Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните)

Обн. L ОВ. бр.119 от 4 Май 2016г.
Серия, номер на ОВ, дата, страници

ОВ L 119, 4.5.2016 г. стр. 1-88

Celex номер: 32016R0679

Дати

Дата на документа: 27.4.2016 г. дата на подписване

Дата на влизане в сила: 24.5.2016 г. влизане в сила дата на публикуване +20 виж **член 99**

Дата на влизане в сила: 25.5.2018 г. приложение, прилагане виж **член 99**

Дата на подписване: 27.4.2016 г.

Краен срок: 25.5.2020 г. не по-късно от виж **член 97**

Дата на изтичане на валидността: 31.12.9999 г.

Библиография

Класификации

EUROVOC дескриптор:

презграничен поток от данни

неприкосновеност на частен живот

физическо лице

достъп до информация

защита на информация

разпространение на информацията

закон за информатиката

пространство на свобода, сигурност и правосъдие

лични данни

Обща информация

Автор: Европейски парламент; Съвет на Европейския съюз

Вид: Регламент

Процедура:

Номер на процедурата: 2012/0011/COD

Връзки между документите

Всички консолидирани версии:

2016-05-04 - **02016R0679-20160504**

Актове, цитирани в съдебната практика:

12012E263

52012AE1303

12012P047

12012E267

12012E179

12012M/TXT

32000L0031

32009R0223

52012XX0630(01)

32003H0361

32008R0765

32014R0536

12012P/TXT

12012M005

12012P008

32012R1215

31993L0013

12012P011

32008R1338

12012E101

32015L1535

12012E102

12012E017

32003L0098

32001R1049

32001R0045

12012E338

32011R0182

52016AG0006(01)

32016L0680

32011L0024

12012E290

32002L0058

Правно основание:

12012E016

Засегнат от дело:

Член A64 тълкува се от **62019CJ0645**

Член A60 тълкува се от **62019CJ0645**

Член A55P1 тълкува се от **62019CJ0645**

Член A68 тълкува се от **62019CJ0645**

Член A58P5 тълкува се от **62019CJ0645**

Член A65 тълкува се от **62019CJ0645**

Член A57 тълкува се от **62019CJ0645**

Член A63 тълкува се от **62019CJ0645**

Член A56P1 тълкува се от **62019CJ0645**

Член A67 тълкува се от **62019CJ0645**

Член A62 тълкува се от **62019CJ0645**

Член A61 тълкува се от **62019CJ0645**

Член A66 тълкува се от **62019CJ0645**

Член A04PT11 тълкува се от **62017CJ0673**

Член A06P1LA тълкува се от **62017CJ0673**

тълкува се от **62017CJ0496**

Член A04PT7 тълкува се от **62019CJ0272**

Член A06P1L1L3 тълкува се от **62020CJ0184**

Член A06P3 тълкува се от **62020CJ0184**

Член A09P1 тълкува се от **62020CJ0184**

Член A02P2 тълкува се от **62018CJ0311**

Член A58P2LJ тълкува се от **62018CJ0311**

Член A02P1 тълкува се от **62018CJ0311**

Член A45 тълкува се от **62018CJ0311**

Член A46 тълкува се от **62018CJ0311**

Член A45P2 тълкува се от **62018CJ0311**

Член A46P1 тълкува се от **62018CJ0311**

Член A58P2LF тълкува се от **62018CJ0311**

Член A46P2LC тълкува се от **62018CJ0311**

Член A05P1 тълкува се от **62019CJ0439**

Член A10 тълкува се от **62019CJ0439**

Член A06P1LE тълкува се от **62019CJ0439**

тълкува се от **62020CJ0319**

Член A04PT11 тълкува се от **62019CJ0061**

Член A06P1LA тълкува се от **62019CJ0061**

Член A38P3SNT2 тълкува се от **62020CJ0534**

тълкува се от **62020CJ0175**

Член A06P1L1LF тълкува се от **62019CJ0597**

тълкува се от **62020CJ0245**

Предложение:

52012PC0011, 2016-04-27

[15 Околна среда, потребители и защита на здравето 15]

[1520 Потребители 15.20]

[152020 Информация за потребителите, образование и представяне на потребителите 15.20.20]

[19 Пространство на свобода, сигурност и правосъдие 19]

[1940 Програми 19.40]

Текст на документа в сайта на EUR-Lex

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на **Директива 95/46/ЕО** (Общ регламент относно защитата на данните)

(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** 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**),

като взеха предвид становището на Комитета на регионите(**2**),

в съответствие с обикновената законодателна процедура(**3**),

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 личните му данни.

(2) Принципите и правилата относно защитата на физическите лица във връзка с обработването на личните им данни следва, независимо от тяхното гражданство или местопребиваване, да са съобразени с техните основни права и свободи, и по-конкретно — с правото на защита на личните им данни. Настоящият регламент има за цел да допринесе за изграждането на пространство на свобода, сигурност и правосъдие и на икономически съюз, за постигането на икономически и социален напредък, за укрепването и сближаването на икономиките в рамките на вътрешния пазар, както и за благосъстоянието на хората.

(3) Целта на **Директива 95/46/ЕО на Европейския парламент и на Съвета**(**4**) е да се хармонизира защитата на основните права и свободи на физическите лица по отношение на дейностите по обработване на данни и да се осигури свободното движение на лични данни между държавите членки.

(4) Обработването на лични данни следва да е предназначено да служи на човечеството. Правото на защита на личните данни не е абсолютно право, а трябва да бъде разглеждано във връзка с функцията му в обществото и да бъде в равновесие с другите основни права съгласно принципа на пропорционалност. Настоящият регламент е съобразен с всички основни права и в него се спазват свободите и принципите, признати от **Хартата**, както са залегнали в Договорите, и по-специално зачитането на личния и семейния живот, дома и комуникациите, защитата на личните данни, свободата на мисълта, съвестта и религията, свободата на изразяване на мнение и свободата на информацията, свободата на стопанската инициатива, правото на ефективни правни средства за защита и на справедлив съдебен процес, както и културното, религиозното и езиковото многообразие.

(5) Икономическата и социална интеграция, произтичаща от функционирането на вътрешния пазар, доведе до съществено увеличение на трансграничните потоци от лични данни. Нарасна обменът на лични данни между публични и частни участници, включително физически лица, сдружения и предприятия в Съюза. Правото на Съюза предвижда националните органи в държавите членки да си сътрудничат и обменят лични данни, така че да са в състояние да изпълняват своите задължения или да изпълняват задачи от името на орган на друга държава членка.

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

(7) Тези промени изискват силна и по-съгласувана рамка за защита на данните в Съюза, подкрепена от силно правоприлагане, като се има предвид значението на изграждането на доверие, което да позволи на цифровата икономика да се развива на вътрешния пазар. Физическите лица следва да имат контрол върху собствените си лични данни. Правната и практическата сигурност за физическите лица, икономическите оператори и публичните органи следва да бъдат засилени.

(8) Когато в настоящия регламент се предвиждат уточнения или ограничения на съдържащите се в него правила от правото на държавите членки, държавите членки могат, доколкото това е необходимо с оглед на последователността и разбираемостта на националните разпоредби за лицата, по отношение на които те се прилагат, да включат елементи на настоящия регламент в собственото си право.

(9) Въпреки че целите и принципите на **Директива 95/46/ЕО** ѝ дават солидна основа, тя не предотврати фрагментирането на прилагането на защитата на данни в Съюза, нито правната несигурност и широко разпространеното в обществото схващане, че съществуват значителни рискове за защитата на физическите лица, по-специално по отношение на дейностите онлайн. Разликите в осигуреното в държавите членки ниво на защита на правата и свободите на физическите лица, по-специално на правото на защита на личните данни, във връзка с обработването на лични данни в държавите членки, могат да възпрепятстват свободното движение на лични данни в рамките на Съюза. Поради това тези разлики може да представляват препятствие за осъществяването на икономически дейности на равнището на Съюза, да нарушават конкуренцията и да възпрепятстват органите при изпълнението на техните отговорности съгласно правото на Съюза. Различието в нивата на защита се дължи на съществуването на разлики при въвеждането и прилагането на **Директива 95/46/ЕО**.

(10) За да се гарантира последователно и високо ниво на защита на физическите лица, както и за да се премахнат препятствията пред движението на лични данни в Съюза, нивото на защита на правата и свободите на физическите лица във връзка с обработването на такива данни следва да бъде равностойно във всички държави членки. Следва да се гарантира последователно и еднородно прилагане в рамките на Съюза на правилата за защита на основните права и свободи на физическите

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

(11) Ефективната защита на личните данни в рамките на Съюза изисква укрепване и подробно описание на правата на субектите на данните и задълженията на онези, които обработват и определят обработването на личните данни, както и еквивалентни правомощия за наблюдение и гарантиране на спазването на правилата за защита на личните данни и еквивалентни санкции за нарушенията в държавите членки.

(12) В **член 16, параграф 2 от ДФЕС** се възлага на Европейския парламент и Съвета да установят правилата относно защитата на физическите лица във връзка с обработването на лични данни, както и правилата, засягащи свободното движение на лични данни.

(13) За да се гарантира съгласувано ниво на защита на физическите лица в целия Съюз и да се попречи на различията да възпрепятстват свободното движение на лични данни в рамките на вътрешния пазар, е необходим регламент, който да осигурява правна сигурност и прозрачност за икономическите оператори, включително за микропредприятията и малките и средните предприятия, и да предоставя на физическите лица във всички държави членки еднакви по степен законно приложими права и задължения и отговорности за администраторите и обработващите лични данни, както и да осигури последователно наблюдение на обработването на лични данни, еквивалентни санкции във всички държави членки и ефективно сътрудничество между надзорните органи на различните държави членки. За доброто функциониране на вътрешния пазар е необходимо свободното движение на лични данни в рамките на Съюза да не се ограничава, нито забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни. За да се отчете особеното положение на микропредприятията и малките и средните предприятия, в настоящия регламент е включена дерогация за организации с по-малко от 250 служители по отношение на воденето на регистър. Освен това, институциите и органите на Съюза, както и държавите членки и техните надзорни органи се приканват да вземат предвид специфичните нужди на микропредприятията и малките и средните предприятия при прилагането на настоящия регламент. Разбирането на понятието за микропредприятия и малки и средни предприятия следва да се основава на член 2 от приложението към Препоръка **2003/361/ЕО** на Комисията(**5**).

(14) Защитата, предоставена с настоящия регламент, следва да се прилага за физическите лица, независимо от тяхното гражданство или местопребиваване, във връзка с обработването на техните лични данни. 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.

(15) 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. Защитата на физическите лица следва да се прилага за обработването на лични данни с автоматични средства, както и за ръчното им обработване, ако личните данни се съхраняват или са предназначени да се съхраняват в регистър с лични данни. Досиетата или групите от досиета, както и заглавните им страници, които не са структурирани съгласно специфични критерии, не следва да попадат в обхвата на настоящия регламент.

(16) Настоящият регламент не се прилага за въпросите на защитата на основните права и свободи или на свободното движение на лични данни, свързани с дейности, които са извън приложното поле на правото на Съюза, например дейности в областта на националната сигурност. Настоящият регламент не се прилага за обработването на лични данни от държавите членки, когато извършват дейности във връзка с общата външна политика и политика на сигурност на Съюза.

(17) **Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета**(6) се прилага за обработването на лични данни от институциите, органите, службите и агенциите на Съюза. **Регламент (ЕО) № 45/2001** и другите правни актове на Съюза, приложими за такова обработване на лични данни, следва да бъдат адаптирани към принципите и правилата, установени в настоящия регламент и прилагани съобразно настоящия регламент. С цел да се осигури силна и съгласувана рамка за защита на данните в Съюза, след приемането на настоящия регламент следва да се направят необходимите адаптации на **Регламент (ЕО) № 45/2001**, за да се даде възможност за едновременното му прилагане с настоящия регламент.

(18) Настоящият регламент не се прилага за обработването на лични данни от физическо лице в рамките на изцяло лична дейност или дейност в рамките на домакинството, която следователно няма връзка с професионална или търговска дейност. Личните дейности или дейностите в рамките на домакинството биха могли да включват воденето на кореспонденция и поддържането на адресни указатели или участието в социални мрежи и онлайн дейности, предприети в контекста на тези дейности. Настоящият регламент обаче се прилага за администратори или обработващи лични данни, които осигуряват средствата за обработване на лични данни при такива лични дейности или дейности в рамките на домакинството.

