира субекта на данните единствено с цел спазване на някоя от разпоредбите на настоящия регламент. Администраторът обаче не следва да отказва да приеме допълнителна информация, подадена от субекта на данни, за да подпомогне упражняването на неговите права. Идентификацията следва да включва цифровата идентификация на субекта на данни, например чрез механизъм за удостоверяване на автентичността като използването от субекта на данни на една и съща информация за удостоверяване на идентичността при регистрация за онлайн услуга, предлагана от администратора на лични данни.

(33) Обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели следва да се извършва при прилагане на подходящи гаранции за правата и свободите на субекта на данните в съответствие с настоящия регламент. Посочените гаранции следва да осигурят наличието на технически и организационни мерки, по-специално с оглед на спазването на принципа за свеждане на данните до минимум. По-нататъшното обработване на лични данни за целите на архивирането в обществен интерес,

([1]) Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета от 16 декември 2008 г. относно статистиката на Общността в областта на общественото здраве и здравословните и безопасни условия на труд (ОВ L 354, 31.12.2008 г., стр. 70).

за научни или исторически изследвания или за статистически цели се извършва, когато администраторът е преценил възможността за постигане на тези цели чрез обработването на лични данни, които не позволяват или повече не позволяват идентифицирането на субекта на данните, при условие че съществуват подходящи гаранции (като напр. псевдонимизацията на данните). Институциите и органите на Съюза следва да предвидят подходящи гаранции за обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели в правото на Съюза, което може да включва вътрешни правила, приети от институциите и органите на Съюза по въпроси, свързани с тяхното функциониране.

(34) Следва да бъдат предвидени ред и условия за улесняване на упражняването на правата на субектите на данни съгласно настоящия регламент, включително механизми за искане и ако е приложимо — получаване, без заплащане, по-специално на достъп до, коригиране или изтриване на лични данни и упражняване на правото на възражение. Администраторът следва да предостави и средства за подаване на искания по електронен път, особено когато личните данни се обработват електронно. Администраторът следва да бъде задължен да отговоря на исканията на субекта на данни без ненужно забавяне и най-късно в рамките на един месец, както и да посочи причините, ако не възнамерява да се съобрази с тези искания.

(35) Принципите на добросъвестно и прозрачно обработване изискват субектът на данни да бъде информиран за съществуването на операция по обработване и за нейните цели. Администраторът следва да предостави на субекта на данните всяка допълнителна информация, която е необходима, за да се гарантира добросъвестно и прозрачно обработване на данните, като се вземат предвид конкретните обстоятелства и контекст, в които се обработват личните данни. Освен това субектът на данни следва да бъде информиран за извършването на профилиране и за последствията от това профилиране. Когато личните данни се събират от субекта на данни, той следва да бъде информиран и за това дали е задължен да предостави личните данни и за последствията, в случай че не ги предостави. Тази информация може да бъде предоставена в комбинация със стандартизирани икони, така че по лесно видим, разбираем и ясно четим начин да се представи съдържателен преглед на планираното обработване. Ако иконите се представят в електронен вид, те следва да бъдат машинночитаеми.

(36) Информацията за обработването на лични данни, свързани със субекта на данните, следва да му бъде предоставена в момента на събирането ѝ от субекта на данните или ако личните данни са получени от друг източник — в рамките на разумен срок, в зависимост от обстоятелствата на конкретния случай. В случаите, в които личните данни могат да бъдат законно разкрити на друг получател, субектът на данните следва да бъде информиран, когато личните данни се разкриват за първи път на получателя. Когато администраторът възнамерява да обработва личните данни за цел, различна от тази, за която те са събрани, той следва да предостави на субекта на данните преди това по-нататъшно обработване информация за въпросната друга цел и друга необходима информация. Когато на субекта на данните не може да се предостави информация за произхода на личните данни поради използването на различни източници, се представя обобщена информация.

(37) Всяко физическо лице следва да има право на достъп до събраните лични данни, които го засягат, и да упражнява това право лесно и на разумни интервали, за да бъде осведомено за обработването и да провери законосъобразността му. Това включва правото на субектите на данни на достъп до данните за здравословното им състояние, например данните в медицинските им досиета, които съдържат информация като диагнози, резултати от прегледи, становища на лекуващите лекари и проведени лечения или извършени операции. Поради това всеки субект на данни следва да има правото да е запознат и да получава информация, по-специално относно целите, за които се обработват личните данни, когато е възможно — срока, за който се обработват личните данни, получателите на личните данни, логиката на автоматизираното обработване на личните данни и последствията от такова обработване, най-малкото когато се извършва на основата на профилиране. Това право не следва да влияе неблагоприятно върху правата или свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера. Тези съображения обаче не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни. Когато администраторът обработва голямо количество информация относно субекта на данни, администраторът следва да може да поиска от субекта на данните, преди да бъде предадена информацията, да посочи точно информацията или дейностите по обработването, за които се отнася искането.

(38) Субектът на данни следва да има право на коригиране на личните данни, свързани с него, както и правото „да бъде забравен“, когато запазването на тези данни е в нарушение на настоящия регламент или на правото на Съюза, което се прилага спрямо администратора. Субектът на данни следва да има право личните му данни да се изтриват и да не бъдат обработвани повече, когато личните данни престанат да бъдат необходими с оглед на целите, за които те са били събрани или обработвани по друг начин, когато субектът на данните е оттеглил своето съгласие или е възразил срещу обработването на лични данни, свързани с него, или когато обработването на личните му данни по друг начин не е в съответствие с настоящия регламент. Това право е важно особено когато субектът на данни е дал съгласието си

като дете и не е осъзнавал напълно рисковете, свързани с обработването, и впоследствие желае да премахне такива лични данни, особено когато са в интернет. Субектът на данни следва да може да упражни това право независимо от факта, че вече не е дете. По-нататъшното запазване на личните данни обаче следва да бъде законно, ако е необходимо за упражняване на правото на свобода на изразяване на мнение и правото на информация, за спазване на правно задължение, за изпълнение на задача от обществен интерес или при изпълнение на официални функции, възложени на администратора, по причини от обществен интерес в областта на общественото здравеопазване, за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели, или за установяване, упражняване или защита на правни претенции.

(39) С цел утвърждаване на „правото да бъдеш забравен“ в онлайн средата правото на изтриване следва да бъде разширено, като от администратора, който е направил личните данни обществено достъпни, следва да се изисква да информира администраторите, които обработват такива лични данни, да изтрият всякакви връзки към тези лични данни или техните копия или реплики. За тази цел администраторът следва да предприеме разумни мерки, като вземе предвид наличните технологии и средствата на разположение на администратора, включително технически мерки, за да информира администраторите, които обработват личните данни, за искането на субекта на данните.

(40) Методите за ограничаване на обработването на лични данни биха могли да включват, *inter alia*, временно преместване на избраните лични данни в друга система за обработване, прекратяване на достъпа на ползвателите до тях или временно премахване на публикуваните данни от уебсайт. В автоматизираните регистри на лични данни ограничаването на обработването следва по принцип да бъде осигурено с технически средства, така че личните данни да не подлежат на операции по по-нататъшно обработване и да не могат да се променят. Фактът, че обработването на лични данни е ограничено, следва да бъде ясно посочен в системата.

(41) С цел допълнително засилване на контрола над собствените данни, когато обработването на лични данни става с автоматични средства, субектът на данните следва да има и правото да получава отнасящите се до него лични данни, които той е предоставил на администратора, в структуриран, широко използван, пригоден за машинно четене и оперативно съвместим формат и да ги предава на друг администратор. Администраторите следва да бъдат насърчавани да разработват оперативно съвместими формати, които позволяват преносимост на данните. Това право следва да се прилага, когато субектът на данни е предоставил личните данни въз основа на собственото си съгласие или обработването е необходимо поради договорно задължение. Ето защо това право не следва да се прилага, когато обработването на личните данни е необходимо за спазване на правно задължение на администратора, или за изпълнение на задача от обществен интерес, или при упражняване на официално правомощие, предоставено на администратора. Правото на субекта на данни да предава или получава отнасящи се до него лични данни не следва да поражда задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване. Когато в определен пакет от лични данни е засегнат повече от един субект на данни, правото личните данни да бъдат получавани следва да не засяга правата и свободите на други субекти на данни в съответствие с настоящия регламент. Освен това, това право не следва да засяга правото на субекта на данни на изтриване на лични данни и ограниченията на това право, както е посочено в настоящия регламент, и по-специално не следва да включва изтриването на лични данни относно субекта на данните, които той е предоставил в изпълнение на договор, в степента и за сроковете, за които личните данни са необходими за изпълнението на този договор. Когато това е технически осъществимо, субектът на данни следва да има право на пряко прехвърляне на личните данни от един администратор към друг.

(42) Когато личните данни биха могли да се обработват законносъобразно, тъй като обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официално правомощие, предоставено на администратора, всеки субект на данни следва все пак да има право на възражение срещу обработването на лични данни, свързани с неговото конкретно положение. Администраторът следва да докаже, че неговите неоспорими законни интереси имат предимство пред интересите или основните права и свободи на субекта на данни.

(43) Субектът на данни следва да има право да не бъде адресат на решение, което може да включва мярка за оценка на свързани с него лични аспекти единствено въз основа на автоматизирано обработване и което поражда правни последствия за него или го засяга също толкова значително, като например електронни практики за набиране на персонал без човешка намеса. Това обработване включва „профилиране“, което се състои от всякакви форми на автоматизирано обработване на лични данни за оценка на личните аспекти във връзка с дадено физическо лице, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към изпълнението на

професионалните задължения на субекта на данни, неговото икономическо състояние, здраве, лични предпочитания или интереси, надеждност или поведение, местонахождение или движения, когато то поражда правни последствия по отношение на лицето или го засяга също толкова значително.

Въпреки това вземането на решения въз основа на такова обработване, включително профилиране, следва да бъде позволено, когато е изрично разрешено от правото на Съюза. Във всеки случай такова обработване следва да подлежи на подходящи гаранции, които следва да включват конкретна информация за субекта на данните и правото на човешка намеса, на изразяване на мнение, на получаване на обяснение за решението, взето в резултат на такава оценка, и на обжалване на решението. Такава мярка не следва да се отнася до дете. С цел да се осигури добросъвестно и прозрачно обработване по отношение на субекта на данните, като се отчитат конкретните обстоятелства и контекстът, при които се обработват личните данни, администраторът следва да използва подходящи математически или статистически процедури за профилирането, да прилага съответните технически и организационни мерки, по-специално за да гарантира, че факторите, които водят до неточности в личните данни, се коригират, а рискът от грешки се свежда до минимум, да защити личните данни по начин, който отчита потенциалните заплахи за интересите и правата на субекта на данните и да предотврати, *inter alia*, ефект на дискриминация на физически лица въз основа на тяхната раса или етнически произход, политически възгледи, вероизповедание или убеждения, членство в синдикални организации, генетичен или здравен статус или сексуална ориентация или обработване, от което произтичат мерки с такъв ефект. Автоматизираното вземане на решения и профилирането на базата на специални категории лични данни следва да бъде разрешено само при определени условия.

(44) Правни актове, приети въз основа на Договорите, или вътрешни правила, приети от институции и органи на Съюза по въпроси, свързани с тяхната дейност, могат да налагат ограничения относно специални принципи и относно правото на информация, достъп до и коригиране или изтриване на лични данни, правото на преносимост на данните, поверителността на данните от електронните съобщения, както и уведомяването на субекта на данни за нарушение на сигурността на личните данни и определени свързани с това задължения на администраторите, доколкото това е необходимо и пропорционално в едно демократично общество с оглед защитата на обществената сигурност и за предотвратяването, разследването и наказателното преследване на престъпления или изпълнението на наказания. Това включва защитата срещу заплахи за обществената сигурност и тяхното предотвратяване, защитата на човешкия живот, особено при природни или предизвикани от човека бедствия, вътрешната сигурност на институциите и органите на Съюза, други важни цели от общ обществен интерес на Съюза или на държава членка, по-специално целите на общата външна политика и политика на сигурност на Съюза или важен икономически или финансов интерес на Съюза или на държава членка, и поддържането на публични регистри поради причини от широк обществен интерес или защитата на субекта на данни или на правата и свободите на други лица, включително социалната защита, общественото здраве и хуманитарните цели.

(45) Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-специално администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съответствие с настоящия регламент, включително ефективността на мерките. Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица.

(46) Рискът за правата и свободите на физическите лица, с различна вероятност и тежест, може да произтича от обработване на лични данни, което би могло да доведе до физически, имуществени или неимуществени вреди, по-специално: когато обработването може да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация или други значителни икономически или социални неблагоприятни последствия; когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху техните лични данни; когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и когато се обработват генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и престъпления или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения, икономическото състояние, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; когато обработването включва голям обем лични данни и засяга голям брой субекти на данни.

(47) Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до риск или до висок риск.

(48) Защитата на правата и свободите на физическите лица с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира изпълнението на изискванията на настоящия регламент. За да може да докаже спазването на настоящия регламент, администраторът следва да приеме вътрешни политики и да приложи мерки, които отговарят по-специално на принципите за защита на данните на етапа на проектирането и защита на данните по подразбиране. Такива мерки могат да се изразяват, *inter alia*, в свеждане до минимум на обработването на лични данни, псевдонимизиране на лични данни на възможно най-ранен етап, прозрачност по отношение на функциите и обработването на лични данни, създаване на възможност за субекта на данни да наблюдава обработването на данни, възможност за администратора да създава и подобрява елементите на сигурността. Принципите на защита на данните на етапа на проектирането и по подразбиране следва да се вземат предвид и в контекста на процедурите за възлагане на обществени поръчки.

(49) Регламент (ЕС) 2016/679 изисква от администраторите да докажат, че спазват задълженията си, като се придържат към одобрени механизми за сертифициране. Институциите и органите на Съюза също така следва да могат да докажат, че спазват настоящия регламент, като получат сертифициране в съответствие с член 42 от Регламент (ЕС) 2016/679.

(50) Защитата на правата и свободите на субектите на данни, както и отговорността и задълженията на администраторите и обработващите лични данни изискват ясно определяне на отговорностите съгласно настоящия регламент, включително когато администраторът определя целите и средствата на обработването съвместно с други администратори или когато дадена операция по обработване се извършва от името на даден администратор.

(51) За да се гарантира спазването на изискванията на настоящия регламент по отношение на обработването, извършвано от обработващия лични данни от името на администратора, когато на обработващия лични данни се възлагат дейности по обработването, администраторът следва да използва само такива обработващи лични данни, които предоставят достатъчни гаранции, по-специално по отношение на експертни знания, надеждност и ресурси, че предприемат технически и организационни мерки, които отговарят на изискванията на настоящия регламент, включително на изискванията за сигурността на обработването. Придържането от страна на обработващите лични данни, различни от институциите и органите на Съюза, към одобрен кодекс на поведение или одобрен механизъм за сертифициране може да се използва като елемент за доказване, че са спазени задълженията на администратора. Извършването на обработването от обработващ лични данни, различен от институция или орган на Съюза, следва да се урежда с договор или, в случай че обработването се извършва от институции или органи на Съюза — с договор или друг правен акт съгласно правото на Съюза, който обвързва обработващия лични данни с администратора, регламентира предмета и продължителността на обработването, естеството и целите на обработването, вида лични данни и категориите субекти на данни, като се вземат предвид конкретните задачи и отговорности на обработващия лични данни в контекста на обработването, което следва да се извърши, както и рискът за правата и свободите на субекта на данни. Администраторът и обработващият лични данни следва да могат да изберат да използват индивидуален договор или стандартни договорни клаузи, приети или пряко от Комисията, или от Европейския надзорен орган по защита на данните и впоследствие приети от Комисията. След приключване на обработването от името на администратора обработващият личните данни следва, по избор на администратора, да ги върне или заличи, освен ако не е налице изискване за съхраняване на въпросните лични данни по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни.

(52) За да докажат спазването на настоящия регламент, както администраторите, така и обработващите лични данни следва да поддържат регистри на всички категории дейности по обработване, за които отговарят. Институциите и органите на Съюза следва да са длъжни да си сътрудничат с Европейския надзорен орган по защита на данните и да му предоставят своите регистри при поискване, за да могат да бъдат използвани за наблюдение на тези операции по обработване. Освен ако е нецелесъобразно, като се вземе предвид размерът на институцията или органа на Съюза, институциите и органите на Съюза следва да могат да създадат централен регистър на своите дейности по обработване на данни. От съображения за прозрачност те следва също така да могат да направят този регистър публичен.

(53) С цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на настоящия регламент, администраторът или обработващият лични данни следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид достиженията на техническия

прогрес и разходите по изпълнението спрямо рисковете и естеството на личните данни, които трябва да бъдат защитени. При оценката на риска за сигурността на данните следва да се разгледат рисковете, произтичащи от обработването на лични данни, като случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване или достъп до предадени, съхранявани или обработвани по друг начин лични данни, което може по-конкретно да доведе до физически, имуществени или неимуществени вреди.

(54) Институциите и органите на Съюза следва да гарантират поверителността на електронните съобщения, предвидена в член 7 от Хартата. По-специално институциите и органите на Съюза следва да гарантират сигурността на своите електронни съобщителни мрежи. Те следва да защитават информацията, свързана с крайните устройства на ползвателите, осъществяващи достъп до техните обществено достъпни уебсайтове и мобилни приложения в съответствие с Директива 2002/58/ЕО на Европейския парламент и на Съвета ([1]). Те следва да защитават също и личните данни, съхранявани в указателите на ползвателите.

(55) Нарушението на сигурността на личните данни може, ако по отношение на него не бъдат взети подходящи и своевременни мерки, да доведе до физически, имуществени или неимуществени вреди за физическите лица. Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми Европейския надзорен орган по защита на данните за нарушението на сигурността на личните данни без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа, след като е разбрал за него, освен ако администраторът е в състояние да докаже в съответствие с принципа на отчетност, че няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато такова уведомление не може да бъде подадено в срок от 72 часа, то следва да посочва причините за забавянето и информацията може да се подаде поетапно без излишно допълнително забавяне. Когато такова забавяне е основателно, не толкова чувствителната или конкретна информация относно нарушението следва да бъде предоставена на възможно най-ранен етап, вместо преди уведомяването да се изчаква цялостно разрешаване на инцидента, който е в основата на нарушението.

(56) Администраторът следва да уведоми субекта на данни за нарушението на сигурността на личните данни без ненужно забавяне, когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическото лице, за да му се даде възможност да предприеме необходимите предпазни мерки. В уведомлението следва да се посочва естеството на нарушението на сигурността на личните данни, както и да се дават препоръки на засегнатото физическо лице за това как да ограничи потенциалните неблагоприятни последици. Такива уведомления до субектите на данни следва да бъдат правени веднага щом това е разумно осъществимо и в тясно сътрудничество с Европейския надзорен орган по защита на данните, като се спазват насоките, предоставени от него или от други съответни органи, като например правоприлагащите органи.