(19) 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 наложените наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване, както и свободното движение на такива данни, са предмет на специален правен инструмент на Съюза. Следователно настоящият регламент не следва да се прилага за дейности по обработване на лични данни за такива цели. Обработването на лични данни от страна на публичните органи по силата на настоящия регламент, когато е за тези цели, обаче следва да бъде уредено с по-специфичен правен акт на Съюза, а именно с **Директива (ЕС) 2016/680 на Европейския парламент и на Съвета**(7). Държавите членки могат да възлагат на компетентните органи по смисъла на **Директива (ЕС) 2016/680** други задачи, чието изпълнение не е свързано задължително с целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от заплахи за обществената сигурност и предотвратяването им, така че обработването на лични данни за тези цели, доколкото то е в обхвата

на правото на Съюза, попада в приложното поле на настоящия регламент.

По отношение на обработването на лични данни от тези компетентни органи за цели, попадащи в обхвата на настоящия регламент, държавите членки следва да могат да запазят или да въведат по-конкретни разпоредби, за да адаптират прилагането на разпоредбите на настоящия регламент. Подобни разпоредби могат да определят по-точно специфичните изисквания относно обработването на личните данни от тези компетентни органи за посочените други цели, като се взема предвид конституционната, организационната и административната структура на съответната държава членка. Когато обработването на лични данни от частни структури попада в приложното поле на настоящия регламент, регламентът следва да предвижда възможност при определени условия държавите членки да наложат със закон ограничения върху определени задължения и права, ако такова ограничение представлява необходима и пропорционална мярка в едно демократично общество за защита на конкретни значими интереси, включително обществената сигурност и предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наложените наказания, включително предпазването от заплахи за обществената сигурност и предотвратяването им. Това е от значение например в рамките на дейностите срещу изпирането на пари или на дейностите на съдебномедицинските лаборатории.

(20) Макар настоящият регламент да се прилага, inter alia, спрямо дейностите на съдилищата и други съдебни органи, в правото на Съюза или в правото на държава членка могат да се определят конкретно операциите и процедурите по обработване на лични данни от съдилищата и другите съдебни органи. Компетентността на надзорните органи не следва да обхваща обработването на лични данни, когато съдилищата действат при изпълнение на своите съдебни функции, за да се гарантира независимостта на съдебната власт при изпълнението на съдебните ѝ задължения, включително вземането на решения. Следва да е възможно да се повери надзорът на такива операции по обработване на данни на специални органи в рамките на съдебната система на държавата членка, които по-конкретно следва да осигурят спазването на правилата на настоящия регламент, да повишават осведомеността сред членовете на съдебното съсловие за техните задължения по силата на настоящия регламент и да се занимават с жалбите във връзка с такива операции по обработване на данни.

(21) Настоящият регламент не засяга прилагането на **Директива 2000/31/ЕО на Европейския парламент и на Съвета**(**8**), и по-специално разпоредбите относно междинните доставчици на услуги в **членове 12—15** от посочената директива. Тази директива има за цел да допринесе за нормалното функциониране на вътрешния пазар, като осигурява свободното движение на услуги на информационното общество между държавите членки.

(22) Всякакъв вид обработване на лични данни в контекста на дейностите на мястото на установяване на администратор или на обработващ лични данни в Съюза следва да се извършва в съответствие с настоящия регламент, независимо от това дали самото обработване се извършва в рамките на Съюза. Установяването предполага ефективното и действителното упражняване на дейност по силата на стабилни договорености. Правната форма на тези договорености, независимо дали става въпрос за клон или дъщерно дружество с правосубектност, не е определящ фактор в това отношение.

(23) За да се гарантира, че физическите лица не са лишени от защитата, на която те имат право по силата на настоящия регламент, обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ лични данни, който не е установен в Съюза,

следва да подлежи на разпоредбите на настоящия регламент в случаите, когато дейностите по обработване на данни са свързани с предлагането на стоки или услуги на такива субекти на данни, независимо дали това е свързано с плащане. За да се установи дали този администратор или обработващ лични данни предлага стоки или услуги на субекти на данни, които се намират в Съюза, следва да бъде уточнено дали е очевидно, че администраторът или обработващият данни възнамерява да предлага услуги на субекти на данни в една или повече държави членки в Съюза. Като се има предвид, че само достъпността на уебсайт на посредник в Съюза, на администратора или обработващия данни, на електронен адрес или на други данни за контакт или използването на език, който по правило се използва в третата държава, където е установен администраторът, са недостатъчни за удостоверяване на такова намерение, фактори като използването на език или парична единица, които по правило се използват в една или повече държави членки, наред с възможността за поръчване на стоки и услуги на този друг език или споменаването на потребители или ползватели, които се намират в Съюза, могат да свидетелстват за това, че администраторът възнамерява да предлага стоки или услуги на субекти на данни в Съюза.

(24) Обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ лични данни, който не е установен в Съюза, следва също да се урежда от настоящия регламент, когато е свързано с наблюдението на поведението на такива субекти на данни, доколкото тяхното поведение се проявява в рамките на Съюза. С цел да се определи дали дадена дейност по обработване може да се смята за наблюдение на поведението на субектите на данни, следва да се установи дали физическите лица се следят в интернет, включително да се установи евентуално последващо използване на техники за обработване на лични данни, които се състоят в профилиране на дадено физическо лице, по-специално с цел да се вземат отнасящи се до него решения или да се анализират или предвиждат неговите лични предпочитания, поведение и начин на мислене.

(25) Когато правото на дадена държава членка се прилага по силата на международното публично право, настоящият регламент следва да се прилага и спрямо администратор, който не е установен в Съюза, например ако е установен в дипломатическа мисия или консулска служба на държава членка.

(26) 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 установи дали има достатъчна вероятност дадени средства да бъдат използвани за идентифициране на физическото лице, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат наличните към момента на обработване на данните технологии и технологичните развития. Поради това принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, т.е. 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 да не може или вече не може да бъде идентифициран. Ето защо настоящият регламент не се отнася за обработването на такава анонимна информация, включително

за статистически или изследователски цели.

(27) Настоящият регламент не следва да се прилага за личните данни на починали лица. Държавите членки могат да предвидят правила във връзка с обработването на лични данни на починали лица.

(28) 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.

(29) За да се създадат стимули за прилагане на псевдонимизация при обработването на лични данни, като същевременно се дава възможност за общ анализ, мерките за псевдонимизация следва да са възможни при един и същи администратор на данни, когато той е взел необходимите технически и организационни мерки, за да се гарантира при съответната обработка, че настоящият регламент е приложен и че допълнителната информация, свързваща личните данни с конкретен субект на данните, се съхранява отделно. Администраторът, който обработва личните данни, следва да посочва упълномощените лица в рамките на същия администратор на данни.

(30) 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.

(31) Публични органи, пред които се разкриват лични данни в съответствие с правно задължение за упражняване на официалната им функция, например данъчни и митнически органи, звена за финансово разследване, независими административни органи или органи за финансовите пазари, отговарящи за регулирането и надзора на пазарите на ценни книжа, не следва да се разглеждат като получатели, ако получават лични данни, които са необходими за провеждането на конкретно разследване от общ интерес, в съответствие с правото на Съюза или на държава членка. Исканията за разкриване на данни, изпратени от публичните органи, следва винаги да бъдат в писмена форма, да са обосновани и да засягат само отделни случаи и не следва да се отнасят до целия регистър с лични данни или да водят до свързване на регистри на лични данни. Обработването на личните данни от посочените публични органи следва да е в съответствие с приложимите правила за защита на данните съобразно целите на обработването.

(32) 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.

(33) Често в момента на събиране на данните целта на обработването на лични данни за научноизследователски цели не може да бъде напълно определена. 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 преследваната цел.

(34) Генетичните данни следва да се определят като лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които са получени в резултат на анализ на биологична проба от въпросното физическо лице, по-специално чрез хромозомен анализ, анализ на дезоксирибонуклеиновата киселина (ДНК) или на рибонуклеиновата киселина (РНК) или анализ на всеки друг елемент, позволяващ получаване на равностойна информация.

(35) Личните данни за здравословното състояние следва да обхващат всички данни, свързани със здравословното състояние на субекта на данните, които разкриват информация за физическото или психическото здравословно състояние на субекта на данните в миналото, настоящето или бъдещето. Това включва информация относно физическото лице, събрана в хода на регистрацията за здравни услуги или тяхното предоставяне, както е посочено в **Директива 2011/24/ЕС на Европейския парламент и на Съвета**(**9**), на същото физическо лице; номер, символ или характеристика, определени за дадено физическо лице с цел уникалното му идентифициране за здравни цели; информация, получена в резултат от изследването или прегледа на част от тялото или на телесно вещество, включително от генетични данни и биологични проби; и всякаква информация, например за заболяване, увреждане, риск от заболяване, медицинска история, клинично лечение или физиологично или биомедицинско състояние на субекта на данните, независимо от източника на информация, като например лекар или друг медицински специалист, болница, медицинско изделие или ин витро диагностично изследване.

(36) Основното място на установяване на администратор на данни в Съюза следва да бъде мястото в Съюза, където се намира централното му управление в Съюза, освен ако решенията относно целите и средствата за обработването на лични данни не се вземат на друго място на установяване на администратора на данни в Съюза, в който случай това друго място на установяване следва да се счита за основното място на установяване. Основното място на установяване на администратор в Съюза следва да се определя съгласно обективни критерии и следва да означава ефективното и действително упражняване на управленски дейности, определящи основните решения по отношение на целите и средствата за обработване на данни по силата на стабилни договорености. Този критерий не следва да зависи от това дали обработването на лични данни се извършва на това място. Наличието и употребата на технически средства и технологии за обработване на лични данни или дейностите по обработване не представляват сами по себе си основно място на установяване и следователно не са определящи критерии за понятието „основно място на установяване“. Основното място на установяване на обработващия лични данни следва да бъде мястото, където се намира централното му управление в Съюза, а ако няма централно управление в Съюза, мястото в Съюза, където се осъществяват основните дейности по обработването. В случаи, когато участват и администратор, и обработващ лични данни, компетентният водещ надзорен орган следва да остане надзорният орган на държавата членка, в която се намира основното място на установяване на

администратора, а надзорният орган на обработващия лични данни следва да се счита за засегнат надзорен орган и този надзорен орган следва да участва в процедурата за сътрудничество, предвидена в настоящия регламент. При всички положения надзорните органи на държавата членка или държавите членки, където е установен обработващият лични данни, не следва да се считат за засегнати надзорни органи, когато проектът за решение засяга единствено администратора. Когато обработването се извършва от група предприятия, основното място на установяване на контролиращото предприятие следва да се счита за основно място на установяване на групата предприятия, с изключение на случаите, в които целите и средствата на обработването на данни се определят от друго предприятие.

(37) Дадена група предприятия следва да обхваща контролиращо предприятие и контролираните от него предприятия, като контролиращото предприятие следва да бъде предприятие, което може да упражнява доминиращо влияние върху другите предприятия въз основа на това, че има например право на собственост или финансово участие, или въз основа на правилата за неговото управление или правомощието да прилага правила за защита на личните данни. Предприятие, което осъществява контрол на обработването на лични данни в свързани с него предприятия, следва да се разглежда, заедно с тези предприятия,като „група предприятия“.

(38) 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 използването на лични данни на деца за целите на маркетинга или за създаване на личностни или потребителски профили и събирането на лични данни по отношение на деца при ползване на услуги, предоставяни пряко на деца. Съгласието на носещия родителска отговорност не следва да е необходимо в контекста на пряко предлаганите на деца услуги за превенция и консултиране.

(39) 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 принципа 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 и до оборудване за тяхното обработване или за предотвратяване на използването им.

(40) За да бъде обработването законосъобразно, личните данни следва да бъдат обработвани въз основа на съгласието на съответния субект на данни или на друго легитимно основание, установено по законодателен път в настоящия регламент или в друг правен акт на Съюза или на държава членка, както е посочено в настоящия регламент, включващо необходимостта от спазване на правното задължение, наложено на администратора на лични данни, или 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.

(41) Когато в настоящия регламент се прави позоваване на правно основание или законодателна мярка, това не налага непременно приемането на законодателен акт от парламент, без с това да се засягат изискванията съгласно конституционния ред на съответната държава членка. Такова правно основание или законодателна мярка обаче следва да бъдат ясни и точни и прилагането им следва да бъде предвидимо за лицата, за които се прилагат, в съответствие с практиката на Съда на Европейския съюз („Съдът“) и на Европейския съд по правата на човека.

(42) 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**(**10**) 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 които 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.

(43) 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, по-специално когато администраторът е публичен орган, поради което изглежда малко вероятно съгласието да е дадено свободно при всички обстоятелства на конкретната ситуация. Смята се, че съгласието не е дадено свободно, ако не се предоставя възможност да бъде дадено отделно съгласие за различните операции по обработване на лични данни, макар и да е подходящо в конкретния случай, или ако изпълнението на даден договор, включително предоставянето на услуга, се поставя в зависимост от даването на съгласие, въпреки че това съгласие не е необходимо за изпълнението.

(44) Обработването на данни следва да е законосъобразно, когато то е необходимо в контекста на договор или при намерение за сключване на договор.

(45) Когато обработването се извършва в съответствие с правно задължение, наложено на администратора на лични данни, или когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официални правомощия, за обработването следва да има основание в правото на Съюза или в правото на държава членка. Настоящият регламент не

изисква за всяко отделно обработване конкретен законодателен акт. Може да е достатъчен законодателен акт като основание за няколко операции по обработване на данни, основаващи се на правно задължение, наложено на администратора на лични данни, или когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официални правомощия. Правото на Съюза или на държава членка следва да определя също и целта на обработването. Нещо повече, в това право биха могли да се посочат общите условия на настоящия регламент, които определят законосъобразността на обработването на лични данни, да се установяват спецификациите за определянето на администратора на лични данни, видът данни, които подлежат на обработване, съответните субекти на лични данни, образуванията, пред които могат да бъдат разкривани лични данни, ограниченията по отношение на целите, периодът на съхранение и други мерки за гарантиране на законосъобразното и добросъвестно обработване. Също така в правото на Съюза или на държава членка следва да се определи дали администраторът на лични данни, изпълняващ задача от обществен интерес или упражняващ официални правомощия, следва да бъде публичен орган или друго физическо или юридическо лице, субект на публичното право или когато това е оправдано поради съображения от обществен интерес, включително за здравни цели, като например общественото здраве и социалната закрила и управлението на здравните служби субект на частното право, като например професионално сдружение.

(46) 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.

(47) Законните интереси на даден администратор, включително на администратор, пред когото може да бъдат разкрити лични данни, или на трета страна могат да предоставят правно основание за обработването, при условие че интересите или основните права и свободи на съответния субект на данни нямат преимущество, като се вземат предвид основателните очаквания на субектите на данни въз основа на техните взаимоотношения с администратора.Такъв законен интерес може да е налице, когато например между субекта на данни и администратора на лични данни съществува съответното определено взаимоотношение, например когато субектът на данни е клиент или подчинен на администратора на лични данни. При всички случаи, за установяването на законен интерес би била необходима внимателна преценка, включително дали субектът на данни може по времето и в контекста на събирането на данни основателно да очаква, че може да се осъществи обработване на личните данни за тази цел. Интересите и основните права на субекта на данни биха могли по-конкретно да имат преимущество пред интереса на администратора, когато личните данни се обработват при обстоятелства, при които субектите на данни основателно не очакват по-нататъшна обработка. Като се има предвид, че е задължение на законодателя да уреди със закон правното основание за обработването на лични данни от публичните органи, това правно основание не следва да се прилага спрямо обработването на данни от публичните органи при изпълнението на техните задачи. Обработването на лични данни, строго необходимо за целите на предотвратяването на измами, също представлява законен интерес на съответния администратор на данни. Обработването на лични данни за целите на директния маркетинг може да се разглежда като осъществявано поради законен интерес.

(48) Администратори, които представляват част от група предприятия или институции, свързана с централен орган, могат да имат законен интерес да предадат личните данни в рамките на групата предприятия за вътрешни административни цели, включващи обработването на лични данни на клиенти или служители. Общите принципи на предаването на лични данни на предприятие, разположено в трета държава, в рамките на група предприятия, остават непроменени.

(49) Обработването на лични данни в степен, която е строго необходима и пропорционална на целите на гарантирането на мрежовата и информационната сигурност, т.е. способността на дадена мрежа или информационна система да издържа, със съответно равнище на доверие, на случайни събития или неправомерни или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхраняваните или предаваните лични данни, както и на сигурността на свързаните услуги, предлагани или достъпни посредством тези мрежи и системи, от страна на публични органи, екипи за незабавно реагиране при компютърни инциденти (ЕНРКИ), екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), доставчици на мрежи и услуги за електронни съобщения и доставчици на технологии и услуги за сигурност, представлява законен интерес на съответния администратор на данни. Това може да включва например предотвратяването на непозволен достъп до електронни съобщителни мрежи и разпространение на зловреден софтуер и спиране на атаки с цел отказване на услугите и вреди за компютрите и електронните съобщителни системи.

(50) 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 на лични данни, в правото на Съюза или в правото на държава членка 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 съвместими законосъобразни операции по обработване. Правното основание, предвидено от правото на Съюза или правото на държава членка 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 им, 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.

Когато субектът на данните е дал съгласието си или когато обработването се основава на правото на Съюза или правото на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество, за да се гарантират по-специално важни цели от широк обществен интерес, на администратора следва да се позволи да обработва по-нататък личните данни,

независимо от съвместимостта на целите. Във всеки случай, прилагането на принципите, установени в настоящия регламент, и по-специално информирането на субекта на данните относно тези други цели и относно неговите права, включително правото да възрази, следва да бъдат гарантирани. Съобщаването от администратора за евентуални престъпни деяния или заплахи за обществената сигурност и предаването на съответните лични данни в отделни случаи или в няколко случая, свързани с едно и също престъпно деяние или заплахи за обществената сигурност, на компетентен орган следва да се разглеждат като част от законния интерес, преследван от администратора. Въпреки това, подобно предаване, което е от законен интерес за администратора, или по-нататъшно обработване на лични данни следва да бъдат забранени, ако обработването не е съвместимо с никакво правно, професионално или друго обвързващо задължение за пазене на тайна.

(51) 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. 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 или удостоверяване на автентичността на дадено физическо лице. Тези лични данни не следва да се обработват, освен ако обработването не е разрешено в определени случаи, предвидени в настоящия регламент, като се има предвид, че в правото на държавите членки могат да бъдат определени специфични разпоредби за защита на данните с цел да се адаптира прилагането на съдържащите се в настоящия регламент правила за спазване на правно задължение или за изпълнение на задача от обществен интерес или свързана с упражняването на официални правомощия, предоставени на администратора на лични данни. В допълнение към конкретните изисквания за такова обработване 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.

(52) Дерогация от забраната за обработване на специални категории лични данни също следва бъде разрешена, когато е предвидена в правото на Съюза или правото на държава членка, и при подходящи гаранции, така че да бъдат защитени личните данни и други основни права, когато съображения, свързани с обществения интерес, оправдават това, по-специално обработването на лични данни в областта на трудовото право, правото в областта на социалната закрила, включително пенсиите, както и за целите на сигурността, наблюдението и предупрежденията в сферата на здравеопазването, предотвратяването или контрола на заразните болести и други сериозни заплахи за здравето. Такава дерогация може да се извърши за здравни цели, включително общественото здраве и управлението на здравните услуги, особено с цел да се гарантират качеството и рентабилността на използваните процедури за уреждане на искове за обезщетения и услуги в системата за здравно осигуряване, или за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели. Чрез дерогация следва да се даде възможност да се обработват и такива лични данни, когато е необходимо, с цел установяване, упражняване или защита на правни претенции, независимо дали това е в рамките на съдебна, административна или

друга извънсъдебна процедура.

(53) Специални категории лични данни, които се нуждаят от по-голяма защита, могат да бъдат обработвани единствено за здравни цели, когато е необходимо тези цели да бъдат постигнати в полза на отделни физически лица и на обществото като цяло, по-специално в рамките на управлението на услугите и системите за здравеопазване или социални грижи, включително обработването от страна на органите за управление и от централните национални здравни органи на такива данни за целите на контрола на качеството, информацията за управлението и общото наблюдение на национално и местно равнище на системата за здравеопазване или социални услуги, както и за осигуряване на непрекъснатост на здравното обслужване или на социалните услуги и на трансграничното здравно обслужване или за целите на сигурността, наблюдението и предупрежденията в сферата на здравеопазването, или за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели въз основа на правото на Съюза или националното право, което трябва да отговаря на цел от обществен интерес, както и за проучванията в областта на общественото здраве, провеждани в обществен интерес. Поради това настоящият регламент следва да предвижда хармонизирани условия за обработването на специални категории лични данни за здравословното състояние по отношение на специфични нужди, по-специално когато обработването на тези данни се извършва за определени цели, свързани със здравето, от лица, обвързани от правното задължение за професионална тайна. Правото на Съюза или националното право следва да предвижда конкретни и подходящи мерки за защита на основните права и личните данни на физическите лица. Държавите членки следва да разполагат с възможност да запазят или да въведат допълнителни условия, включително ограничения, по отношение на обработването на генетични, биометрични или данни за здравословното състояние. Това обаче не следва да възпрепятства свободното движение на лични данни в рамките на Съюза, когато тези условия се прилагат за трансгранично обработване на такива данни.

(54) 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**(**11**) 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 от трети страни като работодатели или застрахователни дружества и банки.

(55) Освен това обработването на лични данни от официални органи за постигането на целите, определени в конституционното право или в международното публично право, на официално признати религиозни сдружения се извършва по съображения от обществен интерес.

(56) Когато демократичната система в дадена държава членка предполага по време на предизборна дейност политическите партии да събират лични данни за политическите възгледи на гражданите, обработването на тези данни може да бъде разрешено по съображения от обществен интерес, при условие че са предвидени подходящи гаранции.

(57) 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.

(58) Принципът на прозрачност изисква всяка информация както за обществеността, така и за субекта на данните да бъде в кратка, прозрачна, разбираема и лесно достъпна форма и да се използват ясни и недвусмислени формулировки, а в допълнение когато е необходимо, да се използва и визуализация. Тази информация може да бъде представена в електронна форма, например чрез уебсайт, когато е адресирана до обществеността. Това важи в особена степен за ситуации, където нарастването на участниците и технологичната сложност на тази практика правят трудно за субекта на данни да узнае и разбере дали се събират свързани с него лични данни, от кого и с каква цел, като в случая на онлайн рекламите. Като се има предвид, че на децата се полага специална защита, когато обработването е насочено към дете, всяка информация и комуникация следва да се предоставя с ясни и недвусмислени формулировки, които да бъдат лесноразбираеми за детето.

(59) 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.

(60) 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.

(61) 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.

(62) Не е необходимо обаче да се налага задължение за предоставяне на информация, когато субектът на данни вече разполага с информацията, когато записването или разкриването на личните данни е изрично предвидено със закон или когато предоставянето на информация на субекта на данни се окаже невъзможно или изисква непропорционално големи усилия. Такъв би бил случаят по-специално когато обработването се извършва за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели. В този контекст следва да бъде взет предвид броят на субектите на данни, актуалността на данните и съответните установени гаранции.

(63) 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. Когато е възможно, администраторът следва да може да предоставя достъп от разстояние до сигурна система, която да предоставя на субекта на данните пряк достъп до неговите лични данни. 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.

(64) Администраторът следва да използва всички разумни мерки за проверка на самоличността на субекта на данни, който иска достъп, по-специално по отношение на онлайн услугите и онлайн идентификаторите. Администраторът не следва да запазва лични данни с единствената цел да може да реагира на евентуални искания.

(65) Субектът на данни следва да има право на коригиране на личните данни, свързани с него, както и правото „да бъде забравено“, когато запазването на тези данни е в нарушение на настоящия регламент или на правото на Съюза или правото на държава членка, под чиято юрисдикция е администраторът. По-специално, 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 публичен 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 искове.

(66) 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 уведоми 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, в това число технически мерки, за да информира администраторите, които обработват личните данни, за искането на субекта на данните.

(67) 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.