(57) Регламент (ЕО) № 45/2001 предвижда общо задължение на администратора да уведоми за обработването на лични данни длъжностното лице по защита на данните. Освен ако е нецелесъобразно, като се вземе предвид размерът на институцията или органа на Съюза, длъжностното лице по защита на данните води регистър на операциите по обработване, за които е направено уведомление. Наред с това общо задължение следва да се въведат ефективни процедури и механизми за наблюдение на онези видове операции по обработване, които има вероятност да доведат до висок риск за правата и свободите на физическите лица поради своето естество, обхват, контекст и цели. Такива процедури следва да бъдат прилагани по-специално, когато видовете операции по обработване включват използването на нови технологии или представляват нов вид технологии, във връзка с които преди това от администратора не е извършвана оценка на въздействието върху защитата на данните или които стават необходими предвид времето, изминало от първоначалното обработване. В такива случаи преди обработването администраторът следва да извърши оценка на въздействието върху защитата на данните, за да се оценят конкретната вероятност и тежестта на високия риск, като се вземат предвид естеството, обхватът, контекстът и целите на обработването и източниците на риска. Посочената оценка на въздействието следва да включва по-специално предвидените мерки, гаранции и механизми за ограничаване на този риск, с които се осигурява защитата на личните данни и се доказва спазването на настоящия регламент.

(58) Когато в оценката на въздействието върху защитата на данните е указано, че при липса на гаранции, мерки за сигурност и механизми за ограничаване на риска обработването би довело до висок риск за правата и свободите на физическите лица, и администраторът счита, че рискът не може да бъде ограничен с разумни средства от гледна точка на наличните технологии и разходи за прилагане, преди началото на дейностите по обработването следва да се осъществи консултация с Европейския надзорен орган по защита на данните. Има вероятност такъв висок риск да бъде породен от определени видове обработване и от степента и честотата на обработване, които могат да доведат и до нанасяне на вреди или до възпрепятстване на упражняването на правата и свободите на физическото лице. Европейският надзорен орган по защита на данните следва да отговори на искането за консултация в рамките на определен срок. Въпреки това отсъствието на отговор от Европейския надзорен орган по защита на данните в рамките

([1]) Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

на този срок не следва да препятства евентуалната намеса на Европейския надзорен орган по защита на данните в съответствие със задълженията и правомощията му, установени в настоящия регламент, включително правомощието да забранява операции по обработване. Като част от този процес на консултации следва да бъде възможно да се представи на Европейския надзорен орган по защита на данните резултатът от оценка на въздействието върху защитата на данните, извършена във връзка с въпросното обработване, и по-конкретно мерките, предвидени за ограничаване на възможните рискове за правата и свободите на физическите лица.

(59) Европейският надзорен орган по защита на данните следва да бъде информиран за административните мерки и с него да бъдат провеждани консултации относно вътрешните правила, приемани от институциите и органите на Съюза по въпроси, свързани с тяхната дейност, когато те предвиждат обработването на лични данни, определят условия за ограничаване на правата на субекта на данни или предоставят подходящи гаранции за правата на субекта на данни, за да се гарантира, че планираното обработване отговаря на изискванията на настоящия регламент, по-специално относно ограничаването на рисковете, свързани със субекта на данни.

(60) С Регламент (ЕС) 2016/679 бе създаден Европейският комитет по защита на данните като независим орган на Съюза, притежаващ правосубектност. Комитетът следва да допринася за съгласуваното прилагане на Регламент (ЕС) 2016/679 и Директива (ЕС) 2016/680 навсякъде в Съюза, включително като съветва Комисията. В същото време Европейският надзорен орган по защита на данните следва да продължи да упражнява своите надзорни и консултативни функции по отношение на всички институции и органи на Съюза, включително по своя собствена инициатива или при поискване. С цел да се гарантира съгласуваност на правилата за защита на данните навсякъде в Съюза, Комисията следва да полага усилия за консултация с Европейския надзорен орган по защита на данните при подготовката на предложения или препоръки. Комисията следва да извършва задължително консултация след приемането на законодателни актове или при подготовката на делегирани актове и актове за изпълнение, определени в членове 289, 290 и 291 от ДФЕС, и след приемането на препоръки и предложения, свързани със споразумения с трети държави и международни организации, предвидени в член 218 от ДФЕС, които имат въздействие върху правото на защита на личните данни. В тези случаи Комисията следва да бъде задължена да се консултира с Европейския надзорен орган по защита на данните, с изключение на случаите, при които Регламент (ЕС) 2016/679 предвижда задължителна консултация с Европейския комитет по защита на данните, например във връзка с решения относно адекватното ниво на защита или делегирани актовете относно стандартизирани икони и изисквания за механизмите за сертифициране. Когато въпросният акт има особено значение за защитата на правата и свободите на физическите лица по отношение на обработването на лични данни, Комисията следва да може също така да се консултира с Европейския комитет по защита на данните. В тези случаи Европейският надзорен орган по защита на данните следва, като член на Европейския комитет по защита на данните, да координира работата си с него с оглед на изготвянето на съвместно становище. Европейският надзорен орган по защита на данните и когато е приложимо, Европейският комитет по защита на данните следва да представят писменото си становище в срок от осем седмици. Този срок следва да бъде намален за спешни случаи или когато това е уместно, например когато Комисията подготвя делегирани актове и актове за изпълнение.

(61) В съответствие с член 75 от Регламент (ЕС) 2016/679 Европейският надзорен орган по защита на данните следва да осигурява секретариата на Европейския комитет по защита на данните.

(62) Във всички институции и органи на Съюза трябва да има длъжностно лице по защита на данните, което да гарантира прилагането на разпоредбите на настоящия регламент и да съветва администраторите и обработващите лични данни по изпълнението на техните задължения. Длъжностното лице по защита на данните следва да бъде лице с експертни познания в областта на правото и практиките за защита на данните, което следва да се определя по-специално в съответствие с извършваните операции по обработване на данни от администратора или обработващия лични данни и защитата, която е необходима за личните данни. Тези длъжностни лица по защита на данните следва да са в състояние да изпълняват своите задължения и задачи по независим начин.

(63) Когато лични данни се предават от институциите или органите на Съюза на администратори, обработващи лични данни или други получатели в трети държави или на международни организации, нивото на защита на физическите лица, осигурено в Съюза с настоящия регламент, следва да бъде гарантирано. Същите гаранции следва да се прилагат 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 и при спазване на основните права и свободи, заложени в Хартата. 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.

(64) Комисията може да реши в съответствие с член 45 от Регламент (ЕС) 2016/679 или с член 36 от Директива (ЕС) 2016/680, че дадена трета държава, територия или конкретен сектор в трета държава или дадена международна организация предоставя адекватно ниво на защита на данните. В тези случаи предаването на лични данни на такава трета държава или международна организация от институция или орган на Съюза може да се извършва, без да е необходимо допълнително разрешение.

(65) 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. Тези подходящи гаранции може да се състоят от стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от Европейския надзорен орган по защита на данните, или договорни клаузи, разрешени от Европейския надзорен орган по защита на данните. Когато обработващият лични данни не е институция или орган на Съюза, тези подходящи гаранции може също така да се състоят от задължителни фирмени правила, кодекси за поведение и механизми за сертифициране, използвани за международното предаване на данни по силата на Регламент (ЕС) 2016/679. 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 изпълняеми 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 проектирането и по подразбиране. Данни може да се предават и от институциите или органите на Съюза на публични органи или организации в трети държави или на международни организации със съответните задължения или функции, включително въз основа на разпоредбите, които ще бъдат включени в административните договорености, като например меморандум за разбирателство, с които да се предоставят изпълняеми и ефективни права за субектите на данни. Когато гаранциите са предвидени в административни договорености, които нямат задължителен характер, следва да се получи разрешение от Европейския надзорен орган по защита на данните.

(66) Възможността администраторът или обработващият лични данни да използва стандартни клаузи за защита на данните, приети от Комисията или от Европейския надзорен орган по защита на данните, 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 Европейския надзорен орган по защита на данните, 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 на данните.

(67) Някои трети държави приемат закони, подзаконови и други правни актове, които имат за цел пряко да регулират дейностите по обработване на данни от страна на институциите или органите на Съюза. Това може да включва решения на съдилища или трибунали или решения на административни органи в трети държави, с които от администратора или обработващия лични данни се изисква да предаде или да разкрие лични данни и които не се основават на международно споразумение, което е в сила между третата държава, отправила искането, и Съюза. Извънтериториалното прилагане на тези закони, подзаконови и други правни актове може да бъде в нарушение на международното право и да възпрепятства осигуряването на защитата на физическите лица, гарантирана в Съюза с настоящия регламент. Предаването на данни следва да е разрешено само когато са изпълнени условията на настоящия регламент относно предаването на данни на трети държави. Такъв може да бъде случаят, *inter alia*, когато разкриването е необходимо поради важно съображение от обществен интерес, признато в правото на Съюза.

(68) Следва да се предвиди възможността в особени случаи да се предават данни при определени обстоятелства, когато субектът на данните е дал изричното си съгласие, когато предаването засяга отделни случаи и е необходимо във връзка с договор или правна претенция, независимо от това дали е в рамките на съдебна, административна или друга извънсъдебна процедура, включително процедура пред регулаторни органи. Следва да се предвиди и възможността да се предават данни, когато това се налага поради важни съображения от обществен интерес, предвидени в правото на Съюза, или когато предаването се извършва от регистър, създаден със закон и предназначен за справки от обществеността или от лица, които имат законен интерес. В този случай, освен ако това е разрешено от правото на Съюза, предаването не следва да включва всички лични данни или цели категории данни, съдържащи се в регистъра, а когато регистърът е предназначен за справка от лица, които имат законен интерес, предаването следва да се извършва единствено по искане на тези лица или ако те са получателите, като се вземат изцяло под внимание интересите и основните права на субекта на данните.

(69) Тези дерогации следва да се прилагат по-специално за предаването на данни, което се изисква и е необходимо по важни причини от обществен интерес, например при международен обмен на данни между институциите и органите на Съюза и органи по защита на конкуренцията, данъчни или митнически власти, органи за финансов надзор и служби, компетентни по въпросите на социалната сигурност или общественото здраве, например в случай на проследяване на контакти при заразни болести или с цел намаляване и/или премахване на употребата на допинг в спорта. Предаването на лични данни следва също да се разглежда като законосъобразно, когато е необходимо за

защитата на интерес от съществено значение за жизненоважни интереси на субекта на данни или на друго лице, включително физическата неприкосновеност или живота, ако субектът на данните не е в състояние да даде съгласие. При липсата на решение относно адекватното ниво на защита правото на Съюза може по важни причини от обществен интерес изрично да определи ограничения за предаването на специални категории от данни на трета държава или международна организация. Всяко предаване на международна хуманитарна организация на лични данни на субект на данни, който е физически или юридически неспособен да даде своето съгласие, с оглед на изпълнението на задължение по силата на Женевските конвенции или прилагането на международното хуманитарно право, приложимо в условията на военни конфликти, може да се счита за необходимо поради важна причина от обществен интерес или защото е от жизненоважен интерес за субекта на данни.

(70) 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 изпълняеми и ефективни 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.

(71) 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 националните надзорни органи и Европейският надзорен орган по защита на данните, могат да бъдат изправени пред невъзможността да разглеждат жалби или да провеждат разследвания, свързани с дейности, извършвани извън тяхната юрисдикция. 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. Поради това по-тясното сътрудничество между Европейския надзорен орган по защита на данните и националните надзорни органи следва да бъде насърчавано, за да им се помогне да обменят информация със своите международни партньори.

(72) Създаването с Регламент (ЕО) № 45/2001 на Европейския надзорен орган по защита на данните, който е оправомощен да изпълнява своите задачи и упражнява своите правомощия при пълна независимост, е първостепенен елемент от защитата на физическите лица във връзка с обработването на личните им данни. Настоящият регламент следва допълнително да укрепи и да изясни неговите роля и независимост. Европейският надзорен орган по защита на данните следва да бъде лице, чиято независимост не подлежи на съмнение и за което е признато, че притежава необходимите опит и умения, за да изпълнява задълженията на Европейски надзорен орган по защита на данните, например поради това, че е работило в един от надзорните органи, създадени по силата на член 51 от Регламент (ЕС) 2016/679.

(73) За да се гарантира съгласувано наблюдение и прилагане на правилата за защита на данните навсякъде в Съюза, Европейският надзорен орган по защита на данните следва да има еднакви задачи и ефективни правомощия с националните надзорни органи, включително правомощия за разследване, корективни правомощия и правомощия за налагане на санкции, правомощия за даване на разрешения и становища, особено в случаи на жалби от физически лица, правомощия за довеждане на нарушенията на настоящия регламент до знанието на Съда и правомощия за участие в съдебни производства в съответствие с първичното право. Тези правомощия следва да включват и правомощието за налагане на временно или окончателно ограничаване, включително забрана, на обработването на данни. С цел избягване на излишни разходи и прекалени неудобства за лицата, които могат да бъдат засегнати по неблагоприятен начин, всяка мярка на Европейския надзорен орган по защита на данните следва да бъде подходяща, необходима и пропорционална с оглед на осигуряването на съответствие с настоящия регламент, като се отчитат обстоятелствата при всеки конкретен случай и се зачита правото на всяко лице да бъде изслушано, преди да бъде взета каквато и да е конкретна мярка. Всяка мярка със задължителен характер на Европейския надзорен орган по защита на данните следва да бъде в писмена форма, да бъде ясна и недвусмислена, да посочва датата на издаване на мярката, да е подписана от Европейския надзорен орган по защита на данните, да посочва основанията за мярката и да се позовава на правото на ефективни правни средства за защита.

(74) Компетентността на Европейския надзорен орган по защита на данните във връзка с надзора не следва да обхваща обработването на лични данни от Съда, когато той действа при изпълнение на своите съдебни функции, за да се гарантира независимостта на Съда при изпълнението на съдебните му задължения, включително вземането на решения. За такива операции по обработване Съдът следва да установи независим надзор в съответствие с член 8, параграф 3 от Хартата, например чрез вътрешен механизъм.

(75) Решенията на Европейския надзорен орган по защита на данните относно изключенията, гаранциите, разрешенията и условията във връзка с операциите по обработване на данни, както са определени в настоящия регламент, следва да се публикуват в доклад за дейността. Независимо от публикуването на годишен доклад за дейността, Европейският надзорен орган по защита на данните може да публикува доклади по конкретни теми.

(76) Европейският надзорен орган по защита на данните следва да спазва Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета ([1]).

(77) Националните надзорни органи наблюдават прилагането на Регламент (ЕС) 2016/679 и допринасят за неговото съгласувано прилагане навсякъде в Съюза с цел защита на физическите лица по отношение на обработването на личните им данни и улесняване на свободното движение на личните данни в рамките на вътрешния пазар. С цел да се повиши съгласуваността при прилагане на правилата за защита на данните, приложими в държавите членки, и на правилата за защита на данните, приложими за институциите и органите на Съюза, Европейският надзорен орган по защита на данните следва да си сътрудничи ефективно с националните надзорни органи.

(78) В някои случаи правото на Съюза предвижда модел на споделен между Европейския надзорен орган по защита на данните и националните надзорни органи координиран надзор. Европейският надзорен орган по защита на данните е също и надзорният орган на Европол и за тези цели, а посредством съвет за сътрудничеството, който има консултативни функции, е създаден конкретен модел на сътрудничество с националните надзорни органи. С цел подобряване на ефективния надзор и прилагане на материалноправните разпоредби за защита на данните, в Съюза следва да бъде въведен единен, съгласуван модел на координиран надзор. Поради това Комисията следва да направи, когато е целесъобразно, законодателни предложения за изменение на правните актове на Съюза, които предвиждат модел на координиран надзор, за да се приведат в съответствие с модела за координиран надзор от настоящия регламент. Европейският комитет по защита на данните следва да служи като единен форум за гарантиране на ефективен координиран надзор във всички области.

(79) Всеки субект на данни следва да има право да подаде жалба до Европейския надзорен орган по защита на данните, както и право на ефективни правни средства за защита пред Съда в съответствие с Договорите, ако счита, че правата му по настоящия регламент са нарушени или ако Европейският надзорен орган по защита на данните 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. Разследването въз основа на жалби следва да подлежи на съдебен контрол и да се извършва в целесъобразна за конкретния случай степен. Европейският надзорен орган по защита на данните следва да информира субекта на данните за напредъка в процеса на разглеждане и резултата от жалбата в разумен срок. Ако случаят изисква допълнително координиране с национален надзорен орган, на субекта на данните следва да бъде предоставена междинна информация. За да се улесни подаването на жалбите, Европейският надзорен орган по защита на данните следва да вземе мерки, като например осигуряване на формуляр за подаване на жалби, който да може да бъде попълнен и по електронен път, без да се изключват други средства за комуникация.

(80) Всяко лице, което е претърпяло имуществени или неимуществени вреди в резултат на нарушение на настоящия регламент, следва да има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди при спазване на условията, предвидени в Договорите.

(81) С цел да се укрепи надзорната роля на Европейския надзорен орган по защита на данните и ефективното прилагане на настоящия регламент Европейският надзорен орган по защита на данните следва да има правомощието да налага като санкция в краен случай административна имуществена санкция. Тя следва да имат за цел санкционирането на институцията или органа на Съюза, а не на физически лица, за неспазване на настоящия регламент, възпирането на бъдещи нарушения на настоящия регламент, както и насърчаването на култура на защита на личните данни в рамките на институциите и органите на Съюза. В настоящия регламент следва да се посочат нарушенията, за които се налага административна имуществена санкция, както и горните граници и критериите за определяне на свързаните имуществени санкции. Европейският надзорен орган по защита на данните следва да определи размера на имуществената санкция във всеки отделен случай, като взема предвид всички обстоятелства, свързани с конкретната ситуация, по-специално при надлежно отчитане на естеството, тежестта и продължителността на нарушението, на последиците от него и на мерките, предприети, за да се гарантира спазване на задълженията по настоящия регламент и за да се предотвратят или смекчат последиците от нарушението. При налагането на административна имуществена санкция на институция или орган на Съюза Европейския надзорен орган по защита на данните следва да прецени пропорционалността на размера на имуществената санкция. Административното производство за налагането на имуществени санкции на институции и органи на Съюза следва да зачита общите принципи на правото на Съюза, както се тълкуват от Съда.

(82) Когато субектът на данни смята, че правата му по настоящия регламент са нарушени, той следва да има право да възложи на структура, организация или сдружение с нестопанска цел, което е учредено съгласно правото на Съюза или правото на държава членка, има уставни цели, които са в обществен интерес, и работи в областта на защитата на

([1]) Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, Съвета и Комисията (ОВ L 145, 31.5.2001 г., стр. 43).

личните данни, да подаде жалба от негово име до Европейския надзорен орган по защита на данните. Тази структура, организация или сдружение следва също така да може да упражнява правото на съдебна защита от името на субектите на данни или да упражнява правото за обезщетение от името на субектите на данни.

(83) Длъжностно лице или друг служител на Съюза, който не спазва задълженията, предвидени в настоящия регламент, подлежи на дисциплинарна или друга мярка в съответствие с правилата и процедурите, установени в Правилника за длъжностните лица на Европейския съюз и Условията за работа на другите служители на Съюза, установени в Регламент (ЕИО, Евратом, ЕОВС) № 259/68 ([1]) („Правилник за длъжностните лица“).

(84) За да се гарантират еднакви условия за прилагането на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета ([2]). За приемането на стандартните договорни клаузи между администратори и обработващи лични данни и между обработващи лични данни, за приемането на списък на операциите по обработване, за които е необходима предварителна консултация с Европейския надзорен орган по защита на данните от администраторите, обработващи лични данни при изпълнението на задача от обществен интерес и за приемането на стандартни договорни клаузи, предвиждащи подходящи гаранции за международно предаване на данни, следва да бъде използвана процедурата по разглеждане.