(68) С цел допълнително засилване на контрола над собствените данни, когато обработването на лични данни става по автоматичен начин, 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. Правото не следва да се прилага, когато обработването се базира на правно основание, различно от съгласие или договор. Поради самото си естество това право не следва да бъде упражнявано по отношение на администратори, обработващи данни в изпълнение на обществените си задължения. Ето защо това право не следва да се прилага, когато обработването на личните данни е необходимо за спазване на правно задължение, на което е подчинен администраторът, 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.

(69) Когато личните данни биха могли да се обработват законно, тъй като обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официално правомощие, предоставено на администратора, или по съображения, свързани със законните интереси на администратора или на трета страна, 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 преимущество пред интересите или основните права и свободи на субекта на данни.

(70) Когато личните данни се обработват за целите на директния маркетинг, субектът на данни следва да има право безплатно и по всяко време да направи възражение срещу такова обработване, включително профилиране, доколкото то е свързано с директния маркетинг, независимо дали става въпрос за първоначално или по-нататъшно обработване. Субектът на данни изрично следва да бъде уведомен за съществуването на това право, което му се представя по ясен начин и отделно от всяка друга информация.

(71) Субектът на данни следва да има право да не бъде обект на решение, което може да включва мярка, за оценка на свързани с него лични аспекти единствено въз основа на автоматично обработване, и което поражда правни последствия за него или го засяга също толкова значително, като например автоматичен отказ на онлайн искания за кредит или 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 резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията, 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 или правото на държава членка, под чиято юрисдикция е администраторът, включително за целите на наблюдението и предотвратяването на измами и укриването на данъци, осъществявани в съответствие с разпоредбите, стандартите и препоръките на институциите на Съюза или националите надзорни органи, и за гарантиране на сигурността и надеждността на услугите, предоставяни от администратора, или когато е необходимо за сключването или изпълнението на договор между субект на данни и администратор, или когато субектът на данни е дал изричното си съгласие. 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 който не поражда, inter alia, ефект на дискриминация за физическите 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 от който не 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.

(72) Профилирането се подчинява на правилата на настоящия регламент относно обработването на лични данни, например правните основания за обработването или принципите за защитата на данни. Европейският комитет по защита на данните, създаден с настоящия регламент („Комитетът“), следва да може да издава насоки в това отношение.

(73) Ограничения относно специални принципи и относно правото на информация, достъп до, и коригиране или изтриване на лични данни, правото на преносимост на данните, правото на оспорване на решения, основани на профилиране, както и уведомяването на субекта на данни за нарушение на сигурността на личните данни и определени свързани с това задължения на администраторите, могат да бъдат налагани от правото на Съюза или от правото на държава членка, доколкото това е необходимо и пропорционално в едно демократично общество с оглед защитата на обществената сигурност, включително защитата на човешкия живот, особено при природни или предизвикани от човека бедствия, предотвратяването, разследването и наказателното преследване на престъпления или изпълнението на наложените наказания, включително защитата срещу заплахи пред обществената сигурност и тяхното предотвратяване, или нарушения на етичните кодекси при регламентираните професии, други важни цели от общ обществен интерес на Съюза или на държава членка, и по-специално важен икономически или финансов интерес на Съюза или на държава членка, поддържането на публичен регистър поради причини от широк обществен интерес, по-нататъшното обработване на архивирани лични данни с цел предоставяне на конкретна информация, свързана с политическото поведение по време на бивши режими в тоталитарни държави или защитата на субекта на данни или на правата и свободите на други лица, включително социалната защита, общественото здраве и хуманитарните цели. Тези ограничения следва да бъдат в съответствие с изискванията, определени в **Хартата** и в **Европейската конвенция за защита на правата на човека и основните свободи**.

(74) 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.

(75) 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, материални или нематериални 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; или когато субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни;

когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, и обработването на генетични данни, данни за здравословното състояние или данни за сексуалния живот или за присъди и нарушения или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили; когато се обработват лични данни на уязвими лица, по-специално на деца; или когато обработването включва голям обем лични данни и засяга голям брой субекти на данни.

(76) 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.

(77) Насоки за прилагането на подходящи мерки и за доказване на съответствие от страна на администратора или обработващия лични данни, особено по отношение на идентифицирането на риска, свързан с обработването, оценката по отношение на произход, естество, вероятност и тежест и определянето на добри практики за ограничаване на риска, биха могли да се предоставят по-специално чрез одобрени кодекси на поведение, одобрени механизми за сертифициране, насоки на Комитета или чрез указания, предоставени от длъжностното лице за защита на данните. Комитетът може също да издава насоки относно операции по обработване, за които се счита, че е малко вероятно да доведат до висок риск за правата и свободите на физическите лица, и да даде указания какви мерки могат да бъдат достатъчни в такива случаи за преодоляването на такъв риск.

(78) 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 съответствието с 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. При разработването, проектирането, подбора и използването на приложения, услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, за да изпълнят функцията си, производителите на продукти, услуги и приложения следва да бъдат насърчавани да вземат предвид правото на защита на лични данни при разработването и проектирането на такива продукти, услуги и приложения и като отчитат надлежно достиженията на техническия прогрес, да се уверят, че администраторите и обработващите лични данни са в състояние да изпълняват своите задължения за защита на данните. 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.

(79) Защитата на правата и свободите на субектите на данни, както и отговорността и задълженията на администраторите и обработващите лични данни, а също и по отношение на наблюдението и мерките от страна на надзорните органи, 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.

(80) Когато даден администратор или обработващ лични данни, който не е установен в Съюза, обработва лични данни на субекти на данни, които се намират в Съюза, и дейностите му по обработването са свързани с предлагането на стоки или услуги, независимо дали от субекта на данни се изисква плащане, на такива субекти на данни в Съюза или за наблюдението на тяхното поведение, доколкото поведението им се проявява в рамките на Съюза, администраторът или обработващият лични данни следва да определи представител, освен ако обработването не засяга само отделни случаи, не включва мащабно обработване на специалните категории лични данни или обработване на лични данни, свързани с присъди и нарушения и няма вероятност да породи риск за правата и свободите на физическите лица, предвид естеството, контекста, обхвата и целите на обработването, или ако администраторът е публичен орган или структура. Представителят следва да действа от името на администратора или обработващия лични данни, а надзорният орган може да се обръща към него. Представителят следва да бъде посочен изрично от администратора или от обработващия лични данни с писмен мандат да действа от негово име във връзка с неговите задължения съгласно настоящия регламент. Посочването на такъв представител не засяга отговорностите или задълженията на администратора или на обработващия лични данни съгласно настоящия регламент. Този представител следва да изпълнява задачите си в съответствие с получения от администратора или обработващия лични данни мандат, включително да си сътрудничи с компетентните надзорни органи във връзка с всяко действие, което предприема, за да се осигури спазването на настоящия регламент. Посоченият представител следва да бъде обект на правоприлагащи процедури, в случай на нарушение от страна на администратора или обработващия лични данни.

(81) 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 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 ще предприемат технически и организационни мерки, които отговарят на изискванията на настоящия регламент, включително на изискванията за сигурността на обработването. Придържането от страна на обработващия лични данни 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 следва да се урежда с договор или друг правен акт, съгласно правото на Съюза или правото на държава членка, 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 могат да изберат да използват индивидуален договор или стандартни договорни клаузи, приети или пряко от Комисията, или от надзорен орган в съответствие с механизма за съгласуваност 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 личните данни по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни.

(82) За да докаже спазването на настоящия регламент, администраторът или обработващият данни следва да поддържа документация за дейностите по обработване, за които той е отговорен. Всеки администратор и обработващ лични данни следва да е длъжен да си сътрудничи с надзорния орган и да му осигури достъп до тази документация при поискване, за да може да бъде използвана за наблюдение на тези операции по обработване.

(83) 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, материални или нематериални вреди.

(84) За да се подобри спазването на настоящия регламент, когато има вероятност операциите по обработването да доведат до висок риск за правата и свободите на физическите лица, администраторът следва да отговаря за изготвянето на оценка на въздействието върху защитата на личните данни, за да се оценят по-специално произходът, естеството, спецификата и степента на този риск. Резултатите от оценката следва да бъдат взети предвид, когато се определят съответните мерки, за да се докаже, че обработването на лични данни отговаря на изискванията на настоящия регламент. Когато в оценка на въздействието върху защитата на личните данни е указано, че операциите по обработването водят до висок риск, който администраторът не може да ограничи с подходящи мерки от гледна точка на налични технологии и разходи за прилагане, преди обработването следва да се осъществи консултация с надзорния орган.

(85) Нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен начин, да доведе до физически, материални или нематериални вреди за физическите лица, като загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица. Поради това, веднага след като установи нарушение на сигурността на личните данни, администраторът следва да уведоми надзорния орган 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 не 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 че информацията може да се подаде поетапно без ненужно допълнително забавяне.

(86) 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 надзорния орган, като се спазват насоките, предоставени от него или от други съответни органи, като правоприлагащите органи. Така например необходимостта да се ограничи непосредственият риск от вреди би наложила незабавното уведомяване на субектите на данните, докато необходимостта от предприемането на целесъобразни мерки срещу продължаването на нарушения на сигурността на личните данни или срещу подобни нарушения би оправдало по-дълги срокове за уведомлението.

(87) Следва да се установи дали са били приложени всички подходящи мерки за технологична защита и организационни мерки, за да се определи незабавно дали е налице нарушение на лични данни и своевременно да се информират надзорният орган и субектът на данни. Фактът, че уведомлението е направено без ненужно забавяне следва да бъде установен, като се отчитат по-конкретно естеството и тежестта на нарушението на личните данни и последиците и неблагоприятното въздействие от него върху субекта на данни. Такова уведомление може да доведе до намесата на надзорния орган в съответствие със задачите и правомощията, които са му предоставени с настоящия регламент.

(88) При установяване на подробни правила за формàта и процедурите, приложими за уведомяването за нарушения на сигурността на личните данни, следва да се отдаде необходимото внимание на обстоятелствата, свързани с нарушението, включително дали личните данни са били защитени чрез подходящи технически мерки за защита, ефективно ограничаващи вероятността за измама с фалшива самоличност или други форми на злоупотреба. Освен това при такива правила и процедури следва да се отчитат законните интереси на правоприлагащите органи, когато ранното разкриване може ненужно да попречи при разследването на обстоятелствата, свързани с нарушението на сигурността на личните данни.

(89) В **Директива 95/46/ЕО** се предвижда общо задължение за уведомяване на надзорните органи относно обработването на лични данни. Това задължение създава административна и финансова тежест и невинаги е допринасяло за подобряването на защитата на личните данни. Ето защо такива неправещи разграничения общи задължения за уведомяване следва да бъдат премахнати и заменени с ефективни процедури и механизми, които да са насочени към 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 могат да бъдат операциите по обработване, които по-конкретно включват използването на нови технологии или представляват нов вид технологии и при 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.

(90) 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 съответствието с настоящия регламент.

(91) Това следва да се прилага по-специално за широкомащабни операции по обработване, чиято цел е обработване на значителен обем лични данни на регионално, национално и наднационално равнище, които биха могли да засегнат голям брой субекти на данни и които е вероятно да доведат до висок риск, например поради чувствителното си естество, когато в съответствие с постигнатото ниво на технически познания се използва нова технология в голям мащаб, както и за други операции по обработване, които пораждат висок риск за правата и свободите на субектите на данни, по-специално когато тези операции затрудняват субектите на данни да упражняват правата си. Оценка на въздействието върху защитата на данни следва да се извършва и когато личните данни се обработват с цел вземане на решения относно конкретни физически лица след систематична и обстойна оценка на личните аспекти, свързани с физически лица, въз основа на профилирането на тези данни или след обработването на специални категории лични данни, биометрични данни или данни за присъди и нарушения или свързани с това мерки за сигурност. Оценка на въздействието върху защитата на данните се изисква също за широкомащабно наблюдение на публично достъпни зони, особено когато се използват оптичноелектронни уреди, или за всякакви други операции, когато компетентният надзорен орган счита, че има вероятност обработването да доведе до висок риск за правата и свободите на субектите на данни, по-специално поради това, че възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор, или поради това, че се извършват систематично в голям мащаб. Обработването на лични данни не следва да се счита за широкомащабно, ако засяга лични данни на пациенти или клиенти на отделен лекар, друг здравен работник или адвокат. В такива случаи оценката на въздействието върху защитата на данните не следва да бъде задължителна.