(85) Поверителната информация, която статистическите органи на национално равнище и на равнището на Съюза събират за изготвянето на официална европейска и официална национална статистика, следва да бъде защитена. Европейската статистика следва да се разработва, изготвя и разпространява в съответствие със статистическите принципи, установени в член 338, параграф 2 от ДФЕС. Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета ([3]) конкретизира допълнително изискванията относно поверителността на данните на европейската статистика.

(86) Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО на Европейския парламент, на Съвета и на Комисията ([4]) следва да бъдат отменени. Позоваванията на отменения регламент и на отменените решение следва да се считат за позовавания на настоящия регламент.

(87) За да се гарантира пълната независимост на членовете на независимия надзорен орган, мандатите на настоящия Европейски надзорен орган по защита на данните и неговия заместник следва да не бъдат засегнати от настоящия регламент. Настоящият заместник следва да продължи да изпълнява мандата си до края на срока му, освен ако е изпълнено някое от условията за преждевременно прекратяване на мандата на Европейския надзорен орган по защита на данните, определени в настоящия регламент. До края на мандата на заместника спрямо него следва да се прилагат съответните разпоредби на настоящия регламент.

(88) В съответствие с принципа на пропорционалност е необходимо и подходящо за постигането на основната цел за осигуряване на еквивалентно ниво на защита на физическите лица във връзка с обработването на лични данни и свободното движение на лични данни навсякъде в Съюза да бъдат установени правила относно обработването на лични данни в институциите и органите на Съюза. С настоящия регламент не се надхвърля необходимото за постигането на поставените цели в съответствие с член 5, параграф 4 от ДЕС.

(89) В съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001 беше проведена консултация с Европейския надзорен орган по защита на данните, който представи становище на 15 март 2017 г. ([5]),

---

([1]) ОВ L 56, 4.3.1968 г., стр. 1.

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

([3]) Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета от 11 март 2009 г. относно европейската статистика и за отмяна на Регламент (ЕО, Евратом) № 1101/2008 за предоставянето на поверителна статистическа информация на Статистическата служба на Европейските общности, на Регламент (ЕО) № 322/97 на Съвета относно статистиката на Общността и на Решение 89/382/ЕИО, Евратом на Съвета за създаване на Статистически програмен комитет на Европейските общности (ОВ L 87, 31.3.2009 г., стр. 164).

([4]) Решение № 1247/2002/ЕО на Европейския парламент, на Съвета и на Комисията от 1 юли 2002 година относно статута и общите условия, регулиращи изпълнението на задълженията на Европейския надзорен орган по защита на данните (ОВ L 183, 12.7.2002 г., стр. 1).

([5]) ОВ C 164, 24.5.2017 г., стр. 2.

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и цели

1. С настоящия регламент се определят правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни от институциите и органите на Съюза, както и правилата по отношение на свободното движение на лични данни между тях или до други получатели, установени в Съюза.

2. С настоящия регламент се защитават основни права и свободи на физическите лица, и по-специално тяхното право на защита на личните данни.

3. Европейският надзорен орган по защита на данните следи за прилагането на разпоредбите на настоящия регламент по отношение на всички операции по обработване на лични данни, извършвани от институция или орган на Съюза.

Член 2

Обхват

1. Настоящият регламент се прилага за обработването на лични данни от всички институции и органи на Съюза.

2. Само член 3 и глава IX от настоящия регламент се прилагат за обработването на лични данни от оперативен характер от страна на органите, службите и агенциите на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС.

3. Настоящият регламент не се прилага за обработването на лични данни от оперативен характер от страна на Европол и Европейската прокуратура, преди да се адаптират Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета ([1]) и Регламент (ЕС) 2017/1939 на Съвета ([2]) в съответствие с член 98 от настоящия регламент.

4. Настоящият регламент не се прилага за обработването на лични данни от мисиите, посочени в член 42, параграф 1 и членове 43 и 44 от ДЕС.

5. 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.

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, е лице, което може да бъде идентифицирано пряко или непряко, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, икономическата, културната или социалната идентичност на това физическо лице;

2) „лични данни от оперативен характер“ означава всички лични данни, които се обработват от органи, служби или агенции на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС, за постигане на целите и изпълнение на задачите, определени в правните актове за създаване на тези органи, служби или агенции;

([1]) Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и за замяна и отмяна на решения 2009/371/ПВР, 2009/934/ПВР, 2009/935/ПВР, 2009/936/ПВР и 2009/968/ПВР на Съвета (ОВ L 135, 24.5.2016 г., стр. 53).

([2]) Регламент (ЕС) 2017/1939 на Съвета от 12 октомври 2017 г. за установяване на засилено сътрудничество за създаване на Европейска прокуратура (ОВ L 283, 31.10.2017 г., стр. 1).

3) „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;

4) „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

5) „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използването на лични данни за оценяване на определени лични аспекти, свързани с физическо лице, и по-конкретно за анализиране или прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения на това физическо лице, неговото икономическо състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение;

6) „псевдонимизация“ означава обработването на лични данни по такъв начин, че личните данни да не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано;

7) „регистър с лични данни“ означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии, независимо дали е централизиран, децентрализиран или разпределен съгласно функционален или географски принцип;

8) „администратор“ означава институцията или органа на Съюза, или генералната дирекция, или всяка друга организационна структура, която самостоятелно или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за обработването са определени със специален акт на Съюза, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза;

9) „администратори, различни от институции и органи на Съюза“ означава администратори по смисъла на член 4, точка 7 от Регламент (ЕС) 2016/679 и администратори по смисъла на член 3, точка 8 от Директива (ЕС) 2016/680;

10) „институции и органи на Съюза“ означава институциите, органите, службите и агенциите на Съюза, създадени с ДЕС, ДФЕС или Договора за Евратом или въз основа на тези договори;

11) „компетентен орган“ означава всеки публичен орган в държава членка, който е компетентен за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване;

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

13) „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 тези публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

14) „трета страна“ означава физическо или юридическо лице, публичен орган, агенция или друг орган, различен от субекта на данните, администратора, обработващия лични данни и лицата, които под прякото ръководство на администратора или на обработващия лични данни имат право да обработват личните данни;

15) „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

16) „нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

17) „генетични данни“ означава лични данни, свързани с наследените или придобити генетични белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

18) „биометрични данни“ означава лични данни, получени в резултат на специфично техническо обработване, които са свързани с физическите, физиологичните или поведенческите характеристики на дадено физическо лице и които позволяват или потвърждават уникалната идентификация на това физическо лице, като лицеви изображения или дактилоскопични данни;

19) „данни за здравословното състояние“ означава лични данни, свързани с физическото или психичното здраве на физическо лице, включително предоставянето на здравни услуги, които дават информация за здравословното му състояние;

20) „услуга на информационното общество“ означава услуга по смисъла на член 1, параграф 1, буква б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета ([1]);

21) „международна организация“ означава организация и нейните подчинени органи, регламентирана от международното публично право, или всеки друг орган, създаден чрез споразумение между две или повече държави или въз основа на такова споразумение;

22) „национален надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 51 от Регламент (ЕС) 2016/679 или съгласно член 41 от Директива (ЕС) 2016/680;

23) „ползвател“ означава всяко физическо лице, използващо мрежа или крайно устройство, които функционират под контрола на институция или орган на Съюза;

24) „указател“ означава обществено достъпен указател на ползвателите или вътрешен указател на ползвателите, който е наличен в институция или орган на Съюза или е споделен между институциите и органите на Съюза, независимо дали е на хартиен носител, или в електронна форма.

25) „електронна съобщителна мрежа“ означава преносна система, независимо дали базирана на постоянна инфраструктура, или на централизиран административен капацитет, и когато е приложимо — комутационно или маршрутизиращо оборудване и други ресурси, включително неактивни мрежови елементи, които позволяват преноса на сигнали посредством проводници, радиовълни, оптични или други електромагнитни способи, включително спътникови мрежи, фиксирани (с комутиране на канали и пакети, включително интернет) и мобилни наземни мрежи, електропроводни системи, доколкото са използвани за пренос на сигнали, мрежи, използвани за радио- и телевизионно разпръскване и кабелни телевизионни мрежи, независимо от типа на пренасяната информация;

26) „крайно устройство“ означава крайно устройство съгласно определението в член 1, точка 1 от Директива 2008/63/ЕО на Комисията ([2]).

ГЛАВА II

ОБЩИ ПРИНЦИПИ

Член 4

Принципи, свързани с обработването на лични данни

1. Личните данни:

а) се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“);

б) се събират за конкретни, изрично указани и законни цели и не се обработват по-нататък по начин, който е несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита, съгласно член 13, за несъвместимо с първоначалните цели („ограничение на целите“);

в) са адекватни, относими и не надхвърлят необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) са точни и при необходимост се актуализират; трябва да се предприемат всички разумни мерки, за да се гарантира незабавното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват („точност“);

([1]) Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г., установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ L 241, 17.9.2015 г., стр. 1).

([2]) Директива 2008/63/ЕО на Комисията от 20 юни 2008 г. относно конкуренцията на пазарите на крайни далекосъобщителни устройства (ОВ L 162, 21.6.2008 г., стр. 20).

д) се съхраняват във вид, който позволява идентифицирането на субектите на данните за период, не по-дълъг от необходимия за целите, за които се обработват личните данни; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 13, при условие че бъдат приложени подходящите технически и организационни мерки, предвидени в настоящия регламент с цел да бъдат гарантирани правата и свободите на субекта на данните („ограничение на съхранението“);

е) се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

2. Администраторът носи отговорност за спазването на параграф 1 и трябва да е в състояние да го докаже („отчетност“).

Член 5

Законосъобразност на обработването

1. Обработването е законосъобразно само ако и доколкото е приложимо поне едно от следните условия:

а) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официално правомощие, което е предоставено на институцията или органа на Съюза;

б) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

в) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

г) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

д) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице.

2. Основанието за обработването, посочено в параграф 1, букви а) и б), се установява в правото на Съюза.

Член 6

Обработване за друга съвместима цел

Когато обработването за други цели, различни от тези, за които първоначално са били събрани личните данни, не се извършва въз основа на съгласието на субекта на данните или на правото на Съюза, което представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на целите по член 25, параграф 1, администраторът, за да се увери дали обработването за други цели е съвместимо с първоначалната цел, за която са били събрани личните данни, *inter alia*, взема под внимание:

а) всяка връзка между целите, за които са били събрани личните данни, и целите на предвиденото по-нататъшно обработване;

б) контекста, в който са били събрани личните данни, по-специално във връзка с отношенията между субекта на данните и администратора;

в) естеството на личните данни, по-специално дали се обработват специални категории лични данни съгласно член 10, или се обработват лични данни, отнасящи се до присъди и престъпления, съгласно член 11;

г) възможните последствия от предвиденото по-нататъшно обработване за субектите на данните;

д) наличието на подходящи гаранции, които могат да включват криптиране или псевдонимизация.

Член 7

Условия за даване на съгласие

1. Когато обработването се извършва въз основа на съгласие, администраторът трябва да е в състояние да докаже, че субектът на данни е дал съгласие за обработване на личните му данни.

2. Ако съгласието на субекта на данните е дадено в рамките на писмена декларация, която се отнася и до други въпроси, искането за съгласие се представя по начин, който ясно да го отличава от другите въпроси, в разбираема и лесно достъпна форма, като се използва ясен и прост език. Никоя част от такава декларация, която представлява нарушение на настоящия регламент, не е обвързваща.

3. Субектът на данни има правото да оттегли съгласието си по всяко време. Оттеглянето на съгласието не засяга законосъобразността на обработването, основано на дадено съгласие преди неговото оттегляне. Преди да даде съгласие, субектът на данни трябва да бъде информиран за това. Оттеглянето на съгласие трябва да е също толкова лесно, колкото и даването му.

4. Когато се прави оценка дали съгласието е било свободно изразено, се отчита най-вече дали, *inter alia*, изпълнението на даден договор, включително предоставянето на дадена услуга, е поставено в зависимост от съгласието за обработване на лични данни, което не е необходимо за изпълнението на този договор.

Член 8

Условия, приложими за съгласието на дете във връзка с услугите на информационното общество

1. Когато се прилага член 5, параграф 1, буква г) във връзка с прякото предлагане на услуги на информационното общество на деца, обработването на данни на дете е законосъобразно, ако детето е поне на 13 години. Ако детето е под 13 години, това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или потвърдено от носещия родителска отговорност за детето.

2. В такива случаи администраторът полага разумни усилия за удостоверяване, че съгласието е дадено или потвърдено от носещия родителска отговорност за детето, като взема предвид наличната технология.

3. Параграф 1 не засяга общото договорно право на държавите членки като разпоредбите относно действителността, сключването или последиците от даден договор по отношение на дете.

Член 9

Предаване на лични данни на установени в Съюза получатели, различни от институции и органи на Съюза

1. Без да се засягат членове 4—6 и член 10, лични данни се предават само на установени в Съюза получатели, различни от институции и органи на Съюза, ако:

а) получателят установи, че данните са необходими за изпълнението на задача от обществен интерес или при упражняването на предоставени на получателя официални правомощия, или

б) получателят установи, че е необходимо данните да бъдат предадени за конкретна цел от обществен интерес, а администраторът, ако има някакво основание да се предполага, че законните интереси на субекта на данните могат да бъдат накърнени, установи, че е пропорционално личните данни да бъдат предадени специално за тази цел, след като е претеглил по безспорен начин различните противоречащи си интереси.

2. Когато администраторът започва предаването по силата на настоящия член, той доказва, че предаването на лични данни е необходимо и пропорционално за целите на предаването, като прилага критериите, определени в параграф 1, буква а) или буква б).

3. Институциите и органите на Съюза съгласуват правото на защита на личните данни с правото на достъп до документи в съответствие с правото на Съюза.

Член 10

Обработване на специални категории лични данни

1. Забранява се обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в професионални съюзи, както и обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравето или сексуалния живот и сексуалната ориентация на лицето.

2. Параграф 1 не се прилага, ако е налице едно от следните условия:

а) субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на Съюза се предвижда, че посочената в параграф 1 забрана не може да бъде отменена от субекта на данни;

б) обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила дотолкова, доколкото това е разрешено от правото на Съюза, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните;

в) обработването е необходимо, за да бъдат защитени жизненоважни интереси на субекта на данните или на друго лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

г) обработването се извършва в хода на законно упражняваните дейности и при подходящи мерки за защита от орган с нестопанска цел, който представлява интегрирана в дадена институция или орган на Съюза структура, с политическа, философска, религиозна или профсъюзна цел и при условие че обработването касае единствено членове или бивши членове на този орган или лица, които редовно контактуват с него във връзка с неговите цели, и че данните не се разкриват пред трета страна без съгласието на субектите на данните;

д) обработването е свързано с лични данни, които са направени по явен начин обществено достояние от субекта на данните;

е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато Съдът действа в качеството си на правораздаващ орган;

ж) обработването е необходимо по причини от важен обществен интерес на основание на правото на Съюза, което е пропорционално на набелязаната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;

з) обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинска диагноза, осигуряването на здравни или социални грижи или лечение или за целите на управлението на услугите и системите за здравеопазване или социални грижи на основание на правото на Съюза или съгласно договор с медицинско лице и при условията и гаранциите, посочени в параграф 3;

и) обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия, на основание на правото на Съюза, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна; или

й) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели на основание на правото на Съюза, което е пропорционално на набелязаната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

3. Личните данни, посочени в параграф 1, може да бъдат обработвани за целите, посочени в параграф 2, буква з), когато въпросните данни се обработват от или под ръководството на професионален работник, обвързан от задължението за опазване на професионална тайна по силата на правото на Съюза или на държава членка или на правилата, установени от националните компетентни органи, или от друго лице, което също е обвързано от задължение за опазване на тайна по силата на правото на Съюза или на държава членка или на правилата, установени от националните компетентни органи.

Член 11

Обработване на лични данни, свързани с присъди и престъпления

Обработването на лични данни, свързани с присъди и престъпления или със свързаните с тях мерки за сигурност въз основа на член 5, параграф 1, се извършва само под контрола на официален орган или когато обработването е разрешено от правото на Съюза, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни.

Член 12

Обработване, за което не се изисква идентифициране

1. Ако целите, за които администратор обработва лични данни, не изискват или вече не изискват идентифициране на субекта на данните от администратора, администраторът не е задължен да поддържа, да се сдобие с или да обработи допълнителна информация, за да идентифицира субекта на данни с единствената цел да бъде спазен настоящият регламент.

2. Когато в случаи, посочени в параграф 1 от настоящия член, администраторът може да докаже, че не е в състояние да идентифицира субекта на данни, администраторът уведомява съответно субекта на данни, ако това е възможно. В такива случаи членове 17 — 22 не се прилагат, освен когато субектът на данни, с цел да упражни правата си по тези членове, предостави допълнителна информация, позволяваща неговото идентифициране.

Член 13

Гаранции, свързани с обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели

Обработването за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели подлежи в съответствие с настоящия регламент на подходящи гаранции за правата и свободите на субекта на данни. Тези гаранции осигуряват наличието на технически и организационни мерки, по-специално с оглед на спазването на принципа на свеждане на данните до минимум. Мерките може да включват псевдонимизация, при условие че посочените цели могат да бъдат постигнати по този начин. Когато посочените цели могат да бъдат постигнати чрез по-нататъшно обработване, което не позволява или повече не позволява идентифицирането на субектите на данни, целите се постигат по този начин.

ГЛАВА III

ПРАВА НА СУБЕКТА НА ДАННИ

РАЗДЕЛ 1

Прозрачност и условия

Член 14

Прозрачна информация, комуникация и условия за упражняването на правата на субекта на данни

1. Администраторът предприема необходимите мерки за предоставяне на субекта на данните на всякаква информация по членове 15 и 16 и на всякаква комуникация по членове 17—24 и член 35, която се отнася до обработването, в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен и прост език, особено що се отнася до всяка информация, конкретно насочена към деца. Информацията се предоставя писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при условие че идентичността на субекта на данните е доказана с други средства.

2. Администраторът съдейства за упражняването на правата на субекта на данните по членове 17—24. В случаите, посочени в член 12, параграф 2, администраторът не отказва да предприеме действия по искане на субекта на данните за упражняване на правата му по членове 17—24, освен ако докаже, че не е в състояние да идентифицира субекта на данните.

3. Администраторът предоставя на субекта на данни информация относно действията, предприети във връзка с искане по членове 17—24, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането. При необходимост този срок може да бъде удължен с още два месеца, като се вземат предвид сложността и броят на исканията. Администраторът информира субекта на данните за всяко такова удължаване в срок от един месец от получаване на искането, като посочва и причините за забавянето. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако субектът на данни е поискал друго.

4. Ако администраторът не предприеме действия по искането на субекта на данни, администраторът уведомява субекта на данни без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до Европейския надзорен орган по защита на данните и търсене на защита по съдебен ред.

5. Информацията по членове 15 и 16 и всякаква комуникация и действия по членове 17—24 и член 35 се предоставят безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може да откаже да предприеме действия по искането. Администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

6. Без да се засягат разпоредбите на член 12, когато администраторът има основателни съмнения във връзка със самоличността на физическото лице, което подава искане по членове 17—23, той може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

7. Информацията, която трябва да се предостави на субектите на данни съгласно членове 15 и 16, може да бъде предоставена в комбинация със стандартизирани икони, чрез което по лесно видим, разбираем и ясно четим начин да се представи смислен преглед на планираното обработване. Ако иконите се представят в електронен вид, те трябва да бъдат машинночитаеми.

8. Ако Комисията приеме съгласно член 12, параграф 8 от Регламент (ЕС) 2016/679 делегирани актове за определяне на информацията, която трябва да бъде представена под формата на икони, и на процедурите за предоставяне на стандартизирани икони, институциите и органите на Съюза предоставят, когато е целесъобразно, в комбинация с тези стандартизирани икони информацията по членове 15 и 16 от настоящия регламент.

РАЗДЕЛ 2

Информация и достъп до лични данни

Член 15

Информация, предоставяна при събиране на лични данни от субекта на данните

1. Когато лични данни, свързани с даден субект на данни, се събират от субекта на данните, в момента на получаване на личните данни администраторът предоставя на субекта на данните цялата посочена по-долу информация:

а) самоличността и координатите за връзка на администратора;

б) координатите за връзка на длъжностното лице по защита на данните;

в) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването;

г) получателите или категориите получатели на личните данни, ако има такива;

д) когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или липсата на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 48, позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

2. Освен информацията, посочена в параграф 1, в момента на получаване на личните данни администраторът предоставя на субекта на данните следната допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване:

а) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

б) съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или когато е приложимо, право да се направи възражение срещу обработването или правото на преносимост на данните;

в) когато обработването се основава на член 5, параграф 1, буква г) или член 10, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

г) правото на подаване на жалба до Европейския надзорен орган по защита на данните;

д) дали предоставянето на лични данни е законоустановено или договорно изискване, или изискване, необходимо за сключването на договор, както и дали субектът на данните е длъжен да предостави личните данни и какви са евентуалните последствия, ако тези данни не бъдат предоставени;

е) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 24, параграфи 1 и 4, и поне в тези случаи — съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

3. Когато администраторът възнамерява да обработва по-нататък личните данни за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в параграф 2.

4. Параграфи 1, 2 и 3 не се прилагат, когато и доколкото субектът на данните вече разполага с информацията.

Член 16

Информация, предоставяна, когато личните данни не са получени от субекта на данните

1. Когато личните данни не са получени от субекта на данните, администраторът предоставя на субекта на данните следната информация:

а) самоличността и координатите за връзка на администратора;

б) координатите за връзка на длъжностното лице по защита на данните;

в) целите на обработването, за което са предназначени личните данни, както и правното основание за обработването;

г) съответните категории лични данни;

д) получателите или категориите получатели на личните данни, ако има такива;

е) когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или липсата на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно член 48, позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

2. Освен информацията, посочена в параграф 1, администраторът предоставя на субекта на данните следната допълнителна информация, необходима за осигуряване на добросъвестно и прозрачно обработване на данните по отношение на субекта на данните:

а) срока, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определяне на този срок;

б) съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или когато е приложимо, право да се направи възражение срещу обработването или правото на преносимост на данните;

в) когато обработването се основава на член 5, параграф 1, буква г) или член 10, параграф 2, буква а), съществуването на право на оттегляне на съгласието по всяко време, без да се засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

г) правото на подаване на жалба до Европейския надзорен орган по защита на данните;

д) източника на личните данни и ако е приложимо, дали данните са от обществено достъпен източник;

е) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 24, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

3. Администраторът предоставя информацията, посочена в параграфи 1 и 2:

а) в разумен срок след получаването на личните данни, но най-късно в срок до един месец, като се отчитат конкретните обстоятелства, при които личните данни се обработват;

б) ако данните се използват за връзка със субекта на данните, най-късно при осъществяване на първия контакт с този субект на данните; или

в) ако е предвидено разкриване пред друг получател, най-късно при разкриването на личните данни за първи път.

4. Когато администраторът възнамерява да обработва по-нататък личните данни за цел, различна от тази, за която са придобити, той предоставя на субекта на данните преди това по-нататъшно обработване информация за тази друга цел и всякаква друга необходима информация, както е посочено в параграф 2.

5. Параграфи 1—4 не се прилагат, когато и доколкото:

а) субектът на данните вече разполага с информацията;

б) предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия; по-специално за обработване на данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели или доколкото съществува вероятност задължението, посочено в параграф 1 от настоящия член, да направи невъзможно или сериозно да затрудни постигането на целите на това обработване;

в) получаването или разкриването е изрично установено от правото на Съюза, в което са предвидени подходящи мерки за защита на законните интереси на субекта на данните; или

г) личните данни трябва да останат поверителни при спазване на задължение за опазване на професионална тайна, което се урежда от правото на Съюза, включително законовото задължение за опазване на тайна.

6. В случаите по параграф 5, буква б) администраторът взема подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните, включително като предоставя обществен достъп до информацията.

Член 17

Право на достъп на субекта на данните

1. Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

а) целите на обработването;

б) съответните категории лични данни;

в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

д) съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

е) правото на подаване на жалба до Европейския надзорен орган по защита на данните;

ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

з) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 24, параграфи 1 и 4, и поне в тези случаи — съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

2. Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции по член 48 във връзка с предаването.

3. Администраторът предоставя копие от личните данни, които са в процес на обработване. Когато субектът на данни подава искане с електронни средства, информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни е поискал друго.

4. Правото на получаване на копие, посочено в параграф 3, не влияе неблагоприятно върху правата и свободите на други лица.

РАЗДЕЛ 3

Коригиране и изтриване

Член 18

Право на коригиране

Субектът на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването, субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнителна декларация.

Член 19

Право на изтриване (право „да бъдеш забравен“)

1. Субектът на данни има правото да поиска от администратора изтриване на свързаните с него лични данни без ненужно забавяне, а администраторът има задължението да изтрие без ненужно забавяне личните данни, когато е приложимо някое от следните основания:

а) личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;

б) субектът на данните оттегля своето съгласие, върху което се основава обработването на данните съгласно член 5, параграф 1, буква г) или член 10, параграф 2, буква а), и няма друго правно основание за обработването;

в) субектът на данните възразява срещу обработването съгласно член 23, параграф 1 и няма законни основания за обработването, които да имат предимство;

г) личните данни са били обработвани незаконосъобразно;

д) личните данни трябва да бъдат изтрити с цел спазването на правно задължение, което се прилага спрямо администратора;

е) личните данни са били събрани във връзка с предлагането на услуги на информационното общество по член 8, параграф 1.

2. Когато администраторът е направил личните данни обществено достояние и е задължен съгласно параграф 1 да изтрие личните данни, той, като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите или администраторите, различни от институции и органи на Съюза, обработващи личните данни, че субектът на данните е поискал изтриване от тези администратори на всички връзки, копия или реплики на тези лични данни.

3. Параграфи 1 и 2 не се прилагат, доколкото обработването е необходимо:

а) за упражняване на правото на свобода на изразяването и правото на информация;

б) за спазване на правно задължение, което се прилага спрямо администратора, или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора;

в) по причини от обществен интерес в областта на общественото здраве в съответствие с член 10, параграф 2, букви з) и и), както и член 10, параграф 3;

г) за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, доколкото съществува вероятност правото, посочено в параграф 1, да направи невъзможно или сериозно да затрудни постигането на целите на това обработване; или

д) за установяването, упражняването или защитата на правни претенции.

Член 20

Право на ограничаване на обработването

1. Субектът на данните има право да изиска от администратора ограничаване на обработването, когато е налице едно от следните условия:

а) точността на личните данни се оспорва от субекта на данните — за срок, който позволява на администратора да провери точността, включително пълнотата, на личните данни;

б) обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;

в) администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;

г) субектът на данните е възразил срещу обработването съгласно член 23, параграф 1 в очакване на проверка дали законните основания на администратора имат предимство пред интересите на субекта на данните.

2. Когато обработването е ограничено съгласно параграф 1, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции, или за защита на правата на друго физическо или юридическо лице, или поради важни причини от обществен интерес за Съюза или държава членка.

3. Когато субект на данните е изискал ограничаване на обработването съгласно параграф 1, администраторът го информира преди отмяната на ограничаването на обработването.

4. В автоматизираните регистри с лични данни ограничаването на обработването по принцип се осигурява с технически средства. Фактът, че обработването на личните данни е ограничено, се указва в регистъра по начин, който ясно показва, че личните данни не могат да се ползват.

Член 21

Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването

Администраторът съобщава за всяко извършено в съответствие с член 18, член 19, параграф 1 и член 20 коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия. Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Член 22

Право на преносимост на данните

1. Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на администратор, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от администратора, на когото личните данни са предоставени, когато:

а) обработването е основано на съгласие в съответствие с член 5, параграф 1, буква г) или член 10, параграф 2, буква а) или на договор съгласно член 5, параграф 1, буква в); и

б) обработването се извършва с автоматични средства.

2. Когато упражнява правото си на преносимост на данните по параграф 1, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг или към администратори, различни от институции и органи на Съюза, когато това е технически осъществимо.

3. Упражняването на правото, посочено в параграф 1 от настоящия член, не засяга член 19. Посоченото право не се отнася до обработването, необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

4. Правото, посочено в параграф 1, не влияе неблагоприятно върху правата и свободите на други лица.

РАЗДЕЛ 4

Право на възражение и автоматизирано вземане на индивидуални решения

Член 23

Право на възражение

1. Субектът на данните има право по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него, което се основава на член 5, параграф 1, буква а), включително профилиране, основаващо се на посочената разпоредба. Администраторът прекратява обработването на личните данни, освен ако докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

2. Най-късно в момента на първото осъществяване на контакт със субекта на данните той изрично се уведомява за съществуването на правото по параграф 1, което му се представя по ясен начин и отделно от всяка друга информация.

3. Без да се засягат членове 36 и 37, в контекста на използването на услугите на информационното общество субектът на данните може да упражнява правото си на възражение чрез автоматични средства, като се използват технически спецификации.

4. Когато лични данни се обработват за целите на научни или исторически изследвания или за статистически цели, субектът на данните има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, отнасящи се до него, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от обществен интерес.

Член 24

Автоматизирано вземане на индивидуални решения, включително профилиране

1. Субектът на данните има право да не бъде адресат на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за него или по подобен начин го засяга в значителна степен.

2. Параграф 1 не се прилага, ако решението:

а) е необходимо за сключването или изпълнението на договор между субекта на данни и администратора;

б) е разрешено от правото на Съюза, в което също се предвиждат подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните; или

в) се основава на изричното съгласие на субекта на данни.

3. В случаите, посочени в параграф 2, букви а) и в), администраторът прилага подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните, най-малко правото на човешка намеса от страна на администратора, правото да изрази гледната си точка и да оспори решението.

4. Решенията по параграф 2 от настоящия член не се основават на специалните категории лични данни, посочени в член 10, параграф 1, освен ако се прилага член 10, параграф 2, буква а) или буква ж) и са въведени подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните.

РАЗДЕЛ 5

Ограничения

Член 25

Ограничения

1. Правни актове, приети въз основа на Договорите, или по въпроси, свързани с дейността на институциите и органите на Съюза, вътрешни правила, установени от тези органи и институции, могат да ограничават прилагането на членове 14—22, членове 35 и 36, както и на член 4, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 14—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 гарантират:

а) националната сигурност, обществената сигурност или отбраната на държавите членки;

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

в) други важни цели от широк обществен интерес за Съюза или за държава членка, по-специално целите на общата външна политика и политика на сигурност на Съюза или важен икономически или финансов интерес на Съюза или на държава членка, включително паричните, бюджетните и данъчните въпроси, общественото здраве и социалната сигурност;

г) вътрешната сигурност на институциите и органите на Съюза, включително сигурността на техните електронни съобщителни мрежи;

д) защитата на независимостта на съдебната власт и съдебните производства;

е) предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регулираните професии;

ж) функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия в случаите, посочени в букви а)—в);

з) защитата на субекта на данните или на правата и свободите на други лица;

и) изпълнението по гражданскоправни претенции.

2. По-специално, всички правни актове или вътрешни правила, посочени в параграф 1, съдържат специални разпоредби, 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) спецификациите на администратора или на категориите администратори;

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

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

3. Когато личните данни се обработват за целите на научни или исторически изследвания или за статистически цели, в правото на Съюза, което може да включва вътрешни правила, приети от институции и органи на Съюза по въпроси, свързани с тяхната дейност, могат да бъдат предвидени дерогации от правата, посочени в членове 17, 18, 20 и 23, при спазване на условията и гаранциите, посочени в член 13, доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели и посочените дерогации са необходими за постигането на тези цели.

4. Когато личните данни се обработват за целите на архивирането в обществен интерес, в правото на Съюза, което може да включва вътрешни правила, приети от институции и органи на Съюза по въпроси, свързани с тяхната дейност, може да бъдат предвидени дерогации от правата, посочени в членове 17, 18, 20, 21, 22 и 23, при спазване на условията и гаранциите, посочени в член 13, доколкото има вероятност тези права да направят невъзможно или сериозно да затруднят постигането на конкретните цели и посочените дерогации са необходими за постигането на тези цели.

5. Вътрешните правила, посочени в параграфи 1, 3 и 4, са ясни и точни актове от общ характер, които са предназначени да породят правни последици по отношение на субектите на данни, приети са на най-високото равнище на управление на институциите и органите на Съюза и подлежат на публикуване в *Официален вестник на Европейския съюз*.

6. Ако бъде наложено ограничение съгласно параграф 1, субектът на данните се информира в съответствие с правото на Съюза за основните причини, на които се основава прилагането на ограничението, и за правото му да подаде жалба до Европейския надзорен орган по защита на данните.

7. Ако ограничение, наложено съгласно параграф 1, се използва за обосноваване на отказ на достъп на субекта на данните, при разглеждане на жалбата Европейският надзорен орган по защита на данните го информира единствено за това дали данните са били правилно обработени и ако не са, дали са извършени необходимите корекции.

8. Предоставянето на информацията, посочена в параграфи 6 и 7 от настоящия член и в член 45, параграф 2, може да бъде отложено, пропуснато или отказано, ако предоставянето би премахнало ефекта от ограничението, наложено съгласно параграф 1 от настоящия член.

ГЛАВА IV

АДМИНИСТРАТОР И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

РАЗДЕЛ 1

Общи задължения

Член 26

Отговорност на администратора

1. Като взема предвид естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът въвежда подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с настоящия регламент. Тези мерки се преразглеждат и при необходимост се актуализират.

2. Когато това е пропорционално на дейностите по обработване, посочените в параграф 1 мерки включват прилагане от страна на администратора на подходящи политики за защита на данните.

3. Придържането към одобрени механизми за сертифициране, посочени в член 42 от Регламент (ЕС) 2016/679, може да се използва като елемент, с който да се докаже спазването на задълженията на администратора.

Член 27

Защита на данните на етапа на проектирането и по подразбиране

1. Като взема предвид 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 на физическите лица, администраторът въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, например псевдонимизация, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и интегриране на необходимите гаранции в процеса на обработване, за да се спазят изискванията на настоящия регламент и да се осигури защита на правата на субектите на данни.

2. Администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по подразбиране се обработват само лични данни, които са необходими за всяка конкретна цел на обработването. Това задължение се отнася до обема на събраните лични данни, степента на обработването, срока на съхраняването им и тяхната достъпност. По-специално подобни мерки гарантират, че по подразбиране без намеса от страна на физическото лице личните данни не са достъпни за неограничен брой физически лица.

3. Като елемент за доказване на спазването на изискванията, предвидени в параграфи 1 и 2 от настоящия член, може да се използва одобрен механизъм за сертифициране съгласно член 42 от Регламент (ЕС) 2016/679.

Член 28

Съвместни администратори

1. Когато двама или повече администратори или един или повече администратори, или съвместно с един или повече администратори, различни от институции и органи на Съюза, съвместно определят целите и средствата на обработването, те са съвместни администратори. Те определят по прозрачен начин съответните си отговорности за изпълнение на задълженията си за защита на данните, по-специално що се отнася до упражняването на правата на субекта на данни и съответните си задължения за предоставяне на информацията, посочена в членове 15 и 16, посредством договореност помежду си, освен ако и доколкото съответните отговорности на съвместните администратори не са определени от правото на Съюза или правото на държава членка, което се прилага спрямо съвместните администратори. В договореността може да се посочи точка за контакт за субектите на данни.

2. Договореността, посочена в параграф 1, надлежно отразява съответните роли и връзки на съвместните администратори спрямо субектите на данни. Съществените характеристики на договореността са достъпни за субекта на данните.

3. Независимо от условията на договореността, посочена в параграф 1, субектът на данните може да упражнява своите права съгласно настоящия регламент по отношение на всеки и срещу всеки от администраторите.

Член 29

Обработващ личните данни

1. Когато обработването се извършва от името на даден администратор, администраторът използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на настоящия регламент и да гарантира защитата на правата на субектите на данни.

2. Обработващият лични данни не включва друг обработващ лични данни без предварителното конкретно или общо писмено разрешение на администратора. В случай на общо писмено разрешение обработващият лични данни винаги информира администратора за всякакви планирани промени за включване или замяна на други обработващи лични данни, като по този начин дава възможност на администратора да оспори тези промени.

3. Обработването от страна на обработващия лични данни се урежда с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни спрямо администратора и който регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни и задълженията и правата на администратора. В този договор или друг правен акт се предвижда по-специално, че обработващият лични данни:

а) обработва личните данни само по документирано нареждане на администратора, включително що се отнася до предаването на лични данни на трета държава или международна организация, освен когато е длъжен да направи това съгласно правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни; в такъв случай обработващият лични данни информира администратора за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес;

б) гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

в) взема всички необходими мерки съгласно член 33;

г) спазва условията по параграфи 2 и 4 за включване на друг обработващ лични данни;

д) като взема предвид естеството на обработването, подпомага администратора, доколкото е възможно, чрез подходящи технически и организационни мерки при изпълнението на задължението на администратора да отговори на искания за упражняване на предвидените в глава III права на субектите на данни;

е) подпомага администратора да гарантира изпълнението на задълженията съгласно членове 33—41, като отчита естеството на обработване и информацията, до която е осигурен достъп на обработващия лични данни;

ж) по избор на администратора заличава или връща на администратора всички лични данни след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка изисква тяхното съхранение;

з) осигурява достъп на администратора до цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити, включително проверки, от страна на администратора или друг одитор, оправомощен от администратора.

Предвид буква з) от първа алинея обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава настоящия регламент или други разпоредби на Съюза или на държавите членки относно защитата на данни.

4. Когато обработващ лични данни включва друг обработващ лични данни за извършването на специфични дейности по обработване от името на администратора, чрез договор или друг правен акт съгласно правото на Съюза или правото на държава членка на това друго лице се налагат същите задължения за защита на данните, както задълженията, предвидени в договора или друг правен акт между администратора и обработващия лични данни, както е посочено в параграф 3, по-специално да предостави достатъчно гаранции за прилагане на подходящи технически и организационни мерки, така че обработването да отговаря на изискванията на настоящия регламент. Когато другият обработващ лични данни не изпълни задължението си за защита на данните, първоначалният обработващ данните продължава да носи пълна отговорност пред администратора за изпълнението на задълженията на този друг обработващ лични данни.

5. Когато обработващ лични данни не е институция или орган на Съюза, придържането на този обработващ към одобрен кодекс за поведение, посочен в член 40, параграф 5 от Регламент (ЕС) 2016/679, или към одобрен механизъм за сертифициране, посочен в член 42 от Регламент (ЕС) 2016/679, може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграфи 1 и 4 от настоящия член.