(92) При определени обстоятелства може да бъде разумно и рентабилно предметът на дадена оценка на въздействието върху защитата на данните да обхваща повече от един проект, например когато обществени органи или структури възнамеряват да създадат общо приложение или платформа за обработване на данни или когато няколко администратори планират внедряването на общо приложение или среда за обработване на данните в цял промишлен сектор или сегмент или за широко използвана хоризонтална дейност.

(93) В контекста на приемането на право на държава членка, на чието основание съответният публичният орган или структура изпълнява своите задачи и които уреждат въпросната конкретна операция или набор от операции по обработване на данни, държавите членки могат да сметнат за необходимо да извършат такива оценки преди започване на дейностите по обработването.

(94) 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 надзорния орган. 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. Надзорният орган следва да отговори на искането за консултация в рамките на определен срок. Въпреки това отсъствието на отговор от надзорния орган в рамките на този срок не следва да препятства евентуалната намеса на надзорния орган 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, на надзорния орган може да се представи 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.

(95) При необходимост и при поискване, обработващият лични данни следва да подпомага администратора, за да се гарантира спазването на задълженията, произтичащи от извършването на оценки на въздействието върху защитата на личните данни и от предварителната консултация с надзорния орган.

(96) Следва да се проведе консултация с надзорния орган и при изготвяне на законодателна или регулаторна мярка, която предвижда обработване на лични данни, за да се гарантира, че планираното обработване отговаря на изискванията на настоящия регламент, и по-специално за да се ограничат рисковете, свързани със субекта на данни.

(97) Когато обработването на данни се извършва от публичен орган, с изключение на съдилища или съдебни органи, които действат в изпълнение на съдебните си функции, когато в частния сектор обработването се извършва от администратор, чиито основни дейности се състоят от операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни, или когато основните дейности на администратора или на обработващия лични данни се състоят в мащабно обработване на специални категории лични данни и данни относно присъди и нарушения, администраторът или обработващият лични данни следва да бъде подпомаган при наблюдението на вътрешното спазване на настоящия регламент от лице с експертни познания в областта на правото и практиките за защита на данните. В частния сектор основните дейности на администратора се отнасят до неговите първични дейности, а не до обработването на лични данни като вторични дейности. Необходимото ниво на експертни познания следва да се определя по-специално в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за личните данни, обработвани от администратора или обработващия лични данни. Тези служители по защита на данните, независимо от това дали са служители на администратора, следва да бъдат в състояние да изпълняват своите задължения и задачи независимо.

(98) Сдруженията или други структури, представляващи категории администратори или обработващи лични данни, следва да се насърчават да изготвят кодекси за поведение, в рамките на настоящия регламент, за да се улесни ефективното прилагане на настоящия регламент, като се вземат предвид особеностите на обработването на данни в определени сектори и специфичните потребности на микропредприятията и малките и средните предприятия. По-специално в тези кодекси на поведение може да се установят параметрите на задълженията на администраторите и обработващите лични данни, като се вземе предвид рискът, който е вероятно да произтече от обработването на данни за правата и свободите на физическите лица.

(99) Когато се изготвя, изменя или допълва кодекс на поведение, сдруженията и другите структури, представляващи категории администратори или обработващи лични данни, следва да се консултират със съответните заинтересовани страни, включително субектите на данни, когато това е осъществимо, и да вземат под внимание становищата, изразени писмено и устно в рамките на тези консултации.

(100) За да се повишат прозрачността и съответствието с настоящия регламент, следва да се насърчава създаването на механизми за сертифициране, както и на печати и маркировки за защита на данните, които позволяват на субектите на данни бързо да оценяват нивото на защита на данните на съответните продукти и услуги.

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

(102) Настоящият регламент не засяга разпоредбите на международните споразумения, сключени между Съюза и трети държави, с които се урежда предаването на лични данни, включително подходящите гаранции за субектите на данни. Държавите членки могат да сключват международни споразумения, които включват предаването на лични данни на трети държави или международни организации, доколкото тези споразумения не засягат настоящия регламент или други разпоредби на правото на Съюза и доколкото включват подходящо ниво на защита на основните права на субектите на данни.

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

(104) В съответствие с основните ценности, въз основа на които е създаден Съюзът, по-специално защитата на правата на човека, в оценката си на третата държава или на територия или на конкретен сектор в третата държава, Комисията следва да вземе предвид как се зачитат в конкретната трета държава принципите на правовата държава, достъпът до правосъдие и международните норми и стандарти за правата на човека, както и нейното общо и секторно право, включително законодателството ѝ в областта на обществената сигурност, отбраната и националната сигурност, а също и обществения ред и наказателното право. При приемането на решение относно адекватното ниво на защита за територия или конкретен сектор в трета държава, следва да се вземат предвид ясни и обективни критерии, като например специфични дейности по обработване и обхватът на приложимите правни стандарти и на действащото законодателство в третата държава. Третата държава следва да предостави гаранции, които осигуряват адекватно ниво на защита, което по същество е равностойно на нивото, гарантирано в рамките на Съюза, по-специално когато личните данни се обработват в един или няколко конкретни сектора. Третата държава следва по-специално да осигури ефективен независим надзор в областта на защитата на данните и да предвиди механизми за

сътрудничество с органи по защита на данните на държавите членки, а на субектите на данните следва да бъдат предоставени действителни и приложими права и ефективни средства за административна и съдебна защита.

(105) Освен международните ангажименти, които третата държава или международната организация е поела, Комисията следва да вземе предвид задълженията, произтичащи от участието на третата държава или международната организация в многостранни или регионални системи, по-специално по отношение на защитата на личните данни, както и изпълнението на тези задължения. По-специално следва да се вземе предвид присъединяването на третата държава към Конвенцията на Съвета на Европа от 28 януари 1981 г. за защита на лицата при автоматизираната обработка на лични данни и допълнителния протокол към нея. Комисията следва да провежда консултации с Комитета при оценяването на нивото на защита в трети държави или международни организации.

(106) Комисията следва да наблюдава изпълнението на решенията относно нивото на защита в дадена трета държава, територия или конкретен сектор в трета държава, или в международна организация, и да наблюдава изпълнението на решения, приети въз основа на **член 25, параграф 6 или член 26, параграф 4 от Директива 95/46/ЕО**. В решенията си относно адекватното ниво на защита Комисията следва да предвиди механизъм за периодичен преглед на тяхното изпълнение. Този периодичен преглед следва да се извършва в консултация с въпросната трета държава или международна организация и да отчита всички съответни развития в третата държава или международната организация. За целите на наблюдението и извършването на периодичните прегледи Комисията следва да вземе предвид становищата и констатациите на Европейския парламент и на Съвета, както и на други релевантни органи и източници. Комисията следва да направи оценка в рамките на разумен срок на изпълнението на посочените решения и да докладва на Европейския парламент и на Съвета за всякакви отнасящи се до тази оценка констатации на Комитета по смисъла на **Регламент (ЕС) № 182/2011 на Европейския парламент и Съвета**(**12**), съгласно установеното в настоящия регламент.

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

(108) При липсата на решение относно адекватното ниво на защита администраторът или обработващият лични данни следва да предприеме мерки, за да компенсира липсата на защита на данни в дадена трета държава чрез подходящи гаранции за субекта на данните. Такива подходящи гаранции може да се състоят в използването на задължителни фирмени правила, стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от надзорен орган, или договорни клаузи, разрешени от надзорен орган. Тези гаранции следва да осигуряват спазването на изискванията относно защитата на данните и на правата на субектите на данни, подходящи при обработване в рамките на Съюза, включително наличието на приложими права на субектите на данни и на ефективни средства за правна защита, включително с цел

получаване на ефективна административна или съдебна защита и предявяване на искове за обезщетение в Съюза или в трета държава. Те следва да се отнасят по-специално до спазването на общите принципи, свързани с обработването на лични данни, и до принципите за защита на данните на етапа на изготвяне и по подразбиране. Данни може да се предават и от публични органи или организации 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 приложими и действителни права за субектите на данни. Следва да се получи разрешение от компетентния надзорен орган, когато гаранциите са предвидени в административни договорености, които нямат задължителен характер.

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

(110) Дадена група предприятия или група дружества, участващи в съвместна стопанска дейност, следва да може да използва одобрени задължителни фирмени правила за своите международни предавания на данни от Съюза до организации в същата група предприятия или група дружества, участващи в съвместна стопанска дейност, при условие че такива фирмени правила включват всички основни принципи и приложими права, за да се осигурят подходящи гаранции за предаването или категориите предавания на лични данни.

(111) Следва да се предвиди възможността 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 правото на държава членка, 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 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.

(112) Тези дерогации следва да се прилагат по-специално за предаванията на данни, които се изискват и са необходими по важни причини от обществен интерес, например при международен обмен на данни между органи по защита на конкуренцията, данъчни или митнически власти, органи за финансов надзор, между 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 или правото на държава членка може, по важни причини от обществен интерес, изрично да определи ограничения за предаването на специални категории от данни на трета държава или международна организация. Държавите членки следва да съобщават тези разпоредби на Комисията. 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.

(113) Предаване на данни, което може да се окачествти като неповтарящо се и засягащо само ограничен брой субекти на данни, също може да бъде възможно за целите на неоспоримите законни интереси на администратора, когато пред тези интереси нямат преимущество интересите или правата и свободите на субекта на данни и когато администраторът е оценил всички обстоятелства около предаването на данните. Администраторът следва да обръща специално внимание на естеството на личните данни, целта и продължителността на предлаганата операция или операции по обработването им, както и на положението в държавата на произход, третата държава и държавата на крайното местоназначение на данните и следва да осигури подходящи гаранции за защита на основните права и свободи на физическите лица при обработването на техните лични данни. Такова предаване на данни следва да бъде възможно само в остатъчни случаи, при които не е приложимо нито едно от останалите основания за предаване. За целите на научни или исторически изследвания или за статистически цели следва да се вземат предвид основателните очаквания на обществото за повишаване на познанието. Администраторът следва да уведомява надзорния орган и субекта на данните за предаването на данни.

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

(115) Някои трети държави приемат закони, подзаконови и други правни актове, които имат за цел пряко да регулират дейностите по обработване на данни на физически и юридически лица под юрисдикцията на държавите членки. 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, например договор за правна взаимопомощ, което е в сила между третата държава, отправила искането, и Съюза или негова държава членка. 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. Предаванията на данни следва да са разрешени 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 основание от обществен интерес, признато в правото на Съюза или в правото на държава членка, на

което е подчинен администраторът.

(116) Трансграничното движение на лични данни извън Съюза може да увеличи риска физическите лица да не могат да упражнят правата на защита на данните, по-специално да се защитят срещу неправомерна употреба или разкриване на тези данни. В същото време надзорните органи могат да бъдат изправени пред невъзможността да разглеждат жалби или да провеждат разследвания, свързани с дейности, извършвани извън техните граници. Техните усилия за сътрудничество в трансграничния контекст могат да бъдат възпрепятствани и от недостатъчни правомощия за предотвратяване или защита, различаващи се правни режими, както и от практически пречки като ограничения на ресурсите. Ето защо е необходимо да се насърчава по-тясното сътрудничество между надзорните органи по защита на данните, за им се помогне да обменят информация и да извършват разследвания съвместно със своите международни партньори. За целите на разработването на механизми за международно сътрудничество, улесняващи и осигуряващи международна взаимопомощ при прилагането на законодателство за защита на личните данни, Комисията и надзорните органи следва да обменят информация и да си сътрудничат в дейностите по упражняването на техните правомощия с компетентните органи в трети държави на реципрочна основа и в съответствие с настоящия регламент.

(117) Създаването в държавите членки на надзорни органи, оправомощени да изпълняват задачите и упражняват своите правомощия при пълна независимост, е първостепенен елемент от защитата на физическите лица във връзка с обработването на личните им данни. Държавите членки следва да могат да създават повече от един надзорен орган, за да отговаря на тяхната конституционна, организационна и административна структура.

(118) Независимостта на надзорните органи не следва да означава, че те не могат да бъдат подлагани на механизъм за контрол или наблюдение по отношение на финансовите им разходи, нито на съдебен контрол.

(119) Когато държава членка създаде няколко надзорни органа, тя следва да установи със закон механизми за гарантиране на ефективното участие на тези надзорни органи в механизма за съгласуваност. Тази държава членка следва по-специално да определи надзорния орган, който функционира като единна точка за контакт, за да гарантира ефективното участие на тези органи в механизма, както и бързото и безпрепятствено сътрудничество с други надзорни органи, Комитета и Комисията.