6. Без да се засягат разпоредбите на индивидуален договор между администратора и обработващия лични данни, договорът или другият правен акт, посочени в параграфи 3 и 4 от настоящия член, може да се основават изцяло или отчасти на стандартни договорни клаузи, посочени в параграфи 7 и 8 от настоящия член, включително когато са част от сертифициране, предоставено на обработващия лични данни, различен от институция или орган на Съюза, съгласно член 42 от Регламент (ЕС) 2016/679.

7. Комисията може да установява стандартни договорни клаузи по въпроси, посочени в параграфи 3 и 4 от настоящия член, и в съответствие с процедурата по разглеждане, посочена в член 96, параграф 2.

8. Европейският надзорен орган по защита на данните може да приема стандартни договорни клаузи по въпросите, посочени в параграфи 3 и 4.

9. Договорът или другият правен акт, посочени в параграфи 3 и 4, се изготвят в писмена форма, включително в електронна форма.

10. Без да се засягат членове 65 и 66, ако обработващ лични данни наруши настоящия регламент, определяйки целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.

Член 30

Обработване под ръководството на администратора или обработващия лични данни

Обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването се изисква от правото на Съюза или правото на държава членка.

Член 31

Регистри на дейности по обработване

1. Всеки администратор поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа цялата по-долу посочена информация:

а) името и координатите за връзка на администратора, на длъжностното лице по защита на данните и когато е приложимо, на обработващия лични данни и на съвместните администратори;

б) целите на обработването;

в) описание на категориите субекти на данни и на категориите лични данни;

г) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в държави членки, трети държави или международни организации;

д) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация и документация за подходящите гаранции;

е) когато е възможно, предвидените срокове за изтриване на различните категории данни;

ж) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 33.

2. Всеки обработващ лични данни поддържа регистър на всички категории дейности по обработването, извършени от името на администратор, в който се съдържат:

а) името и координатите за връзка на обработващия или обработващите лични данни, на всеки администратор, от чието име действа обработващият лични данни, и на длъжностното лице за защита на данните;

б) категориите обработване, извършвано от името на всеки администратор;

в) когато е приложимо, предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация и документация за подходящите гаранции;

г) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 33.

3. Регистрите, посочени в параграфи 1 и 2, се поддържат в писмена форма, включително в електронен формат.

4. Институциите и органите на Съюза предоставят на Европейския надзорен орган по защита на данните достъп до регистрите при поискване от негова страна.

5. Освен ако това не е целесъобразно, като се има предвид размерът на институцията или органа на Съюза, институциите и органите на Съюза съхраняват своите регистри на дейностите по обработване в централен регистър. Те предоставят обществен достъп до този регистър.

Член 32

Сътрудничество с Европейския надзорен орган по защита на данните

При поискване от Европейския надзорен орган по защита на данните институциите и органите на Съюза му сътрудничат при изпълнението на неговите задачи.

РАЗДЕЛ 2

Сигурност на личните данни

Член 33

Сигурност на обработването

1. Като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, включително, *inter alia*, когато е целесъобразно:

а) псевдонимизация и криптиране на личните данни;

б) способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване;

в) способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент;

г) процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

2. При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването, по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

3. Администраторът и обработващият лични данни предприемат стъпки всяко физическо лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до лични данни, да обработва тези данни само по указание на администратора, освен ако от въпросното лице се изисква да прави това по силата на правото на Съюза.

4. Придържането към одобрен механизъм за сертифициране, посочен в член 42 от Регламент (ЕС) 2016/679, може да се използва като елемент, за да се докаже спазването на изискванията, предвидени в параграф 1 от настоящия член.

Член 34

Уведомяване на Европейския надзорен орган по защита на данните за нарушение на сигурността на личните данни

1. В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни Европейския надзорен орган по защита на данните, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до Европейския надзорен орган по защита на данните съдържа причините за забавянето, когато не е подадено в срок от 72 часа.

2. Обработващият лични данни уведомява администратора без ненужно забавяне, след като узнае за нарушаване на сигурността на лични данни.

3. В уведомлението, посочено в параграф 1, се съдържа най-малко следното:

а) описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителният брой на засегнатите записи на лични данни;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

4. Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

5. Администраторът уведомява длъжностното лице по защита на данните за нарушението на сигурността на личните данни.

6. Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на Европейския надзорен орган по защита на данните да провери дали е спазен настоящият член.

Член 35

Съобщаване на субекта на данните за нарушение на сигурността на личните данни

1. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът без ненужно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни.

2. В съобщението до субекта на данните, посочено в параграф 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се посочват най-малко информацията и мерките, посочени в член 34, параграф 3, букви б), в) и г).

3. Посоченото в параграф 1 съобщение до субекта на данните не се изисква, ако е изпълнено някое от следните условия:

а) администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

б) администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се осъществи високият риск за правата и свободите на субектите на данни, посочен в параграф 1;

в) то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

4. Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, Европейският надзорен орган по защита на данните може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията, посочени в параграф 3.

РАЗДЕЛ 3

Поверителност на електронните съобщения

Член 36

Поверителност на електронните съобщения

Институциите и органите на Съюза гарантират поверителността на електронните съобщения, по-специално като осигуряват сигурността на своите електронни съобщителни мрежи.

Член 37

Защита на информацията, предавана към, съхранявана в, свързана с, обработвана и събирана от крайните устройства на ползвателите

Институциите и органите на Съюза защитават информацията, предавана към, съхранявана в, свързана с, обработвана и събирана от крайните устройства на ползвателите, осъществяващи достъп до техните обществено достъпни уебсайтове и мобилни приложения в съответствие с член 5, параграф 3 от Директива 2002/58/ЕО.

Член 38

Указатели на ползвателите

1. Личните данни, които се съдържат в указатели на ползвателите, както и достъпът до такива указатели се ограничават до степента, която е строго необходима за специфичните цели на указателите.

2. Институциите и органите на Съюза предприемат всички необходими мерки за предотвратяване на използването на съдържащите се в посочените указатели лични данни за целите на директния маркетинг, независимо дали те са достъпни за обществеността или не.

РАЗДЕЛ 4

Оценка на въздействието върху защитата на данните и предварителни консултации

Член 39

Оценка на въздействието върху защитата на данните

1. Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.

2. При извършването на оценка на въздействието върху защитата на данните администраторът иска становището на длъжностното лице по защита на данните.

3. Оценката на въздействието върху защитата на данните, посочена в параграф 1, се изисква по-специално в случай на:

а) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматизирано обработване, включително профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

б) мащабно обработване на специални категории данни, посочени в член 10, или на свързани с присъди и престъпления лични данни, посочени в член 11; или

в) систематично мащабно наблюдение на публично достъпна зона.

4. Европейският надзорен орган по защита на данните съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно параграф 1.

5. Европейският надзорен орган по защита на данните може също да състави и оповести списък на видовете операции по обработване, за които не се изисква оценка на въздействието върху защитата на данните.

6. Преди приемането на списъците, посочени в параграфи 4 и 5 от настоящия член, Европейският надзорен орган по защита на данните отправя искане до Европейския комитет по защита на данните, създаден с член 68 от Регламент (ЕС) 2016/679, да проучи тези списъци в съответствие с член 70, параграф 1, буква д) от посочения регламент, когато тези списъци се отнасят до операции по обработване от администратор, действащ съвместно с един или повече администратори, различни от институции и органи на Съюза.

7. Оценката съдържа най-малко:

а) системен опис на предвидените операции по обработване и целите на обработването;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1; и

г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за гарантиране на защитата на личните данни и за доказване на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други засегнати лица.

8. При оценката на въздействието на операциите по обработване, извършвани от съответните обработващи лични данни, различни от институции и органи на Съюза, надлежно се отчита и спазването от тяхна страна на одобрените кодекси за поведение, посочени в член 40 от Регламент (ЕС) 2016/679, по-специално за целите на оценката на въздействието върху защитата на данните.

9. Когато е целесъобразно, администраторът се обръща към субектите на данните или техните представители за становище относно планираното обработване, без да се засяга защитата на обществените интереси или сигурността на операциите по обработване.

10. Когато обработването съгласно член 5, параграф 1, буква а) или б) има правно основание в правен акт, приет въз основа на Договорите, който регулира конкретната операция по обработване или набор от такива операции, и вече е извършена оценка на въздействието върху защитата на личните данни като част от общата оценка на въздействието, предшестваща приемането на въпросния правен акт, параграфи 1 6 от настоящия член не се прилагат, освен ако във въпросния правен акт не е предвидено друго.

11. При необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване.

Член 40

Предварителна консултация

1. Администраторът се консултира с Европейския надзорен орган по защита на данните преди обработването, когато оценката на въздействието върху защитата на данните съгласно член 39 покаже, че при липса на гаранции, мерки за сигурност и механизми за ограничаване на риска обработването би довело до висок риск за правата и свободите на физическите лица, и администраторът счита, че рискът не може да бъде ограничен с разумни средства с оглед на наличните технологии и разходи за прилагане. Администраторът иска становището на длъжностното лице по защита на данните относно необходимостта от предварителна консултация.

2. Когато Европейският надзорен орган по защита на данните е на мнение, че планираното обработване, посочено в параграф 1, нарушава настоящия регламент, особено когато администраторът не е идентифицирал или ограничил риска в достатъчна степен, Европейският надзорен орган по защита на данните в срок до осем седмици от получаване на искането за консултация дава писмено становище на администратора и когато е приложимо, на обработващия лични данни, като може да използва всяко от правомощията си, посочени в член 58. Този срок може да бъде удължен с още шест седмици предвид сложността на планираното обработване. Европейският надзорен орган по защита на данните информира администратора и когато е приложимо, обработващия лични данни за такова удължаване в срок от един месец от получаване на искането за консултация, включително за причините за забавянето. Тези срокове могат да бъдат спрени, докато Европейският надзорен орган по защита на данните получи поисканата от него информация за целите на консултацията.

3. Когато се консултира с Европейския надзорен орган по защита на данните в съответствие с параграф 1, администраторът предоставя на Европейския надзорен орган по защита на данните следната информация:

а) когато е приложимо — информация за съответните отговорности на администратора, съвместните администратори и обработващите лични данни, участващи в обработването;

б) целите на планираното обработване и средствата за него;

в) предвидените мерки и гаранции за защита на правата и свободите на субектите на данни съгласно настоящия регламент;

г) координатите за връзка на длъжностното лице по защита на данните;

д) оценката на въздействието върху защитата на данните, предвидена в член 39; и

е) всякаква друга информация, поискана от Европейския надзорен орган по защита на данните.

4. Комисията може посредством акт за изпълнение да определи списък от случаи, в които администраторите трябва да се консултират с Европейския надзорен орган по защита на данните или да получат неговото предварително разрешение във връзка с обработването на лични данни за целите на изпълнението на задача, осъществявана от администратора в обществен интерес, включително обработването на такива данни във връзка със социалната закрила и общественото здраве.

РАЗДЕЛ 5

Информация и законодателни консултации

Член 41

Информация и консултации

1. Институциите и органите на Съюза информират Европейския надзорен орган по защита на данните при изготвяне на административни мерки и вътрешни правила във връзка с обработването на лични данни от институция или орган на Съюза, независимо дали това обработване става самостоятелно или съвместно с други.

2. Институциите и органите на Съюза провеждат консултации с Европейския надзорен орган по защита на данните, когато изготвят вътрешните правила, посочени в член 25.

Член 42

Законодателни консултации

1. След приемането на предложения за законодателен акт и на препоръки или предложения до Съвета съгласно член 218 от ДФЕС или при подготовката на делегирани актове или актове за изпълнение„ Комисията се консултира с Европейския надзорен орган по защита на данните, когато има въздействие върху защитата на правата и свободите на физическите лица по отношение на обработването на лични данни.

2. Когато акт, посочен в параграф 1, има особено значение за защита на правата и свободите на физическите лица по отношение на обработката на лични данни, Комисията може също така да се консултира с Европейския комитет по защита на данните. В тези случаи Европейският надзорен орган по защита на данните и Европейския комитет по защита на данните координират работата си с оглед на издаването на съвместно становище.

3. Консултациите, посочени в параграфи 1 и 2, се предоставят в писмена форма в срок до осем седмици от получаване на искането за провеждане на консултация, посочена в параграфи 1 и 2. В спешни случаи или при друга необходимост Комисията може да съкрати крайния срок.

4. Настоящият член не се прилага, когато Комисията е длъжна в съответствие с Регламент (ЕС) 2016/679 да се консултира с Европейския комитет по защита на данните.

РАЗДЕЛ 6

Длъжностно лице по защита на данните

Член 43

Определяне на длъжностното лице по защита на данните

1. Всяка институция или орган на Съюза определя длъжностно лице по защита на данните.

2. Няколко институции и органи на Съюза могат да определят за себе си едно-единствено длъжностно лице по защита на данните, като вземат предвид своите организационна структура и размер.

3. Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите, посочени в член 45.

4. Длъжностното лице по защита на данните е член на персонала на институцията или органа на Съюза. Като се вземе предвид числения им състав и ако не е упражнено правото на избор посочено в параграф 2, институциите и органите на Съюза могат да определят длъжностно лице по защита на данните, което да изпълнява задачите си въз основа на договор за услуги.

5. Институциите и органите на Съюза публикуват координатите за връзка на длъжностното лице по защита на данните и ги съобщават на Европейския надзорен орган по защита на данните.

Член 44

Длъжност на длъжностното лице по защита на данните

1. Институциите и органите на Съюза гарантират, че длъжностното лице по защита на данните участва по подходящ начин и своевременно по всички въпроси, свързани със защитата на личните данни.

2. Институциите и органите на Съюза подпомагат длъжностното лице по защита на данните при изпълнението на посочените в член 45 задачи, като осигуряват ресурсите, необходими за изпълнението на тези задачи, и достъп до личните данни и операциите по обработване, а така също поддържат неговите експертни знания.

3. Институциите и органите на Съюза гарантират, че длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на тези задачи. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни.

4. Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно настоящия регламент.

5. Длъжностното лице по защита на данните и неговият персонал са длъжни да спазват секретността или поверителността на изпълняваните от тях задачи в съответствие с правото на Съюза.

6. Длъжностното лице по защита на данните може да изпълнява и други задачи и задължения. Администраторът или обработващият лични данни гарантира, че тези задачи и задължения не водят до конфликт на интереси.

7. Администраторът и обработващият личните данни, съответният комитет по персонала и всяко физическо лице могат да се консултират с длъжностното лице по защита на данните по всеки въпрос, отнасящ се до тълкуването или прилагането на настоящия регламент, без да е необходимо да следват официална процедура. Никой не трябва да претърпява неблагоприятни последици, поради това че е отнесъл до вниманието на компетентното длъжностно лице по защита на данните въпрос, твърдейки за наличие на извършено нарушение на разпоредбите на настоящия регламент.

8. Длъжностното лице по защита на данните се назначава за срок от три до пет години и може да бъде преназначавано. Длъжностното лице по защита на данните може да бъде освободено от длъжността от институцията или органа на Съюза, който го е назначил, ако престане да отговаря на необходимите условия за изпълнение на своите задължения, само със съгласието на Европейския надзорен орган по защита на данните.

9. След назначаване на длъжностното лице по защита на данните институцията или органът, който го е назначил, го регистрира при Европейския надзорен орган по защита на данните.

Член 45

Задачи на длъжностното лице по защита на данните

1. Длъжностното лице по защита на данните изпълнява следните задачи:

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения съгласно настоящия регламент и други разпоредби на Съюза за защитата на данните;

б) да осигурява по независим начин вътрешното прилагане на настоящия регламент, да наблюдава спазването на настоящия регламент, на други разпоредби за защитата на данните, съдържащи се в правото на Съюза, и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

в) да гарантира, че субектите на данните са информирани за своите права и задължения съгласно настоящия регламент;

г) да предоставя при поискване съвети във връзка с необходимостта от уведомяване или съобщаване за нарушение на сигурността на личните данни съгласно членове 34 и 35;

д) да предоставя при поискване съвети във връзка с оценката на въздействието върху защитата на данните и наблюдава извършването на оценката съгласно член 39, и да се консултира с Европейския надзорен орган по защита на данните в случай на съмнение относно необходимостта от оценка на въздействието върху защитата на данните;

е) да предоставя при поискване съвети във връзка с необходимостта от предварителна консултация с Европейския надзорен орган по защита на данните съгласно член 40; и да се консултира с Европейския надзорен орган по защита на данните в случай на съмнение относно необходимостта от предварителна консултация;

ж) да отговаря на запитвания от страна на Европейския надзорен орган по защита на данните; в рамките на своята компетентност, си сътрудничи с Европейския надзорен орган по защита на данните по негово искане или по своя собствена инициатива;

з) да гарантира, че операциите по обработка не засягат неблагоприятно правата и свободите на субектите на данни.

2. Длъжностното лице по защита на данните може да отправя на администратора и на обработващия лични данни препоръки за практическото подобряване на защитата на данните и да ги съветва по въпроси, свързани с прилагането на разпоредби относно защитата на данните. Освен това длъжностното лице по защита на данните може по своя инициатива или по искане на администратора или на обработващия лични данни, на съответния комитет по персонала или на всяко физическо лице да разследва пряко свързани с неговите задачи въпроси и факти, достигнали до знанието му, и да докладва обратно на лицето, което е възложило разследването, или на администратора или обработващия лични данни.

3. Всяка институция или орган на Съюза приема допълнителни правила за прилагане, отнасящи се до длъжностното лице по защита на данните. Правилата за прилагане се отнасят в частност до задачите, задълженията и правомощията на длъжностното лице по защита на данните.

ГЛАВА V

ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Член 46

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 ако при спазване на другите разпоредби на настоящия регламент, 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 гарантира, че нивото на защита на физическите лица, гарантирано от настоящия регламент, не се излага на риск.

Член 47

Предаване на данни въз основа на решение относно адекватното ниво на защита

1. Предаване на лични данни на трета държава или на международна организация може да се осъществява, ако Комисията е решила в съответствие с член 45, параграф 3 от Регламент (ЕС) 2016/679 или член 36, параграф 3 от Директива (ЕС) 2016/680, че съответната трета държава, територия, или един или повече конкретни сектори в тази трета държава или съответната международна организация осигуряват адекватно ниво на защита и ако личните данни се предават единствено, за да стане възможно изпълнението на задачи от компетентността на администратора.

2. Институциите и органите на Съюза информират Комисията и Европейския надзорен орган по защита на данните за случаи, в които те считат, че съответната трета държава, територия, или един или повече конкретни сектори в трета държава, или съответната международна организация не осигурява адекватно ниво на защита по смисъла на параграф 1.

3. Институциите и органите на Съюза предприемат необходимите мерки, за да се съобразят с взетите от Комисията решения, когато съгласно член 45, параграфи 3 или 5 от Регламент (ЕС) 2016/679 или член 36, параграф 3 или 5 от Директива (ЕС) 2016/680, тя установява, че дадена трета държава територия, или един или повече конкретни сектори в трета държава, или международна организация осигурява или вече не осигурява адекватно ниво на защита.

Член 48

Предаване на данни, обвързани с подходящи гаранции

1. При липса на решение съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 или съгласно член 36, параграф 3 от Директива (ЕС) 2016/680, администраторът или обработващият лични данни може да предава лични данни на трета държава или на международна организация само ако администраторът или обработващият лични данни са предвидили подходящи гаранции и при условие че на субекта на данни са предоставени изпълняеми права в това негово качество и ефективни правни средства за защита.

2. Подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени, без да се изисква специално разрешение от Европейския надзорен орган по защита на данните, посредством:

а) правно обвързващ инструмент с изпълнителна сила между публичните органи или структури;

б) стандартни клаузи за защита на данните, приети от Комисията в съответствие с процедурата по разглеждане, посочена в член 96, параграф 2;

в) стандартни клаузи за защита на данните, приети от Европейския надзорен орган по защита на данните и одобрени от Комисията съгласно процедурата по разглеждане, посочена в член 96, параграф 2;

г) когато обработващият лични данни не е институция или орган на Съюза, задължителни фирмени правила, кодекси за поведение и механизъм за сертифициране съгласно член 46, параграф 2, букви б), д) и е) от Регламент (ЕС) 2016/679.

3. При условие че Европейският надзорен орган по защита на данните 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 изпълняеми и ефективни права на субектите на данни.

4. Разрешенията, издадени от Европейския надзорен орган по защита на данните въз основа на член 9, параграф 7 от Регламент (ЕО) № 45/2001, остават валидни, докато не бъдат изменени, заменени или отменени, ако е необходимо, от Европейския надзорен орган по защита на данните.

5. Институциите и органите на Съюза информират Европейския надзорен орган по защита на данните за категориите случаи, в които настоящият член е бил приложен.

Член 49

Неразрешено от правото на Съюза предаване или разкриване на данни

Всяко решение на съд или трибунал и всяко решение на административен орган на трета държава, с което от администратор или обработващ лични данни се изисква да предаде или разкрие лични данни, могат да бъдат признати или да подлежат на изпълнение по какъвто и да било начин само ако се основават на международно споразумение, като договор за правна взаимопомощ, което е в сила между третата държава, отправила искането, и Съюза, без да се засягат другите основания за предаване на данни съгласно настоящата глава.

Член 50

Дерогации за особени случаи

1. При липсата на решение относно адекватното ниво на защита съгласно член 45, параграф 3 от Регламент (ЕС) 2016/679 или съгласно член 36, параграф 3 от Директива (ЕС) 2016/680 или на подходящи гаранции съгласно член 48 от настоящия регламент, 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 него 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; или

ж) предаването се извършва от регистър, който съгласно правото на Съюза е предназначен за предоставяне на информация на обществеността и е открит за извършване на справки от широката общественост или от всяко лице, което може да докаже законен интерес, но само при условие че в конкретния случай са изпълнени предвидените в правото на Съюза условия за извършване на справки.

2. Параграф 1, букви а), б) и в) не се прилага за дейности, извършвани от институциите и органите на Съюза при упражняването на техните публични правомощия.

3. Общественият интерес, посочен в параграф 1, буква г), трябва да е признат в правото на Съюза.

4. Предаването съгласно параграф 1, буква ж) не трябва да включва всички лични данни или всички категории лични данни, съдържащи се в регистъра, освен ако това е разрешено от правото на Съюза. 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.

5. При липсата на решение относно адекватното ниво на защита правото на Съюза може по важни причини от обществен интерес изрично да определи ограничения за предаването на специални категории от лични данни на трета държава или международна организация.

6. Институциите и органите на Съюза информират Европейския надзорен орган по защита на данните за категориите случаи, в които настоящият член е бил приложен.

Член 51

Международно сътрудничество за защита на личните данни

По отношение на трети държави и международни организации Европейският надзорен орган по защита на данните, в сътрудничество с Комисията и Европейския комитет по защита на данните, предприема подходящи мерки за:

а) разработване на механизми за международно сътрудничество с цел подпомагане ефективното прилагане на законодателството за защита на личните данни;

б) осигуряване на международна взаимопомощ при прилагането на законодателството за защита на личните данни, включително чрез уведомяване, препращане на жалби, помощ при разследвания и обмен на информация, при условие че има подходящи гаранции за защитата на личните данни и другите основни права и свободи;

в) включване на съответните заинтересовани страни в обсъждания и дейности, насочени към насърчаване на международното сътрудничество за прилагането на законодателството за защита на личните данни;

г) насърчаване на обмена и документирането на законодателството и практиките в областта на защитата на личните данни, включително относно спорове за компетентност с трети държави.

ГЛАВА VI

ЕВРОПЕЙСКИ НАДЗОРЕН ОРГАН ПО ЗАЩИТА НА ДАННИТЕ

Член 52

Европейският надзорен орган за защита на личните данни;

1. Създава се Европейският надзорен орган по защита на данните.

2. По отношение на обработването на лични данни задачата на Европейския надзорен орган по защита на данните е да гарантира спазването от страна на институциите и органите на Съюза на основните права и свободи на физическите лица, и по-специално правото им на защита на данните.

3. Европейският надзорен орган по защита на данните отговаря за наблюдението и гарантирането на прилагането на разпоредбите на настоящия регламент и всеки друг акт на Съюза, който се отнася до защитата на основните права и свободи на физическите лица по отношение на обработването на лични данни от институция или орган на Съюза, както и за предоставянето на консултации на институциите и органите на Съюза и субектите на данни по всички въпроси, свързани с обработването на лични данни. За тази цел Европейският надзорен орган по защита на данните изпълнява задачите, определени в член 57, и упражнява правомощията, предоставени съгласно член 58.

4. Регламент (ЕО) № 1049/2001 се прилага по отношение на документите, съхранявани от Европейския надзорен орган по защита на данните. Европейският надзорен орган по защита на данните приема подробни правила за прилагането на Регламент (ЕО) № 1049/2001 по отношение на тези документи.

Член 53

Назначаване на Европейския надзорен орган по защита на данните

1. Европейският надзорен орган по защита на данните се назначава с общо съгласие от Европейския парламент и Съвета за срок от пет години въз основа на съставен от Комисията списък след публично отправена покана за представяне на кандидатури. Поканата за представяне на кандидатури предоставя възможност на всички заинтересовани страни в Съюза да представят своите кандидатури. Съставеният от Комисията списък на кандидатите е публичен и включва най-малко трима кандидати. Въз основа на списъка, съставен от Комисията, компетентната комисия на Европейския парламент може да реши да проведе изслушване, за да получи възможност да изрази предпочитанията си.

2. Списъкът от кандидатите, посочен в параграф 1, се състои от лица, чиято независимост не подлежи на съмнение и за които е признато, че притежават експертни познания в областта на защитата на данни, както и необходимите опит и умения, за да изпълняват задълженията на Европейски надзорен орган по защита на данните.

3. Мандатът на Европейския надзорен орган по защита на данните може да бъде подновен еднократно.

4. Задълженията на Европейския надзорен орган по защита на данните се прекратяват при следните обстоятелства:

а) ако Европейският надзорен орган по защита на данните бъде сменен;

б) ако Европейският надзорен орган по защита на данните подаде оставка:

в) ако Европейският надзорен орган по защита на данните бъде освободен от длъжност или ако подлежи на задължително пенсиониране.

5. Европейският надзорен орган по защита на данните може да бъде освободен от длъжност или лишен от правото на пенсия или други заместващи пенсията облаги от Съда по искане на Европейския парламент, Съвета или Комисията, ако престане да отговаря на необходимите условия за изпълнение на своите задължения или в случай на тежко провинение.

6. В случай на нормална смяна или доброволна оставка Европейският надзорен орган по защита на данните въпреки всичко продължава да заема длъжността си, докато бъде сменен.

7. Разпоредбите на членове 11 — 14 и член 17 от Протокола за привилегиите и имунитетите на Европейския съюз се прилагат за Европейския надзорен орган защита на данните.

Член 54

Правилник и общи условия за изпълнение на задълженията на Европейския надзорен орган по защита на данните, персонал и финансови средства

1. Счита се, че Европейският надзорен орган по защита на данните има статут, равностоен на този на съдия от Съда, що се отнася до определяне на размера на възнаграждението, надбавките, пенсията за осигурителен стаж и възраст и всякакви други обезщетения, които заместват възнаграждението.

2. Бюджетният орган гарантира осигуряването на Европейския надзорен орган по защита на данните на необходимите за изпълнение на неговите задачи човешки и финансови ресурси.

3. Бюджетът на Европейския надзорен орган по защита на данните фигурира в отделна бюджетна позиция в раздела за административни разходи на общия бюджет на Съюза.

4. Европейският надзорен орган по защита на данните се подпомага от секретариат. Длъжностните лица и другите служители в секретариата се назначават от Европейския надзорен орган по защита на данните, който е и техен ръководител. Те са изцяло под негово ръководство. Числеността на персонала се определя всяка година като част от бюджетната процедура. Член 75, параграф 2 от Регламент (ЕС) 2016/679 се прилага за служителите на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачите, възложени на Европейския комитет по защита на данните съгласно правото на Съюза.

5. За длъжностните лица и другите служители в секретариата на Европейския надзорен орган по защита на данните се прилагат правилата и разпоредбите, приложими за длъжностните лица и другите служители на Съюза.

6. Седалището на Европейския надзорен орган по защита на данните е в Брюксел.

Член 55

Независимост

1. Европейският надзорен орган по защита на данните действа напълно независимо при изпълнението на задачите си и упражняването на правомощията си съгласно настоящия регламент.

2. При изпълнението на задачите си и упражняването на правомощията си в съответствие с настоящия регламент Европейският надзорен орган по защита на данните остава независим от външно влияние, било то пряко или непряко, и нито търси, нито приема инструкции от когото и да било.

3. Европейският надзорен орган по защита на данните се въздържа от всякакви несъвместими със задълженията му действия и по време на своя мандат не упражнява никакви други дейности, независимо дали срещу възнаграждение, или безвъзмездно.

4. След приключване на мандата си Европейският надзорен орган по защита на данните проявява почтеност и въздържаност относно приемането на постове и облаги.

Член 56

Професионална тайна

По време и след приключване на техния мандат за Европейския надзорен орган по защита на данните и за неговия персонал се прилага задължението за опазване на професионалната тайна по отношение на всякаква поверителна информация, която е стигнала до тяхното знание в хода на изпълнение на служебните им задължения.

Член 57

Задачи

1. Без да се засягат останалите задачи, определени в настоящия регламент, Европейският надзорен орган по защита на данните:

а) наблюдава и осигурява прилагането на настоящия регламент от институциите и органите на Съюза, с изключение на обработването на лични данни от Съда при изпълнение на съдебните му функции;

б) насърчава обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработването. Обръща се специално внимание на дейностите, специално насочени към децата;

в) насърчава информираността на администраторите и обработващите лични данни за задълженията им съгласно настоящия регламент;

г) при поискване предоставя информация на всеки субект на данни във връзка с упражняването на правата му съгласно настоящия регламент и ако е необходимо, си сътрудничи за тази цел с националните надзорни органи;

д) разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение в съответствие с член 67, и разследва предмета на жалбата, доколкото това е целесъобразно, и информира жалбоподателя за напредъка и резултатите от разследването в разумен срок, по-специално ако е необходимо по-нататъшно разследване или координиране с друг надзорен орган;

е) извършва разследвания относно прилагането на настоящия регламент, включително въз основа на информация, получена от друг надзорен или публичен орган;

ж) по собствена инициатива или при поискване съветва всички институции и органи на Съюза относно законодателни и административни мерки, отнасящи се до защитата на правата и свободите на физическите лица по отношение на обработването на лични данни;

з) наблюдава развитието по-специално в областта на информационните и комуникационни технологии дотолкова, доколкото те имат въздействие върху защитата на личните данни;

и) приема стандартните договорни клаузи, посочени в член 29, параграф 8 и член 48, параграф 2, буква в);

й) съставя и поддържа списък във връзка с изискването за оценка на въздействието върху защитата на данните съгласно член 39, параграф 4;

к) участва в дейностите на Европейския комитет по защита на данните;

л) осигурява секретариата на Европейския комитет по защита на данните в съответствие с член 75 от Регламент (ЕС) 2016/679;

м) дава становища по обработването, посочено в член 40, параграф 2;

н) дава разрешение за договорните клаузи и разпоредбите, посочени в член 48, параграф 3;

о) поддържа вътрешен регистър на нарушенията на настоящия регламент, както и на предприетите мерки в съответствие с член 58, параграф 2;

п) изпълнява други задачи, свързани със защитата на лични данни; както и

р) приема свой процедурен правилник.

2. Европейският надзорен орган по защита на данните улеснява подаването на жалбите, посочени в параграф 1, буква д), посредством формуляр за подаване на жалби, който може да бъде попълнен и по електронен път, без да се изключват други средства за комуникация.

3. Изпълнението на задълженията на Европейския надзорен орган по защита на данните е безплатно за субекта на данни.

4. Когато исканията са явно неоснователни или прекомерни, по-специално поради своята повторяемост, Европейският надзорен орган по защита на данните може да откаже да предприеме действия по искането. Европейският надзорен орган по защита на данните носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

Член 58

Правомощия

1. Европейският надзорен орган по защита на данните има следните правомощия за разследване:

а) да разпорежда на администратора и на обработващия лични данни да предоставят всяка информация, която той поиска за изпълнението на своите задачи;

б) да провежда разследвания под формата на одити във връзка със защитата на данните;

в) да уведомява администратора или обработващия лични данни за предполагаемо нарушение на настоящия регламент;

г) да получава от администратора и обработващия лични данни достъп до всички лични данни и до цялата информация, от която се нуждае за изпълнението на своите задачи;

д) да получава достъп до всички помещения на администратора и обработващия лични данни, включително до всяко оборудване и средства за обработване на данни, в съответствие с правото на Съюза.

2. Европейският надзорен орган по защита на данните има следните корективни правомощия:

а) да отправя предупреждения до администратора или обработващия лични данни, когато има вероятност операциите по обработване на данни, които те възнамеряват да извършат, да нарушат разпоредбите на настоящия регламент;

б) да отправя официално предупреждение до администратора или обработващия лични данни, когато операции по обработване на данни са нарушили разпоредбите на настоящия регламент;

в) да отнася въпросите до администратора или обработващия лични данни, а при необходимост и до Европейския парламент, Съвета и Комисията;

г) да разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;

д) да разпорежда на администратора или обработващия лични данни да съобразят операциите по обработване на данни с разпоредбите на настоящия регламент и, ако е целесъобразно, това да стане по указан начин и в определен срок;

е) да разпорежда на администратора да съобщава на субекта на данните за нарушение на сигурността на личните данни;

ж) да налага временно или окончателно ограничаване, включително забрана, на обработването на данни;

з) да разпорежда коригирането или изтриването на лични данни, или ограничаването на обработването им съгласно членове 18, 19 и 20, както и уведомяването за тези действия на получатели, пред които личните данни са били разкрити съгласно член 19, параграф 2 и член 21;

и) да налага административна имуществена санкция съгласно член 66 в случай на неизпълнение от страна на институция или орган на Съюза на една от мерките, посочени в букви г)—з) и й) от настоящия параграф, в зависимост от обстоятелствата по всеки отделен случай;

й) да разпорежда спиране на предаването на данни към получател в държава членка или към международна организация.

3. Европейският надзорен орган по защита на данните има следните правомощия по отношение на даване на разрешения и съвети:

а) да съветва субектите на данни при упражняване на техните права;

б) да съветва администратора в съответствие с процедурата по предварителна консултация, посочена в член 40, и в съответствие с член 41, параграф 2;

в) да издава по собствена инициатива или при поискване становища до институциите и органите на Съюза и до обществеността по всякакви въпроси, свързани със защитата на лични данни;

г) да приема стандартните клаузи за защита на данните, посочени в член 29, параграф 8 и в член 48, параграф 2, буква в);

д) да дава разрешение за договорните клаузи, посочени в член 48, параграф 3, буква а);

е) да дава разрешение за административните договорености, посочени в член 48, параграф 3, буква б).

ж) да дава разрешение за операциите по обработване съгласно актове за изпълнение, приети съгласно член 40, параграф 4.

4. Европейският надзорен орган по защита на данните разполага с правомощието да сезира Съда при условията, предвидени в Договорите, и да встъпва по дела, заведени пред Съда.

5. Упражняването на правомощията, предоставени на Европейския надзорен орган по защита на данните съгласно настоящия член, подлежи на подходящи гаранции, включително ефективни средства за съдебна защита и справедлив съдебен процес, определени в правото на Съюза.

Член 59

Задължение на администраторите и обработващите лични данни за реагиране на твърдения

Когато Европейският надзорен орган по защита на данните упражнява правомощията, предвидени в член 58, параграф 2, букви а), б) и в), администраторът или обработващият лични данни информира Европейския надзорен орган по защита на данните относно становището си в разумен срок, който се определя от Европейския надзорен орган по защита на данните при отчитане на обстоятелствата по всеки отделен случай. Отговорът включва и описание на предприетите мерки, ако има такива, в отговор на отправените от Европейския надзорен орган по защита на данните забележки.

Член 60

Доклад за дейността

1. Европейският надзорен орган по защита на данните представя на Европейския парламент, на Съвета и на Комисията годишен доклад за дейността си и същевременно го публикува.

2. Европейският надзорен орган по защита на данните изпраща посочения в параграф 1 доклад на другите институции и органи на Съюза, които могат да представят коментари с оглед на евентуално разглеждане на доклада от Европейския парламент.

ГЛАВА VII

СЪТРУДНИЧЕСТВО И СЪГЛАСУВАНОСТ

Член 61

Сътрудничество между Европейския надзорен орган по защита на данните и националните надзорни органи

Европейският надзорен орган по защита на данните си сътрудничи с националните надзорни органи, и със съвместния надзорен орган, създаден съгласно член 25 от Решение 2009/917/ПВР на Съвета ([1]), доколкото това е необходимо за изпълнението на съответните им задължения, по-специално чрез взаимно предоставяне на съответната информация, отправяне на искания помежду си за упражняване на своите правомощия и взаимно даване на отговор на отправените искания.

Член 62

Координиран надзор, осъществяван от Европейския надзорен орган по защита на данните и националните надзорни органи

1. В случаите, когато даден акт на Съюза препраща към настоящия член, Европейският надзорен орган по защита на данните и националните надзорни органи, всеки от тях действащ в обхвата на съответните си правомощия, си сътрудничат активно в рамките на отговорностите си, за осигуряване на ефективен надзор на мащабни информационни системи и на органи, служби и агенции на Съюза.

2. Действайки в обхвата на съответните си правомощия и в рамките на отговорностите си, когато е необходимо те осъществяват обмен на съответна информация, оказват си съдействие при извършването на одити и проверки, разглеждат трудности при тълкуването или прилагането на настоящия регламент и други приложими правни актове на Съюза, проучват проблеми, свързани с упражняването на независим надзор или с упражняването на правата на субектите на данни, изготвят хармонизирани предложения за разрешаване на проблеми и насърчават информираността относно правата на защита на данните.

3. За целите, посочени в параграф 2, Европейският надзорен орган по защита на данните и националните надзорни органи провеждат заседания най-малко два пъти в годината в рамките на Европейския комитет по защита на данните. За тези цели Европейският комитет по защита на данните може да разработи допълнителни методи на работа, когато е необходимо.

4. Веднъж на всеки две години Европейският комитет по защита на данните изпраща на Европейския парламент, на Съвета и на Комисията съвместен доклад за дейностите по координиран надзор.

([1]) Решение 2009/917/ПВР на Съвета от 30 ноември 2009 г. относно използването на информационни технологии за митнически цели (ОВ L 323, 10.12.2009 г., стр. 20).

ГЛАВА VIII

СРЕДСТВА ЗА ПРАВНА ЗАЩИТА, ОТГОВОРНОСТ ЗА ПРИЧИНЕНИ ВРЕДИ И САНКЦИИ

Член 63

Право на подаване на жалба до Европейския надзорен орган по защита на данните

1. Без да се засягат които и да било средства за съдебна, административна или извънсъдебна защита, всеки субект на данни има право да подаде жалба до Европейския надзорен орган по защита на данните, ако счита, че обработването на лични данни, отнасящи се до него, нарушава настоящия регламент.

2. Европейският надзорен орган по защита на данните информира жалбоподателя за напредъка в разглеждането на жалбата и за резултата от нея, включително за възможността за съдебна защита съгласно член 64.

3. Ако Европейският надзорен орган по защита на данните в срок от три месеца не разгледа жалбата или не информира субекта на данните за напредъка в разглеждането на жалбата или за резултата от нея, се счита, че Европейският надзорен орган по защита на данните е взел отрицателно решение.

Член 64

Право на ефективна съдебна защита

1. Съдът е компетентен да разглежда всички спорове, свързани с разпоредбите на настоящия регламент, включително искове за вреди.

2. Решенията на Европейския надзорен орган по защита на данните, включително решенията съгласно член 63, параграф 3, се обжалват пред Съда.

3. Съдът разполага с неограничена компетентност за преглед на административната имуществена санкция, посочено в член 66. Той може да отмени, намали или увеличи наложените имуществени санкции в рамките на член 66.

Член 65

Право на обезщетение

Всяко лице, което е претърпяло имуществени или неимуществени вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от институцията или органа на Съюза за нанесените вреди, при спазване на условията, предвидени в Договорите.

Член 66

Административна имуществена санкция

1. Европейският надзорен орган по защита на данните може да налага административна имуществена санкция на институции и органи на Съюза, в зависимост от обстоятелствата по всеки отделен случай, когато институция или орган на Съюза не изпълни разпореждане на Европейския надзорен орган по защита на данните, издадено съгласно член 58, параграф 2, букви а)—з) и буква й). Когато се взема решение дали да бъде наложена административна имуществена санкция и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат следните елементи:

а) естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът или целта на съответното обработване, както и броят на засегнатите субекти на данни и степента на причинената им вреда;

б) действията, предприети от институцията или органа на Съюза за смекчаване на последиците от вредите, претърпени от субектите на данни;

в) степента на отговорност на институцията или органа на Съюза, като се вземат предвид техническите и организационни мерки, въведени от тях в съответствие с членове 27 и 33;

г) всички подобни предишни нарушения от страна на институцията или органа на Съюза;

д) степента на сътрудничество с Европейския надзорен орган по защита на данните с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него;

е) категориите лични данни, засегнати от нарушението;

ж) начинът, по който нарушението е станало известно на Европейския надзорен орган по защита на данните, по-специално дали и до каква степен институцията или органът на Съюза са съобщили за нарушението;

з) спазването на мерките, посочени в член 58, наложени преди на въпросната институция или въпросния орган на Съюза във връзка със същия предмет. Производството, водещо до налагане на тези имуществени санкции, се провежда в разумен срок в зависимост от обстоятелствата по случая и при отчитане на съответните мерки и производства, посочени в член 69.

2. В съответствие с параграф 1 от настоящия член, на институция или орган на Съюза, които нарушат задълженията си съгласно членове 8, 12, 27—35, 39, 40, 43, 44 и 45, се налага административна имуществена санкция в размер до 25 000 EUR за всяко отделно нарушение и в общ размер до 250 000 EUR годишно.

3. В съответствие с параграф 1 на институция или орган на Съюза, които нарушат следните разпоредби, се налага административна имуществена санкция в размер до 50 000 EUR за всяко отделно нарушение и в общ размер до 500 000 EUR годишно:

а) основните принципи за обработване на лични данни, включително условията, свързани с даването на съгласие, в съответствие с членове 4, 5, 7 и 10;

б) правата на субектите на данни съгласно членове 14—24;

в) предаването на лични данни на получател в трета държава или международна организация съгласно членове 46—50.

4. Ако институция или орган на Съюза при една и съща операция или при свързани или непрекъснати операции по обработване наруши няколко разпоредби на настоящия регламент или една и съща разпоредба няколко пъти, общият размер на административната имуществената санкция не може да надвишава сумата, определена за най-тежкото нарушение.

5. Преди да вземе решения съгласно настоящия член, Европейският надзорен орган по защита на данните дава на институцията или органа на Съюза, по отношение на които се провеждат производствата от Европейският надзорен орган, възможността да бъдат изслушани във връзка с въпросите, по които Европейският надзорен орган е изразил възражения. Европейският надзорен орган по защита на данните основава своите решения единствено на възражения, по които засегнатите страни са имали възможност да изразят становище. Жалбоподателите се привличат за тясно сътрудничество в рамките на производството.

6. Правото на защита на засегнатите страни се съблюдава в хода на цялото производство. Те имат правото на достъп до преписката на Европейския надзорен орган по защита на данните, при условие че се зачита законният интерес на физическите лица или на предприятията за защита на техните лични данни или търговски тайни.

7. Средствата, събрани чрез налагането на имуществени санкции съгласно настоящия член, представляват приход в общия бюджет на Съюза.

Член 67

Представителство на субектите на данни

Субектът на данни има право да възложи на структура, организация или сдружение с нестопанска цел, което е надлежно учредено в съответствие с правото на Съюза или с правото на държава членка, има уставни цели, които са в обществен интерес, и действа в областта на защитата на правата и свободите на субектите на данни по отношение на защитата на техните лични данни, да подаде жалба от негово име до Европейския надзорен орган по защита на данните и да упражни от негово име правата по членове 63 и 64, както и правото на обезщетение по член 65.

Член 68

Жалби от длъжностни лица и други служители на Съюза

Всяко лице, което на работа от институция или орган на Съюза, може да подаде жалба до Европейския надзорен орган по защита на данните във връзка с предполагаемо нарушение на разпоредбите на настоящия регламент, без да следва официална процедура. Никой не трябва да претърпява неблагоприятни последици поради това, че е подал жалба до Европейския надзорен орган по защита на данните, в която се твърди, че е извършено такова нарушение.

Член 69

Санкции

Когато длъжностно лице или друг служител на Съюза не спази задълженията, предвидени в настоящия регламент, независимо дали умишлено или по непредпазливост, съответното длъжностно лице или служител подлежи на дисциплинарни или други мерки в съответствие с правилата и процедурите, установени в Правилника за длъжностните лица.

ГЛАВА IX

ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ ОТ ОПЕРАТИВЕН ХАРАКТЕР ОТ ОРГАНИТЕ, СЛУЖБИТЕ И АГЕНЦИИТЕ НА СЪЮЗА ПРИ ИЗВЪРШВАНЕТО НА ДЕЙНОСТИ, КОИТО ПОПАДАТ В ОБХВАТА НА ЧАСТ ТРЕТА, ДЯЛ V, ГЛАВА 4 ИЛИ ГЛАВА 5 ОТ ДФЕС

Член 70

Приложно поле на главата

Настоящата глава се прилага единствено за обработването на лични данни от оперативен характер от органи, служби или агенции на Съюза, осъществяващи дейности, които попадат в обхвата на част трета, дял V, глави 4 и 5 от ДФЕС, без да се засягат специалните правила за защита на данните, приложими по отношение на тези органи, служби или агенции на Съюза.

Член 71

Принципи, свързани с обработването на лични данни от оперативен характер

1. Личните данни от оперативен характер:

а) се обработват законосъобразно и добросъвестно („законосъобразност и добросъвестност“);

б) се събират за конкретни, изрично указани и законни цели и не се обработват по начин, който е несъвместим с тези цели („ограничение до конкретни цели“);

в) са подходящи, относими и не надхвърлят необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

г) са точни и при необходимост поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни от оперативен характер, като се имат предвид целите, за които те се обработват („точност“);

д) се поддържат във вид, който позволява идентифициране на субектите на данните, за период, не по-дълъг от необходимия за целите, за които личните данни от оперативен характер се обработват („ограничено съхраняване“);

е) се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки („цялостност и поверителност“).

2. Обработване от същия или друг администратор за която и да е от целите, посочени в правния акт за създаване на институция, орган или агенция на Съюза, различна от целта, за която личните данни от оперативен характер са събрани, се разрешава, при условие че:

а) администраторът е оправомощен да обработва такива лични данни от оперативен характер за такава цел в съответствие с правото на Съюза; и

б) обработването е необходимо и пропорционално за тази различна цел в съответствие с правото на Съюза.

3. Обработването от същия или друг администратор може да включва архивиране в обществен интерес, използване за научни, статистически или исторически цели съгласно посоченото в правния акт за създаване на институция, орган или агенция на Съюза, при прилагането на подходящи гаранции за правата и свободите на субектите на данните.

4. Администраторът носи отговорност за спазването на параграфи 1, 2 и 3 и трябва да е в състояние да го докаже.

Член 72

Законосъобразност на обработването на лични данни от оперативен характер

1. Обработването на лични данни е законосъобразно само ако и доколкото то е необходимо за изпълнението на задача, която се осъществява от органите, службите и агенциите на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глави 4 и 5 от ДФЕС и е въз основа на правото на Съюза.

2. Специалните правни актове на Съюза, уреждащи обработването в рамките на посочената глава, посочват най-малко целите на обработването, личните данни от оперативен характер, които се обработват, задачите на обработването и сроковете за съхранение на лични данни от оперативен характер или за периодично преразглеждане на необходимостта от продължаване на съхраняването на лични данни от оперативен характер.

Член 73

Разграничение между различните категории субекти на данни

Когато е приложимо и доколкото е възможно, администраторът прави ясно разграничение между личните данни от оперативен характер на различни категории субекти на данни, като категориите, изброени в правните актове за създаване на органите, службите и агенциите на Съюза.

Член 74

Разграничение между лични данни от оперативен характер и проверка на качеството на личните данни от оперативен характер

1. Администраторът разграничава, доколкото е възможно, личните данни от оперативен характер, основани на факти, от лични данни от оперативен характер, основани на лични преценки.

2. Администраторът предприема всички разумни стъпки, за да гарантира, че не се предават или предоставят лични данни от оперативен характер, които са неточни, непълни или неактуални. За тази цел администраторът трябва, доколкото е възможно и където е приложимо, да проверява качеството на личните данни от оперативен характер, преди тяхното предаване или предоставяне, например чрез консултация с компетентния орган, от когото произхождат данните. Доколкото е възможно, при всяко предаване на лични данни от оперативен характер администраторът добавя необходимата информация, позволяваща на получателя да оцени степента на точност, пълнота и надеждност на личните данни от оперативен характер, както и степента им на актуалност.

3. Ако се окаже, че са предадени неверни лични данни от оперативен характер или че личните данни от оперативен характер са предадени незаконосъобразно, получателят се уведомява незабавно. В този случай съответните лични данни се коригират или изтриват или обработването им се ограничава в съответствие с член 82.

Член 75

Специални условия за обработване

1. В случаите, когато правото на Съюза, приложимо по отношение на администратора, предаващ данните, предвижда специални условия за обработването, администраторът информира получателя на личните данни от оперативен характер за тези условия и за изискването те да бъдат изпълнени.

2. Администраторът спазва специалните условия за обработване, предвидени от компетентния орган, предаващ данните в съответствие с член 9, параграфи 3 и 4 от Директива (ЕС) 2016/680.

Член 76

Обработване на специални категории лични данни от оперативен характер

1. Обработването на лични данни от оперативен характер, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, и обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, лични данни от оперативен характер, отнасящи се до здравето или сексуалния живот и сексуалната ориентация на лицето, е разрешено само когато това е абсолютно необходимо за оперативни цели, обхванато е от правомощията на съответния орган, служба или агенция на Съюза, и при подходящи гаранции за правата и свободите на субекта на данни. Забранява се дискриминацията на физически лица въз основа на посочените лични данни.

2. Длъжностното лице по защита на данните се уведомява без излишно забавяне за прибягването до настоящия член.

Член 77

Автоматизирано вземане на индивидуални решения, включително профилиране

1. Забранява се вземането на решение, което се основава единствено на автоматизирано обработване, включително профилиране, което поражда неблагоприятни правни последици за субекта на данните или оказва значително въздействие върху него, освен ако това се допуска от правото на Съюза, което се прилага спрямо администратора и което предоставя подходящи гаранции за правата и свободите на субекта на данни, най-малкото правото на получаване на човешка намеса от страна на администратора.

2. Решенията по параграф 1 от настоящия член не се основават на специалните категории лични данни, посочени в член 76, освен ако не са въведени подходящи мерки за защита на правата и свободите и законните интереси на субекта на данните.

3. В съответствие с правото на Съюза се забранява профилирането, което води до дискриминация на физически лица въз основа на специалните категории лични данни, посочени в член 76.

Член 78

Комуникация и условия за упражняването на правата на субекта на данни

1. Администраторът предприема разумни мерки за предоставяне на субекта на данни на всякаква информация по член 79 и за осигуряване на комуникацията във връзка с членове 80—84 и 92 относно обработването в сбита, разбираема и леснодостъпна форма, като използва ясен и прост език. Информацията се предоставя по всякакъв подходящ начин, включително по електронен път. Като общо правило администраторът предоставя информацията в същата форма като тази на искането.

2. Администраторът улеснява упражняването на правата на субекта на данните съгласно членове 79—84.

3. Администраторът уведомява писмено субекта на данните за отговора на неговото искане без необосновано забавяне и при всички случаи най-късно в срок от три месеца след получаване на искането му.

4. Администраторът предоставя безплатно информацията по член 79 и комуникацията или действията, предприети съгласно членове 80 — 84 и 92. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може да откаже да предприеме действия по искането. Администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

5. Когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искане по членове 80 или 82, администраторът може да поиска да се предостави допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

Член 79

Информация, до която се осигурява достъп или която се предоставя на субекта на данните

1. Администраторът предоставя на субекта на данните най-малко следната информация:

а) посочване на органа, службата или агенцията на Съюза и координатите за връзка с тях;

б) координатите за връзка на длъжностното лице по защита на данните;

в) целите на обработването, за които са предназначени личните данни от оперативен характер;

г) правото да бъде подадена жалба до Европейския надзорен орган по защита на данните и координатите за връзка на този орган;

д) съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни от оперативен характер и ограничаване на обработването на лични данни от оперативен характер, свързани със субекта на данните.

2. Освен информацията, посочена в параграф 1, администраторът предоставя на субекта на данните, в конкретни случаи, предвидени от правото на Съюза и с цел да му се даде възможност да упражни правата си, следната допълнителна информация:

а) правното основание на обработването;

б) срока, за който ще се съхраняват личните данни от оперативен характер, а ако това е невъзможно, критериите, използвани за определяне на този срок;

в) когато е приложимо, категориите получатели на личните данни от оперативен характер, включително в трети държави или международни организации;

г) когато е необходимо, допълнителна информация, по-специално когато личните данни от оперативен характер са събрани без знанието на субекта на данните.

3. Администраторът може да забавя, ограничава или пропуска предоставянето на информация на субекта на данните съгласно параграф 2, до такава степен и за толкова време, за колкото тази мярка е необходима и пропорционална в едно демократично общество, като надлежно се вземат предвид основните права и законните интереси на засегнатото физическо лице, за да:

а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури;

б) не се допуснат неблагоприятни последици върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;

в) се защити обществената сигурност на държавите членки;

г) се защити националната сигурност на държавите членки;

д) се защитят правата и свободите на други лица, като жертвите и свидетелите.

Член 80

Право на достъп на субекта на данните

Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни от оперативен характер, свързани с него, и ако това е така, има право на достъп до личните данни от оперативен характер и до следната информация:

а) целите и правното основание за обработването;

б) съответните категории лични данни от оперативен характер;

в) получателите или категориите получатели, пред които са разкрити личните данни от оперативен характер, по-специално получателите в трети държави или международни организации;

г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, или ако това е невъзможно, критериите за определяне на този срок;

д) съществуването на право да се изиска от администратора коригиране или изтриване на лични данни от оперативен характер, или ограничаване на обработването на лични данни от оперативен характер, свързано със субекта на данните;

е) правото да подаде жалба до Европейския надзорен орган по защита на данните, както и да получи неговите данни за контакт;

ж) съобщаване на личните данни от оперативен характер, които са в процес на обработване, и на всякаква налична информация за техния произход.

Член 81

Ограничения на правото на достъп

1. Администраторът може да ограничи изцяло или частично правото на достъп на субекта на данните, до степен и срок, при които такова частично или пълно ограничаване представлява необходима и пропорционална мярка в едно демократично общество, като надлежно се вземат под внимание основните права и законните интереси на засегнатото физическо лице, за да:

а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури;

б) не се допуснат неблагоприятни последици върху предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;

в) се защити обществената сигурност на държавите членки;

г) се защити националната сигурност на държавите членки;

д) се защитят правата и свободите на други лица, като например жертви и свидетели.

2. В случаите, посочени в параграф 1, администраторът информира без излишно забавяне в писмена форма субекта на данните за всеки отказ на достъп или ограничаване на достъпа и за причините за отказа или ограничаването. Тази информация може да бъде пропусната, когато предоставянето ѝ би възпрепятствало постигането на някоя от целите, посочени в параграф 1. Администраторът уведомява субекта на данните за възможността за подаване на жалба до Европейския надзорен орган по защита на данните или за търсене на защита по съдебен ред пред Съда. Администраторът документира фактическите или правните основания, на които се основава решението. При поискване, тази информация се предоставя на разположение на Европейския надзорен орган по защита на данните.

Член 82

Право на коригиране или изтриване на лични данни от оперативен характер и ограничаване на обработването

1. Всеки субект на данни има право да поиска от администратора да коригира без ненужно забавяне неточните лични данни от оперативен характер, свързани с него. Като се имат предвид целите на обработването, субектът на данните има право непълните лични данни от оперативен характер да бъдат попълнени, включително чрез предоставяне на допълнителна декларация.

2. Администраторът изтрива личните данни от оперативен характер без ненужно забавяне, а субектът на данни има право да поиска от администратора да изтрие негови лични данни от оперативен характер без ненужно забавяне, в случай че обработването се извършва в нарушение на членове 71, 72, параграф 1 или 76 или когато личните данни от оперативен характер трябва да бъдат изтрити с цел спазване на правно задължение, което се прилага спрямо администратора.

3. Вместо да извърши изтриване, администраторът ограничава обработването, когато:

а) точността на личните данни се оспорва от субекта на данните и тяхната точност или неточност не може да бъде проверена; или

б) личните данни трябва да бъдат запазени за доказателствени цели.

Когато обработването е ограничено съгласно първа алинея, буква а), администраторът информира субекта на данните, преди да премахне ограничаването на обработването.

Ограничените данни се обработват единствено с оглед на целта, поради която тяхното изтриване е било възпрепятствано.

4. Администраторът информира писмено субекта на данните за всеки отказ за коригиране или изтриване на лични данни от оперативен характер, или за ограничено обработване и за причините за отказа. Администраторът може да ограничи изцяло или частично предоставянето на такава информация, в степента, в която такова ограничаване представлява необходима и пропорционална мярка в едно демократично общество, като надлежно се вземат под внимание основните права и законните интереси на засегнатото физическо лице, за да:

а) се избегне възпрепятстването на официални или съдебни проучвания, разследвания или процедури;

б) не се допуснат неблагоприятни последици върху предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания;

в) се защити обществената сигурност на държавите членки;

г) се защити националната сигурност на държавите членки;

д) се защитят правата и свободите на други лица, като жертвите и свидетелите.

Администраторът уведомява субекта на данните за възможността за подаване на жалба до Европейския надзорен орган по защита на данните или за търсене на защита по съдебен ред пред Съда.