(120) Всеки надзорен орган следва да получи финансови и човешки ресурси, помещения и инфраструктура, необходими за ефективното изпълнение на неговите задачи, включително задачите по линия на взаимопомощта и сътрудничеството с други надзорни органи навсякъде в Съюза. Всеки надзорен орган следва да има отделен публичен годишен бюджет, който може да е част от общия държавен или национален бюджет.

(121) Общите условия за члена или членовете на надзорния орган следва да бъдат определени със закон във всяка държава членка, и по-специално да осигурят тези членове да се назначават посредством прозрачна процедура от парламента, правителството или от държавния глава на държавата членка въз основа на предложение на правителството или член на правителството или парламента или камара на парламента, или от независим орган, оправомощен съгласно правото на държавата членка. За да се гарантира независимостта на надзорния орган, членът или членовете следва да действат добросъвестно, да се въздържат от всякакви несъвместими със задълженията им

действия и по време на своя мандат да не се ангажират с никакви несъвместими функции, независимо дали срещу възнаграждение или безвъзмездно. Надзорният орган следва да разполага със собствен персонал, подбран от надзорния орган или от независим орган, установен съгласно правото на държава членка, който да е поставен под изключителното ръководство на члена или членовете на надзорния орган.

(122) Всеки надзорен орган следва да бъде компетентен на територията на своята държава членка да упражнява правомощията и изпълнява задачите, възложени му в съответствие с настоящия регламент. Това следва да обхваща по-специално обработването в контекста на дейностите на място на установяване на администратора или обработващия лични данни на територията на неговата държава членка, обработването на лични данни, извършвано от публични органи или частни структури, действащи в обществен интерес, обработване, което засяга субекти на данни на неговата територия, или обработване, извършвано от администратор или обработващ лични данни, който не е установен в Съюза, когато субектите на данни, към които това обработване е насочено, са с местопребиваване на негова територия. Това следва да включва разглеждане на жалби, внесени от субекти на данни, водене на разследвания за прилагането на настоящия регламент и повишаване на обществената осведоменост за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни.

(123) Надзорните органи следва да наблюдават прилагането на разпоредбите съгласно настоящия регламент и да допринасят за неговото последователно 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. За тази цел надзорните органи следва да сътрудничат помежду си и с Комисията, без да е необходимо споразумение между държавите членки относно предоставянето на взаимопомощ или относно такова сътрудничество.

(124) Когато обработването на лични данни се извършва в контекста на дейностите на място на установяване на администратор или обработващ лични данни в Съюза, а администраторът или обработващият лични данни е установен в повече от една държава членка, или когато обработване, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка, надзорният орган на основното място на установяване на администратора или обработващия лични данни или на единственото място на установяване на администратора или обработващия лични данни следва да функционира като водещ орган. Той следва да си сътрудничи с други засегнати органи, тъй като администраторът или обработващият лични данни има място на установяване на територията на тяхната държава членка, тъй като субекти на данни с местопребиваване на тяхната територия са съществено засегнати или тъй като до тях е била подадена жалба. Също когато субект на данни, който не е с местопребиваване в тази държава членка, е подал жалба, надзорният орган, до който е подадена такава жалба, следва също да се счита за засегнат надзорен орган. В рамките на задачите му да дава насоки по всякакви въпроси, отнасящи се до прилагането на настоящия регламент, Комитетът следва да може да дава насоки по-специално относно критериите, които да се вземат предвид, за да се установи дали въпросното обработване засяга съществено субекти на данни в повече от една държава членка и относно това какво представлява едно относимо и обосновано възражение.

(125) Водещият орган следва да е компетентен да приема решения със задължителен характер относно мерките за прилагане на правомощията, които са му предоставени по силата на настоящия регламент. В качеството си на водещ орган надзорният орган следва да осигурява активно

участие и да координира засегнатите надзорни органи в процеса на вземане на решения.Когато решението е за пълно или частично отхвърляне на жалба от субект на данни, това решение следва да се приема от надзорния орган, до който е подадена жалбата.

(126) Решението следва да се съгласува между водещия надзорен орган и засегнатите надзорни органи и следва да е насочено към основното или единственото място на установяване на администратора или обработващия лични данни и да бъде със задължителен характер за администратора или обработващия лични данни. Администраторът или обработващият лични данни следва да вземе необходимите мерки, за да осигури спазването на настоящия регламент и изпълнението на решението, за което водещият надзорен орган е уведомил основното място на установяване на администратора или обработващия лични данни по отношение на дейностите по обработване в Съюза.

(127) Всеки надзорен орган, който не функционира като водещ надзорен орган, следва да бъде компетентен да разглежда случаи на местно равнище, когато администраторът или обработващият лични данни е установен в повече от една държава членка, но предметът на конкретното обработване засяга единствено обработването, извършвано в една държава членка, и включва единствено субекти на данни в тази единствена държава членка, например когато предметът се отнася до обработването на лични данни на наети лица в контекста на специфично трудово правоотношение в държава членка. В такива случаи надзорният орган следва без отлагане да информира за случая водещия надзорен орган. След като бъде информиран, водещият надзорен орган следва да реши дали ще разгледа случая съгласно разпоредбата относно сътрудничеството между водещия надзорен орган и другите засегнати надзорни органи („обслужване на едно гише“) или информиралият го надзорен орган следва да разгледа случая на местно равнище. Когато взема това решение, водещият надзорен орган следва да отчете дали администраторът или обработващият лични данни е установен в държавата членка на надзорния орган, който го е информирал, за да се гарантира ефективно изпълнение на решението спрямо администратора или обработващия лични данни. Когато водещият надзорен орган реши да разгледа случая, информиралият го надзорен орган следва да има възможността да представи проект за решение, което водещият надзорен орган следва да отчита в максимална степен при изготвянето на своя проект за решение в рамките на посочения механизъм „обслужване на едно гише“.

(128) Правилата за водещия надзорен орган и механизма „обслужване на едно гише“ не следва да се прилагат, когато обработването се извършва от публични органи или от частни структури в обществен интерес. В такива случаи единственият надзорен орган, който е компетентен да упражнява правомощията, предоставени му съгласно настоящия регламент, следва да бъде надзорният орган на държавата членка, в която е установен публичният орган или частната структура.

(129) За да се гарантира последователно наблюдение и прилагане на настоящия регламент навсякъде в Съюза, надзорните органи следва да имат еднакви задачи и ефективни правомощия във всяка държава членка, 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, и без да се засягат правомощията на прокуратурата съгласно правото на държавата членка — правомощието да довеждат нарушения на настоящия регламент до знанието на съдебните органи и да встъпват в съдебни производства. Тези правомощия следва да включват и правомощието за налагане на временно или окончателно ограничаване, включително забрана, на обработването на данни. Държавите членки могат да посочат други конкретни задачи,

свързани със защитата на лични данни съгласно настоящия регламент. Надзорните органи следва да упражняват правомощията си в съответствие с подходящите процедурни гаранции, определени в правото на Съюза и правото на държава членка, независимо, справедливо и в разумен срок. По-специално всяка мярка следва да бъде подходяща, необходима и пропорционална с оглед на осигуряването на съответствие с настоящия регламент, като се отчитат обстоятелствата при всеки конкретен случай, зачита се правото на всяко лице да бъде изслушано преди да бъде взета каквато и да е конкретна мярка, която би го засегнала неблагоприятно, и се избягват излишни разходи и прекалени неудобства за засегнатите лица. Правомощията за разследване по отношение на достъпа до помещения следва да се упражняват в съответствие със специфичните изисквания на процесуалното право на държавите членки, като например изискването за получаване на предварително съдебно разрешение. Всяка мярка със задължителен характер на надзорен орган следва да бъде в писмен вид, да бъде ясна и недвусмислена, да посочва надзорния орган, който е издал мярката, датата на издаване на мярката, да е подписана от ръководителя или член на надзорния орган, упълномощен от него, да посочва основанията за мярката и да се позовава на правото на ефективни правни средства за защита. Това не следва да възпрепятства поставянето на допълнителни изисквания съгласно процесуалното право на държавите членки. Приемането на такова решение със задължителен характер предполага, че то може да подлежи на съдебен контрол в държавата членка на надзорния орган, приел решението.

(130) Когато надзорният орган, до когото е подадена жалбата, не е водещият надзорен орган, водещият надзорен орган следва да работи в тясно сътрудничество с надзорния орган, до когото е подадена жалбата, в съответствие с разпоредбите за сътрудничество и съгласуваност, установени в настоящия регламент. В такива случаи, когато взема мерки, предназначени да породят правни последици, включително налагане на административни наказания „глоба“ или „имуществена санкция“, водещият надзорен орган следва да отчита във възможно най-голяма степен становището на надзорния орган, до когото е подадена жалбата и който следва да запази компетентността за провеждане на разследване на територията на собствената си държава членка, като си сътрудничи с компетентния надзорен орган.

(131) Когато друг надзорен орган следва да функционира като водещ надзорен орган за дейностите по обработване на администратора или обработващия лични данни, но конкретният предмет на жалбата или възможното нарушение засяга единствено дейностите по обработване на администратора или обработващия лични данни в държавата членка, в която е подадена жалбата или е установено възможното нарушение, и предметът не засяга съществено или няма вероятност да засегне съществено субекти на данни в други държави членки, надзорният орган, който е получил жалба, е установил или е бил информиран по друг начин за ситуации, които водят до възможни нарушения на настоящия регламент, следва да се стреми към уреждане на спора по взаимно съгласие с администратора, а ако този опит се окаже неуспешен, да упражни целия си набор от правомощия. Това следва да включва специфично обработване, извършвано на територията на държавата членка на надзорния орган или по отношение на субекти на данни на територията на тази държава членка; обработване, което се извършва в контекста на предлагането на стоки или услуги, специално предназначени за субекти на данни на територията на държавата членка на надзорния орган; или обработване, което трябва да се прецени, като се вземат предвид съответните правни задължения съгласно правото на държавата членка.

(132) Дейностите на надзорния орган за повишаване на обществената осведоменост следва да включват специални мерки, насочени към администраторите и обработващите лични данни, в това число микропредприятията и малките и средните предприятия, както и физическите лица, особено в

образователен контекст.

(133) Надзорните органи следва да си сътрудничат при изпълнението на своите задачи и взаимно да се подпомагат, за да се гарантира съгласуваното прилагане и изпълнение на настоящия регламент в рамките на вътрешния пазар. Надзорен орган, който е поискал взаимопомощ, може да приеме временна мярка, ако не е получил отговор на искането за взаимопомощ в рамките на един месец от получаването му от другия надзорен орган.

(134) Всеки надзорен орган следва да участва в съвместни операции с други надзорни органи, когато е целесъобразно. Надзорният орган, до който е отправено искането, следва да е длъжен да отговори в определен срок на искането.

(135) За да се гарантира последователното прилагане на настоящия регламент навсякъде в Съюза, следва да се създаде механизъм за съгласуваност за осъществяване на сътрудничество между надзорните органи. Този механизъм следва по-специално да се прилага, когато даден надзорен орган възнамерява да приеме мярка, целяща да породи правни последици по отношение на операции по обработване на данни, които засягат съществено значителен брой субекти на данни в няколко държави членки. Той следва да се прилага също, когато засегнатият надзорен орган или Комисията поиска този въпрос да бъде разгледан чрез механизма за съгласуваност. Този механизъм следва да действа, без да се засягат мерките, които Комисията може да предприеме в изпълнение на своите правомощия съгласно Договорите.

(136) При прилагането на механизма за съгласуваност Комитетът следва да излезе със становище в рамките на определен срок, ако такова решение бъде взето с мнозинство от неговите членове или ако това бъде поискано от засегнат надзорен орган или от Комисията. На Комитета следва също да бъде делегирано правомощието да приема решения със задължителен характер в случай на спорове между надзорни органи. За целта той следва по принцип да взема с мнозинство от две трети от своите членове решения със задължителен характер в точно определени случаи, когато има противоречиви становища сред надзорните органи, по-специално в механизма за сътрудничество, между водещия надзорен орган и засегнатите надзорни органи по съществото на спора, по-специално дали е налице нарушение на настоящия регламент.