5. Администраторът уведомява за коригирането на неточни лични данни от оперативен характер компетентния орган, от който произхождат неточните лични данни от оперативен характер.

6. Когато лични данни от оперативен характер са коригирани или изтрити, или обработването им е ограничено съгласно параграфи 1, 2 или 3, администраторът уведомява получателите и ги информира, че те трябва да коригират или изтрият личните данни от оперативен характер, или да ограничат обработването на личните данни от оперативен характер, за което носят отговорност.

Член 83

Право на достъп в рамките на наказателното разследване и наказателното производство

Когато личните данни от оперативен характер произхождат от компетентен орган, органите, службите и агенциите на Съюза, преди да вземат решение относно правото на достъп на даден субект на данни, правят справка със съответния компетентен орган дали тези лични данни се съдържат в съдебно решение или регистър или досие, обработвани в хода на наказателно разследване и наказателно производство в държавата членка на компетентния орган. Ако това е така, решение относно правото на достъп се взема в рамките на консултация и в тясно сътрудничество със съответния компетентен орган.

Член 84

Упражняване на правата от субекта на данните и проверка от Европейския надзорен орган по защита на данните

1. В случаите, посочени в член 79, параграф 3, член 81 и член 82, параграф 4, правата на субекта на данните могат да бъдат упражнявани и чрез Европейския надзорен орган по защита на данните.

2. Администраторът информира субекта на данните за възможността да упражнява правата си чрез Европейския надзорен орган по защита на данните в съответствие с параграф 1.

3. Когато е упражнено правото по параграф 1, Европейският надзорен орган по защита на данните информира субекта на данните най-малко за това, че е извършил всички необходими проверки или нужния преглед. Европейският надзорен орган по защита на данните информира също така субекта на данните за правото му да потърси защита по съдебен ред пред Съда.

Член 85

Защита на данните на етапа на проектирането и по подразбиране

1. Като взема предвид 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 на физическите лица, администраторът въвежда, както към момента на определянето на средствата за обработване, така и към момента на самото обработване, подходящи технически и организационни мерки, например псевдонимизация, които са разработени с оглед на ефективното прилагане на принципите за защита на данните, например свеждане на данните до минимум, и с оглед на включване на необходимите гаранции в процеса на обработване, за да се спазят изискванията на настоящия регламент и на правния акт за създаването му, и да се гарантира защитата на правата на субектите на данни.

2. Администраторът въвежда подходящи технически и организационни мерки, за да се гарантира, че по правило се обработват само лични данни от оперативен характер, които са подходящи, относими и не надхвърлят необходимото във връзка с целта на обработването. Това задължение се отнася до обема на събраните лични данни от оперативен характер, степента на обработването, срока на съхраняването им и тяхната достъпност. По-специално, подобни мерки гарантират, че по подразбиране личните данни от оперативен характер не са достъпни за неограничен брой физически лица без намеса от страна на съответното физическо лице.

Член 86

Съвместни администратори

1. Когато двама или повече администратори или един или повече администратори съвместно с един или повече администратори, различни от институции и органи на Съюза, съвместно определят целите и средствата на обработването, те са съвместни администратори. Те определят по прозрачен начин съответните си отговорности за изпълнение на задълженията си за защита на данните, по-специално що се отнася до упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информацията, посочена в член 79, посредством договореност помежду си, освен ако и доколкото съответните отговорности на съвместните администратори не са определени от правото на Съюза или правото на държава членка, което се прилага спрямо съвместните администратори. В договореността може да се посочи точка за контакт за субектите на данни.

2. Договореността, посочена в параграф 1, надлежно отразява съответните роли и връзки на съвместните администратори спрямо субекта на данни. Съществените характеристики на договореността са достъпни за субекта на данните.

3. Независимо от условията на договореността, посочена в параграф 1, субектът на данни може да упражнява своите права по настоящия регламент по отношение на всеки и срещу всеки от администраторите.

Член 87

Обработващ лични данни

1. Когато обработването се извършва от името на даден администратор, администраторът използва само обработващи лични данни, които предоставят достатъчни гаранции за прилагането на подходящи технически и организационни мерки по такъв начин, че обработването да протича в съответствие с изискванията на настоящия регламент и на правния акт за създаване на администратора, и да гарантира защитата на правата на субектите на данни.

2. Обработващият лични данни не включва друг обработващ лични данни без предварителното конкретно или общо писмено разрешение от администратора. В случай на общо писмено разрешение обработващият лични данни информира администратора за всякакви планирани промени за включване или замяна на други обработващи лични данни, като по този начин дава възможност на администратора да се противопостави на тези промени.

3. Обработването от страна на обработващия лични данни се урежда с договор или с друг правен акт съгласно правото на Съюза или правото на държава членка, който е задължителен за обработващия лични данни в отношенията му с администратора и който урежда предмета и срока на обработването, естеството и целта на обработването, вида лични данни от оперативен характер и категориите субекти на данни, както и задълженията и правата на администратора. В този договор или друг правен акт се предвижда по-специално, че обработващият лични данни:

а) действа единствено по указания на администратора;

б) гарантира, че лицата, оправомощени да обработват личните данни от оперативен характер, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;

в) подпомага администратора с всички подходящи средства, за да се гарантира спазването на разпоредбите относно правата на субекта на данни;

г) по избор на администратора заличава или връща на администратора всички лични данни от оперативен характер след приключване на услугите по обработване и заличава съществуващите копия, освен ако правото на Съюза или правото на държава членка изисква съхранението на тези лични данни от оперативен характер;

д) предоставя на администратора цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член;

е) спазва условията по параграф 2 и настоящия параграф за включване на друг обработващ лични данни.

4. Договорът или другият правен акт, посочен в параграф 3, се изготвя в писмена форма, включително в електронна форма.

5. Ако обработващ лични данни наруши настоящия регламент или правния акт за създаване на администратора, като определи целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.

Член 88

Водене на записи

1. Администраторът води записи за всяка от следните операции по обработване на данни в автоматизираните системи за обработка на данни: събиране, промяна, достъп, справки, разкриване, включително предаване, комбиниране и изтриване на лични данни от оперативен характер. Записите за извършена справка или разкриване дават възможност за установяване на обосновката за това, както и датата и часа на такива операции, идентификацията на лицето, което е направило справка или е разкрило лични данни, и — доколкото е възможно, самоличността на получателите на тези лични данни от оперативен характер.

2. Записите се използват единствено за проверяване на законосъобразността на обработването, за вътрешен контрол, за гарантиране на цялостността и сигурността на личните данни от оперативен характер и при наказателни производства. Тези записи се заличават след три години, освен ако са необходими за целите на текущия контрол.

3. Администраторът предоставя, при поискване, записите на своето длъжностно лице по защита на данните и на Европейския надзорен орган по защита на данните.

Член 89

Оценка на въздействието върху защитата на данни

1. Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, администраторът, преди да пристъпи към обработването, извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни от оперативен характер.

2. Оценката, посочена в параграф 1, съдържа най-малко общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни от оперативен характер и за доказване на съответствие с правилата относно защитата на данни, като се вземат предвид правата и законните интереси на субектите на данните и другите засегнати лица.

Член 90

Предварителна консултация с Европейския надзорен орган по защита на данните

1. Администраторът се консултира с Европейския надзорен орган по защита на данните преди обработването на лични данни от оперативен характер, което ще бъде част от нов регистър, чието създаване предстои, когато:

а) оценката на въздействието върху защитата на данните съгласно член 89 покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска; или

б) видът обработване, по-специално когато се използват нови технологии, механизми или процедури, включва висока степен на риск за правата и свободите на субектите на данните.

2. Европейският надзорен орган по защита на данните може да изготви списък на операциите по обработване, за които е необходима предварителна консултация съгласно параграф 1.

3. Администраторът предоставя на Европейския надзорен орган по защита на данните оценката на въздействието върху защитата на данните, посочена в член 89, и при поискване — всякаква друга информация, която позволява на Европейския надзорен орган по защита на данните да направи оценка на съответствието на обработването, и по-специално на рисковете за защитата на личните данни от оперативен характер на субекта на данните и на съответните гаранции.

4. Когато Европейският надзорен орган по защита на данните счита, че планираното обработване, посочено в параграф 1, би било в нарушение на настоящия регламент или на правния акт за създаване на органа, службата или агенцията на Съюза, по-специално когато администраторът не е идентифицирал или ограничил риска в достатъчна степен, Европейският надзорен орган по защита на данните предоставя на администратора писмено становище в срок до шест седмици след получаване на искането за консултация. Този срок може да бъде удължен с още един месец, в зависимост от сложността на планираното обработване. В срок от един месец от получаване на искането за консултация Европейският надзорен орган по защита на данните уведомява администратора за всяко такова удължаване, включително и за причините за забавянето.

Член 91

Сигурност на обработването на лични данни от оперативен характер

1. Администраторът и обработващият лични данни, като отчитат достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, прилагат подходящи технически и организационни мерки за осигуряване на съобразено с тези рискове ниво на сигурност, по-специално по отношение на обработването на специалните категории лични данни от оперативен характер.

2. По отношение на автоматизираното обработване, администраторът и обработващият лични данни след оценка на рисковете прилагат мерки, имащи за цел:

а) да се откаже достъп на неоправомощени лица до оборудването, използвано за обработването на данни („контрол върху достъпа до оборудване“);

б) да се предотврати неразрешеното четене, копиране, изменяне или отстраняване на носители на данни („контрол върху носителите на данни“);

в) да се предотвратят неразрешеното въвеждане на оперативни лични данни и неразрешената проверка, изменяне или заличаване на съхраняваните лични данни от оперативен характер („контрол върху съхраняването“);

г) да се предотврати използването на автоматизирани системи за обработване от неоправомощени лица чрез използване на оборудване за предаване на данни („контрол върху ползвателите“);

д) да се гарантира, че лицата, на които е разрешено да използват автоматизирана система за обработване, имат достъп само до личните данни от оперативен характер, които са обхванати от тяхното разрешение за достъп („контрол върху достъпа до данни“);

е) да се гарантира възможността за проверка и установяване на кои органи са били или могат да бъдат предадени или имат достъп до лични данни от оперативен характер чрез предаване на данни („контрол върху комуникацията“);

ж) да се гарантира възможността за последваща проверка и установяване на това какви лични данни от оперативен характер са били въведени в автоматизираните системи за обработване на данни, както и кога и от кого са били въведени тези лични данни от оперативен характер („контрол върху въвеждането“);

з) да предотвратяват неразрешено четене, копиране, променяне или заличаване на лични данни от оперативен характер при предаване на лични данни от оперативен характер или при транспортиране на носители на данни („контрол на транспортирането“);

и) да се гарантира възможността за възстановяване на инсталираните системи в случай на отказ на системите („възстановяване“);

й) да се гарантира изпълнението на функциите на системата, докладването за появили се във функциите дефекти („надеждност“), както и недопускане на увреждане на съхраняваните лични данни от оперативен характер вследствие на неправилно функциониране на системата („непокътнатост“);

Член 92

Уведомяване на Европейския надзорен орган по защита на данните за нарушение на сигурността на личните данни

1. В случай на нарушение на сигурността на личните данни администраторът, без ненужно забавяне и когато това е осъществимо — не по-късно от 72 часа след като е разбрал за него, уведомява за нарушението на сигурността на личните данни Европейския надзорен орган по защита на данните, освен ако е малко вероятно нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Когато уведомлението до Европейския надзорен орган по защита на данните не е подадено в срок от 72 часа, то се придружава от информация за причините за забавянето.

2. В уведомлението, посочено в параграф 1, се съдържа най-малко следното:

а) описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни от оперативен характер;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните;

в) описание на евентуалните последици от нарушението на сигурността на личните данни;

г) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

3. Когато и доколкото не е възможно информацията, посочена в параграф 2, да се подаде едновременно, тя може да се подаде поетапно без по-нататъшно ненужно забавяне.

4. Администраторът документира всяко нарушение на сигурността на личните данни, посочено в параграф 1, като включва фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на Европейския надзорен орган по защита на данните да провери дали е спазен настоящият член.

5. Когато нарушението на сигурността на личните данни засяга лични данни от оперативен характер, които са били предадени от или на компетентните органи, администраторът съобщава посочената в параграф 2 информация на компетентните органи без излишно забавяне.

Член 93

Съобщаване на субекта на данните за нарушение на сигурността на личните данни

1. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, администраторът без ненужно забавяне съобщава на субекта на данните за нарушението на сигурността на личните данни.

2. В съобщението до субекта на данните, посочено в параграф 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се съдържат най-малко информацията и препоръките, предвидени в член 92, параграф 2, букви б), в) и г).

3. Посоченото в параграф 1 съобщение до субекта на данните не се изисква, ако е изпълнено някое от следните условия:

а) администраторът е предприел подходящи технически и организационни мерки за защита и тези мерки са били приложени по отношение на личните данни от оперативен характер, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят личните данни от оперативен характер неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране;

б) администраторът е взел впоследствие мерки, които гарантират, че вече няма вероятност да се реализира високият риск за правата и свободите на субектите на данни, посочен в параграф 1;

в) то би довело до непропорционални усилия. В такъв случай се прави публично съобщение или се взема друга подобна мярка, така че субектите на данни да бъдат в еднаква степен ефективно информирани.

4. Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, Европейският надзорен орган по защита на данните може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да съобщи за нарушението или да реши, че е изпълнено някое от условията по параграф 3.

5. Съобщението до субекта на данните, посочено в параграф 1 от настоящия член, може да бъде забавено, ограничено или пропуснато, при условията и на основанията, посочени в член 79, параграф 3.

Член 94

Предаване на лични данни от оперативен характер на трети държави и международни организации

1. При спазване на ограниченията и условията, предвидени в правните актове за създаване на орган, служба или агенция на Съюза, администраторът може да предава лични данни от оперативен характер на орган на трета държава или на международна организация, доколкото това предаване е необходимо за изпълнението на задачите на администратора и само когато условията, предвидени в настоящия член, са изпълнени, а именно:

а) Комисията е приела решение относно адекватно ниво на защита в съответствие с член 36, параграф 3 от Директива (ЕС) 2016/680, според което третата държава или територия, или обработващ сектор в тази трета държава, или въпросната международна организация гарантира адекватното ниво на защита;

б) при липса на решение на Комисията съгласно буква а) относно адекватното ниво на защита на личните данни, е сключено международно споразумение между Съюза и тази трета държава или международна организация съгласно член 218 от ДФЕС, с което се предоставят достатъчни гаранции по отношение на защитата на неприкосновеността на личния живот и на основните права и свободи на физическите лица;

в) при липса на решение на Комисията, съгласно буква а), относно адекватното ниво на защита или на международно споразумение, посочено в буква б) е сключено споразумение за сътрудничество, което позволява обмена на лични данни от оперативен характер, преди датата на прилагане на правния акт за създаване на съответния орган, служба или агенция на Съюза, между този орган, служба или агенция на Съюза и съответната трета държава.

2. Правните актове за създаване на органи, служби или агенции на Съюза могат да запазят или да въведат по-конкретни разпоредби относно условията за международно предаване на лични данни от оперативен характер, по-специално относно предаването на данни с подходящи гаранции и относно дерогации за особени ситуации.

3. Администраторът публикува на своя уебсайт и актуализира списък на решения относно адекватното ниво на защита, посочени в параграф 1, буква а), споразумения, административни договори и други инструменти, отнасящи се до предаването на лични данни от оперативен характер в съответствие с параграф 1.

4. Администраторът документира подробно всички случаи на предаване съгласно настоящия член.

Член 95

Тайна при съдебните разследвания и наказателното производство

Правните актове за създаване на органите, службите и агенциите на Съюза, отнасящи се до извършване на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 на от ДФЕС могат да задължат Европейския надзорен орган по защита на данните при упражняването на своите правомощия за надзор да взема предвид в максимална степен тайната на съдебните разследвания и наказателното производство, в съответствие с правото на Съюза или правото на държава членка.

ГЛАВА X

АКТОВЕ ЗА ИЗПЪЛНЕНИЕ

Член 96

Процедура на комитет

1. Комисията се подпомага от комитета, създаден съгласно член 93 от Регламент (ЕС) 2016/679. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

2. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.

ГЛАВА XI

ПРЕГЛЕД

Член 97

Клауза за преглед

Не по-късно от 30 април 2022 г. и на всеки пет години след това Комисията представя на Европейския парламент и на Съвета доклад относно прилагането на настоящия регламент, придружен, ако е необходимо, от подходящи законодателни предложения.

Член 98

Прегледна правните актове на Съюза

1. До 30 април 2022 г. Комисията извършва преглед на правните актове, приети въз основа на Договорите, които уреждат обработването на лични данни от оперативен характер от органи, служби или агенции на Съюза при извършването на дейности, които попадат в обхвата на част трета, дял V, глава 4 или глава 5 от ДФЕС, за да:

а) извърши оценка на тяхната съгласуваност с Директива (ЕС) 2016/680 и с глава IX от настоящия регламент;

б) установи всякакви различия, които могат да възпрепятстват обмена на лични данни от оперативен характер между органите, службите и агенциите на Съюза, когато извършват дейности в тези области, и компетентните органи;

в) установи всякакви различия, които могат да създадат правна разпокъсаност на законодателството в областта на защитата на данните в Съюза.

2. Въз основа на прегледа, с цел да се гарантира единна и съгласувана защита на физическите лица във връзка с обработването, Комисията може да представи подходящи законодателни предложения, по-специално с оглед прилагането на глава IX от настоящия регламент по отношение на Европол и на Европейската прокуратура, включително адаптиране на глава IX от настоящия регламент, ако е необходимо.

ГЛАВА XII

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 99

Отмяна на Регламент (ЕО) № 45/2001 и на Решение № 1247/2002/ЕО

Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО се отменят, считано от 11 декември 2018 г. Позоваванията на отменения регламент и на отменените решение се считат за позовавания на настоящия регламент.

Член 100

Преходни разпоредби

1. Решение № 2014/886/ЕС на Европейския парламент и на Съвета ([1]) и текущият мандат на Европейския надзорен орган по защита на данните и на заместника на надзорния орган не се засягат от настоящия регламент.

([1]) Решение 2014/886/ЕС на Европейския парламент и на Съвета от 4 декември 2014 г. относно назначаването на ръководител на Европейския надзорен орган по защита на данните и на негов заместник (ОВ L 351, 9.12.2014 г., стр. 9).

2. Счита се, че заместникът на надзорния орган има статут, равностоен на този на секретаря на Съда, що се отнася до определяне на размера на възнаграждението, надбавките, пенсията за осигурителен стаж и възраст и всякакви други обезщетения, които заместват възнаграждението.

3. Член 53, параграфи 4, 5 и 7, както и членове 55 и 56 от настоящия регламент се прилагат по отношение на настоящия заместник на надзорния орган до изтичането на мандата му.

4. Заместникът на надзорния орган подпомага Европейския надзорен орган по защита на данните при изпълнението на неговите задължения и го замества, когато Европейският надзорен орган по защита на данните отсъства или е възпрепятстван да изпълнява задълженията си, до изтичането на мандата на настоящия заместник на надзорния орган.

Член 101

Влизане в сила и прилагане

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

2. Въпреки това, настоящият регламент се прилага за обработването на лични данни от Евроюст, считано от 12 декември 2019 г..

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Страсбург на 23 октомври 2018 година.

За Европейския парламент	*За Съвета*
Председател	*Председател*
A. TAJANI	K. EDTSTADLER