(137) Възможно е да има спешна необходимост от действия за защита на правата и свободите на субекти на данни, по-специално когато съществува опасност прилагането на право на субект на данни да бъде значително възпрепятствано. Поради това даден надзорен орган следва да може да приема надлежно обосновани временни мерки на своя територия с определен срок на действие, който не следва да надвишава три месеца.

(138) Прилагането на такъв механизъм следва да бъде условие за законосъобразността на мярка, целяща да породи правни последици, издадена от надзорния орган в случаите, когато прилагането му е задължително. В други случаи с трансгранично значение следва да се прилага механизмът за сътрудничество между водещия надзорен орган и засегнатите надзорни органи и могат да се осъществяват взаимопомощ и съвместни операции между засегнатите надзорни органи на двустранна или многостранна основа, без да се задейства механизмът за съгласуваност.

(139) За да се насърчи последователното прилагане на настоящия регламент, Комитетът следва да бъде създаден като независим орган на Съюза. За да изпълнява целите си, Комитетът следва да притежава правосубектност. Комитетът следва да се представлява от своя председател. Той

следва да замени Работната група за защита на физическите лица при обработването на лични данни, създадена с **Директива 95/46/ЕО**. Той следва да е съставен от ръководителите на надзорните органи на всяка държава членка и на Европейския надзорен орган по защита на данните или съответните им представители. Комисията следва да участва в дейностите на Комитета без право на глас, а Европейският надзорен орган по защита на данните следва да има специално право на глас. Комитетът следва да допринася за съгласуваното прилагане на настоящия регламент навсякъде в Съюза, включително като съветва Комисията, по-специално относно нивото на защита в трети държави или международни организации, и като насърчава сътрудничеството на надзорните органи навсякъде в Съюза. Комитетът следва да действа независимо при изпълнението на задачите си.

(140) Комитетът следва да бъде подпомаган от секретариат, осигурен от Европейския надзорен орган по защита на данните. Служителите на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачите, възложени на Комитета с настоящия регламент, следва да ги изпълняват изключително под ръководството на председателя на Комитета и да се отчитат пред него.

(141) Всеки субект на данни следва да има право да подаде жалба до един надзорен орган, по-специално в държавата членка на обичайно си местопребиваване, както и право на ефективни правни средства за защита в съответствие с **член 47 от Хартата**, ако счита, че правата му по настоящия регламент са нарушени или ако надзорният орган не предприема действия по подадена жалба, изцяло или частично отхвърля или оставя без разглеждане жалба или не предприема действия, когато такива са необходими, за да се защитят правата на субекта на данни. Разследването въз основа на жалби следва да се извършва под съдебен контрол и в целесъобразна за конкретния случай степен. Надзорният орган следва да информира субекта на данните за напредъка и резултата от жалбата в разумен срок. Ако случаят изисква допълнително разследване или координиране с друг надзорен орган, на субекта на данните следва да бъде предоставена междинна информация. За да се улесни подаването на жалбите, всеки надзорен орган 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.

(142) 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 държава членка, има уставни цели, които са от обществен интерес и работи в областта на защитата на личните данни, да подаде жалба от негово име до надзорен орган, да упражни правото на средства за съдебна защита от името на субектите на данни или ако то е предвидено в правото на държавата членка да упражни правото на обезщетение от името на субектите на данни. Държавите членки могат да предвидят такава структура, организация или сдружение да има право да подаде в тази държава членка жалба, независимо от възложения от субекта на данни мандат, и право на ефективни правни средства за защита, когато има основания да смята, че правата на субект на данни са били нарушени в резултат на обработване на лични данни, което нарушава настоящия регламент. Тази структура, организация или сдружение не може да има право да претендира за обезщетение от името на субекта на данни, независимо от възложения от субекта на данни мандат.

(143) Всяко физическо или юридическо лице има правото да внася иск за отмяна на решения на Комитета пред Съда при условията, предвидени в **член 263 от ДФЕС**. Като адресати на тези решения, засегнатите надзорни органи, които желаят да ги оспорят, трябва да внесат иск в срок от два месеца от датата, на която са били уведомени за тях, в съответствие с **член 263 от ДФЕС**. Когато

решенията на Комитета засягат пряко и лично администратора, обработващия личните данни или жалбоподателя, те могат да внесат иск за отмяна на тези решения в срок от два месеца от публикуването им на уебсайта на Комитета, в съответствие с **член 263 от ДФЕС**. Без да се засяга това право по **член 263 от ДФЕС**, всяко физическо или юридическо лице има право на ефективни правни средства за защита пред компетентен национален съд срещу решение на надзорен орган, което има правни последици за това лице. Подобно решение се отнася по-специално за упражняването на правомощията за разследване, даване на разрешение и корективните правомощия на надзорния орган или оставянето без разглеждане или отхвърлянето на жалби. Същевременно правото на ефективни правни средства на защита не обхваща мерки, взети от надзорните органи, които не са с правно задължителен характер, като становища или консултации, предоставени от надзорния орган. Производствата срещу надзорния орган следва да се завеждат пред съдилищата на държавата членка, в която е установен надзорният орган, и следва да се водят в съответствие с процесуалното право на тази държава членка. Тези съдилища следва да разполагат с пълна компетентност, която следва да включва компетентност за разглеждане на всички фактически и правни въпроси, свързани с разглеждания спор.

Когато дадена жалба е била отхвърлена или оставена без разглеждане от надзорен орган, жалбоподателят може да заведе дело в съдилищата на същата държава членка. По отношение на средствата за правна защита, свързани с прилагането на настоящия регламент, националните съдилища, които считат, че е необходимо решение по въпроса, за да им даде възможност да се произнесат с решение, могат или — в случая, предвиден в **член 267 от ДФЕС** — трябва да поискат от Съда преюдициално заключение относно тълкуването на правото на Съюза, включително на настоящия регламент. Освен това в случай на оспорване пред национален съд на решение на надзорен орган, изпълняващ решение на Комитета, и ако валидността на това решение е под въпрос, този национален съд няма правомощието да обявява решението на Комитета за невалидно, а трябва да отнесе въпроса за валидността до Съда в съответствие с **член 267 от ДФЕС**, съгласно тълкуването на Съда, когато счете решението за невалидно. Национален съд обаче не може да отнесе въпрос за валидността на решението на Комитета по искане на физическо или юридическо лице, което е имало възможността да внесе иск за отмяна на това решение, по-специално ако е било пряко и лично засегнато от това решение, но не го е направило в срока, определен в **член 263 от ДФЕС**.

(144) Когато сезиран съд, в който е заведено съдебно производство срещу решение на надзорен орган, има основания да счита, че пред компетентен съд в друга държава членка е образувано производство, засягащо същото обработване, напр. свързано със същия въпрос по отношение на обработване от същия администратор или обработващ личните данни, или същото основание, той следва да установи контакт с този съд, за да потвърди наличието на такова свързано производство. Когато свързано производство е висящо пред съд на друга държава членка, всеки съд, освен първия сезиран съд, може да спре производството или може, по молба на една от страните, да се откаже от компетентност в полза на първия сезиран съд, при условие че този съд е компетентен по отношение на въпросното производство и правото му допуска съединяване на такива свързани производства. Производствата се смятат за свързани, когато те се намират в такава тясна връзка помежду си, че е целесъобразно да бъдат разгледани и решени заедно, за да се избегне рискът от противоречащи си съдебни решения, постановени в отделни производства.

(145) При производства срещу администратор или обработващ лични данни ищецът следва да има избор да заведе дело пред съдилищата на държавите членки, в които администраторът или обработващият лични данни е установен, или по местопребиваването на субекта на данни, освен ако

администраторът не е публичен орган на държава членка, който действа в изпълнение на своите публични правомощия.

(146) Администраторът или обработващият лични данни следва да обезщетят всички вреди, които дадено лице може да претърпи в резултат на обработване на данни, което нарушава настоящия регламент. Администраторът или обработващият лични данни следва да бъде освободен от отговорност, ако докаже, че по никакъв начин не е отговорен за вредите. Понятието „вреда“ следва да се тълкува в по-широк смисъл в контекста на съдебната практика на Съда по начин, който отразява напълно целите на настоящия регламент. Това не засяга евентуални искове за вреди, произтичащи от нарушаване на други правила на правото на Съюза или правото на държава членка. Обработване на данни, което нарушава настоящия регламент, включва и обработване, което нарушава делегираните актове и актовете за изпълнение, приети в съответствие с настоящия регламент, и правото на държава членка, конкретизиращо правилата на настоящия регламент. Субектите на данни следва да получат пълно и действително обезщетение за претърпените от тях вреди. Когато администраторите или обработващите лични данни участват в едно и също обработване на данни, всеки администратор или обработващ лични данни следва да носи отговорност за цялата вреда. Когато обаче те са обединени в едно съдебно производство, в съответствие с правото на държава членка, обезщетението може да се разпределели съобразно отговорността на всеки администратор или обработващ лични данни за причинената от обработването вреда, при условие че на претърпелия вреда субект на данни бъде осигурено пълно и действително обезщетение. Всеки администратор или обработващ лични данни, който е изплатил пълно обезщетение, може впоследствие да предяви регресен иск срещу другите администратори или обработващи лични данни, участвали в същото обработване.

(147) Когато в настоящия регламент се съдържат специфични правила относно компетентността, по-специално по отношение на производствата за търсене на защита по съдебен ред, включително на обезщетение, срещу администратор или обработващ лични данни, общите правила относно компетентността като правилата, предвидени в **Регламент (ЕС) № 1215/2012 на Европейския парламент и на Съвета**(**13**), не следва да засягат прилагането на тези специфични правила.

(148) За да се укрепи прилагането на правилата на настоящия регламент, освен или вместо подходящи мерки, наложени от надзорния орган съгласно настоящия регламент, при нарушение на регламента следва да се налагат санкции, включително административни наказания „глоба“ или „имуществена санкция“. При леки нарушения или ако глобата, която може да бъде наложена, представлява несъразмерна тежест за физическо лице, вместо глоба може да бъде отсъдено порицание. Следва обаче да се отдаде надлежно внимание на естеството, тежестта и продължителността на нарушението, умишления характер на нарушението, действията за смекчаване на последиците от претърпените вреди, степента на отговорност или евентуални предишни нарушения от подобен характер, начина, по който нарушението е станало известно на надзорния орган, спазването на мерките, наложени на администратора или на обработващия лични данни, придържането към кодекс на поведение и всякакви други утежняващи или смекчаващи фактори. Налагането на санкции, включително административни наказания „глоба“ или „имуществена санкция“, следва да подлежи на подходящи процедурни мерки за защита в съответствие с общите принципи на правото на Съюза и **Хартата**, включително ефективна съдебна защита и справедлив съдебен процес.

(149) Държавите членки следва да могат да установят правила относно наказателна

отговорност за нарушения на настоящия регламент, включително за нарушения на националните правила, приети по силата и в рамките на настоящия регламент. Тези наказания могат да предвиждат отнемане на облагите, получени в резултат на нарушаване на настоящия регламент. Налагането на наказания за нарушения на тези национални правила и на административни наказания обаче не следва да води до нарушаване на принципа ne bis in idem съгласно тълкуването на Съда.

(150) С цел да се засилят и хармонизират административните наказания за нарушения на настоящия регламент, всеки надзорен орган следва да има правомощието да налага административни наказания „глоба“ или „имуществена санкция“. В настоящия регламент следва да се посочат нарушенията и максималният размер и критериите за определяне на съответните административни наказания „глоба“ или „имуществена санкция“, които следва да се определят от компетентния надзорен орган във всеки отделен случай, като се вземат предвид всички обстоятелства, свързани с конкретната ситуация, по-специално при надлежно отчитане на естеството, тежестта и продължителността на нарушението и на последиците от него, както и на мерките, предприети, за да се гарантира спазване на задълженията по настоящия регламент и за да се предотвратят или смекчат последиците от нарушението. Когато имуществената санкция се налага на предприятие, понятието „предприятие“ следва да се разбира като предприятие в съответствие с **членове 101 и 102 от ДФЕС** за тези цели. При налагане на административни наказания „глоба“ и „имуществена санкция“ на лица, които не са предприятие, надзорният орган следва да има предвид общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето, за да определи подходящия размер на глобата. Механизмът за съгласуваност може да се използва също за утвърждаването на съгласувано прилагане на административните наказания „глоба“ или „имуществена санкция“. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни наказания „глоба“ или „имуществена санкция“. Налагането на административно наказание „глоба“ или „имуществена санкция“ или отправянето на предупреждение не засяга упражняването на други правомощия на надзорните органи или прилагането на други санкции по настоящия регламент.

(151) Правните системи на Дания и Естония не позволяват налагането на административните наказания „глоба“ или „имуществена санкция“, посочени в настоящия регламент. Правилата относно административните наказания „глоба“ или „имуществена санкция“ могат да се прилагат по такъв начин, че в Дания глобата или имуществената санкция да се налага от компетентни национални съдилища като наказание, а в Естония глобата или имуществената санкция да се налага от надзорния орган в рамките на процедура за нарушение, при условие че това прилагане на правилата в посочените държави членки има ефект, равностоен на административни наказания „глоба“ или „имуществена санкция“, налагани от надзорни органи. Поради това компетентните национални съдилища следва да вземат под внимание препоръката на надзорния орган, инициращ глобата или имуществената санкция. Във всички случаи наложените глоби или имуществени санкции следва да са ефективни, пропорционални и възпиращи.

(152) Когато административните наказания не са хармонизирани в настоящия регламент или при необходимост в други случаи, като например при сериозни нарушения на настоящия регламент, държавите членки следва да прилагат система, която предвижда ефективни, съразмерни и възпиращи санкции. Естеството на тези санкции, наказателни или административни, следва да бъде определено съгласно правото на държавата членка.

(153) Правото на държавите членки следва да съвместява разпоредбите, уреждащи свободата на изразяване на мнение и свободата на информация, включително за журналистически, академични,

художествени или литературни цели, и правото на защита на личните данни по настоящия регламент. Обработването на лични данни единствено за журналистически цели или за академично, художествено или литературно изразяване следва да подлежи на дерогации или освобождаване от изискванията на някои разпоредби на настоящия регламент, за да се съчетае при необходимост правото на защита на личните данни с правото на свобода на изразяване на мнение и свобода на информация, заложени в **член 11 от Хартата**. Това следва да се прилага по-специално по отношение на обработването на лични данни в аудио-визуалната област и в новинарските архиви и библиотеките с печатни издания. Поради това държавите членки следва да приемат законодателни мерки, с които да определят освобождаванията и дерогациите, необходими за постигането на баланс между тези основни права. Държавите членки следва да приемат такива освобождавания и дерогации от общите принципи, правата на субекта на данните, администратора и обработващия лични данни, предаването на лични данни на трети държави или международни организации, независимостта на надзорните органи, сътрудничеството и съгласуваността и специалните случаи на обработване на данни. Когато тези освобождавания или дерогации се различават в отделните държави членки, следва да се прилага правото на държавата членка, на което се подчинява администраторът на лични данни. За да се вземе предвид важността на правото на свобода на изразяване на мнение във всяко демократично общество, е необходимо свързаните с тази свобода понятия, като журналистиката например, да се тълкуват широко.

(154) Настоящият регламент дава възможност при прилагането му да се взема предвид принципът на публичен достъп до официални документи. Публичният достъп до официални документи може да се счита, че е в обществен интерес. Личните данни в документи, съхранявани от публичен орган или публична структура, следва да могат да бъдат разкрити от този орган или структура, ако правото на Съюза или правото на държава членка, чийто субект е публичният орган или публичната структура, предвижда това. Такова законодателство следва да съвместява публичния достъп до официални документи и повторната употреба на информацията в обществения сектор с правото на защита на личните данни и поради това може да осигури необходимото съгласуване с правото на защита на личните данни съгласно настоящия регламент. Във връзка с това позоваването на публични органи и структури следва да включва всички органи или други структури, обхванати от правото на държавата членка относно публичния достъп до документи. **Директива 2003/98/ЕО на Европейския парламент и на Съвета**(**14**) оставя непроменено и по никакъв начин не засяга нивото на защита на физическите лица що се отнася до обработката на лични данни съгласно разпоредбите на Съюза и на националното право и по-специално не променя задълженията и правата, установени в настоящия регламент. По-специално, посочената директива не следва да се прилага за документи, достъпът до които е изключен или ограничен по силата на режимите за достъп на основание защита на личните данни, както и за части от документи, достъпни по силата на тези режими и съдържащи лични данни, чиято повторна употреба е определена от правото като несъвместима с правото за защита на физическите лица по отношение на обработката на лични данни.

(155) В правото на държавите членки или в колективните споразумения, включително „трудови споразумения“, могат да се предвиждат специални разпоредби относно обработването на личните данни на наетите лица по трудово или служебно правоотношение, по-специално във връзка с условията, при които личните данни в контекста на трудово или служебно правоотношение могат да бъдат обработвани въз основа на съгласието на наетото лице, за целите на набирането на персонал, изпълнението на трудовия договор, включително изпълнението на задължения, установени със закон или с колективни споразумения, управлението, планирането и организацията на работата, равенството и многообразието на работното място, здравословните и безопасни условия на труд, както и за целите на упражняването и ползването на индивидуална или колективна основа на правата

и облагите от заетостта, а също и за целите на прекратяването на трудовото или служебното правоотношение.

(156) 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, 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). Държавите членки 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. На държавите членки следва да бъде разрешено да предвиждат, при конкретни условия, при прилагане на подходящи гаранции за субектите на данни, спецификации и дерогации по отношение на изискванията за информация и правото на коригиране, на изтриване на лични данни, на това „да бъдеш забравен“, на ограничаване на обработването, на преносимост на данните и на възражение при обработването на лични данни за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели. Въпросните условия и гаранции могат да доведат до въвеждане на конкретни процедури, за да могат субектите на данни да упражнят тези права, ако това е подходящо с оглед на целите на конкретното обработване, както и до въвеждането на технически и организационни мерки, така че да се сведе до минимум обработването на лични данни в съответствие с принципите на пропорционалност и необходимост. Обработването на лични данни за научни цели следва да съответства и на друго приложимо към този въпрос законодателство, например относно клиничните изпитвания.

(157) Чрез съчетаване на информацията от регистрите изследователите могат да придобият нови познания с голяма стойност, относно широко разпространени медицински условия като сърдечносъдовите заболявания, рака, и депресията. Въз основа на регистрите може да се повиши надеждността на резултатите от научните изследвания, тъй като се базират на много по-голяма част от населението. В социалната област научните изследвания въз основа на регистрите дават възможност на изследователите да придобият съществени познания относно дългосрочното взаимодействие на редица социални условия, като безработица и образование, с останалите условия на живот. Резултатите от научните изследвания, получени чрез регистрите, предоставят солидни, качествени познания, които могат да осигурят базата за формулирането и прилагането на основани на знанието политики, да подобрят качеството на живот на много хора, да повишат ефективността на социалните услуги. За улесняване на научноизследователската дейност личните данни могат да бъдат обработвани за целите на научните изследвания при подходящи условия и гаранции, определени от правото на Съюза или правото на държава членка.

(158) Когато се обработват лични данни за целите на архивирането, настоящият регламент следва да се прилага и за този вид обработване, като се има предвид че настоящият регламент следва да не се прилага за починалите лица. Публичните органи или публичните или частни структури, които съхраняват регистри от обществен интерес, следва да бъдат службите, които, съгласно правото на Съюза или правото на държавата членка, имат законово задължение да получават, съхраняват, оценяват, организират, описват, разпространяват и предоставят достъп до регистри с непреходна

стойност в обществен интерес, както и да предоставят информация за тях и да насърчават тяхното поддържане. Освен това на държавите членки следва да се разреши да предвидят по-нататъшното обработване на лични данни за целите на архивирането, например с оглед осигуряването на определена информация, свързана с политическото поведение по време на бивши тоталитарни режими, геноцид, престъпления срещу човечеството, по-специално Холокоста, или военни престъпления.

(159) Когато се обработват лични данни за научноизследователски цели, настоящият регламент следва да се прилага и за този вид обработване. За целите на настоящия регламент обработването на лични данни за научноизследователски цели следва да се тълкува в по-широк смисъл и да включва напр. технологичното развитие и демонстрационни дейности, фундаменталните научни изследвания, приложните научни изследвания и частно финансираните научни изследвания. Освен това следва да се отчита и заложената в **член 179, параграф 1 от ДФЕС** цел за изграждането на европейско научноизследователско пространство. Научноизследователските цели следва да включват и проучвания, провеждани в обществен интерес в областта на общественото здраве. С оглед на особеностите на обработването на лични данни за научноизследователски цели следва да се прилагат специални условия, по-специално по отношение на публикуването или оповестяването по друг начин на лични данни в контекста на научноизследователските цели. Ако резултатите от научно изследване, по-специално в здравната област, породят необходимост от допълнителни мерки в интерес на субекта на данните, във връзка с тези мерки следва да се прилагат общите правила на настоящия регламент.

(160) Когато се обработват лични данни за целите на исторически изследвания, настоящият регламент следва да се прилага и за този вид обработване. Това следва да включва също исторически изследвания и изследвания за генеалогични цели, като се има предвид че настоящият регламент не следва да се прилага за починали лица.

(161) За целите на даване на съгласие за участие в научноизследователска дейност при клинични изпитвания следва да се прилагат съответните разпоредби на **Регламент (ЕС) № 536/2014 на Европейския парламент и на Съвета**(**15**).

(162) Когато се обработват лични данни за статистически цели, настоящият регламент следва да се прилага за този вид обработване. В рамките на настоящия регламент правото на Съюза или правото на държава членка следва да определя съдържанието на статистическите данни, контрола на достъпа, спецификациите за обработването на лични данни за статистически цели и подходящите мерки за гарантиране на правата и свободите на субекта на данните, както и на поверителността на статистическите данни. Статистически цели означава всяка операция по събиране и обработване на лични данни, необходими за статистически изследвания или за изготвяне на статистически резултати. Тези статистически резултати могат впоследствие да бъдат използвани за различни цели, включително за научноизследователски цели. Статистическата цел означава, че резултатът от обработването за статистически цели не съдържа лични данни, а агрегирани данни, и че този резултат или получените лични данни не се използват в подкрепа на мерки или решения, касаещи конкретно физическо лице.

(163) 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, докато националната статистика следва да съответства и на правото на държавата членка. **Регламент (ЕО) № 223/2009 на Европейския парламент и на Съвета**(**16**) конкретизира допълнително изискванията относно поверителността на данните на европейската статистика.

(164) По отношение на правомощията на надзорните органи да получават от администратора или от обработващия лични данни достъп до лични данни и достъп до помещенията им, държавите членки могат, в рамките на настоящия регламент, да приемат със закон конкретни правила, за да гарантират задължението за опазване на професионална тайна или на други равностойни задължения за опазване на тайна, доколкото това е необходимо за съгласуване на правото на защита на личните данни със задължението за опазване на професионална тайна. Това не засяга съществуващите задължения на държавите членки да приемат правила за професионална тайна, когато това се изисква от правото на Съюза.

(165) Настоящият регламент зачита и не засяга статута, от който се ползват църквите и религиозните сдружения или общности в държавите членки съгласно съществуващото конституционно право, както е признат в **член 17 от ДФЕС**.

(166) С цел да бъдат постигнати целите на настоящия регламент, а именно защита на основните права и свободи на физическите лица, и по-специално на тяхното право на защита на личните данни, както и за да се гарантира свободното движение на лични данни в рамките на Съюза, на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с **член 290 от ДФЕС**. По-специално делегирани актове следва да бъдат приемани по отношение на критериите и изискванията за механизмите за сертифициране, предоставянето на информация под формата на стандартизирани икони и процедурите за представяне на тези икони. От особена важност е по време на подготвителната си работа Комисията да проведе подходящи консултации, включително на експертно равнище. При подготовката и изготвянето на делегираните актове Комисията следва да осигури едновременното и своевременно предаване на съответните документи по подходящ начин на Европейския парламент и на Съвета.

(167) За да се гарантират еднакви условия за прилагане на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия, когато това е предвидено в регламента. Тези правомощия следва да бъдат упражнявани в съответствие с **Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г**. В този контекст Комисията следва да обмисли специалните мерки за микропредприятията, малките и средните предприятия.

(168) Процедурата по разглеждане следва да се използва за приемането на актове за изпълнение относно стандартни договорни клаузи между администратори и обработващи лични данни и между самите обработващи лични данни, кодекси на поведение; технически стандарти и механизми за сертифициране; адекватното ниво на защита на данните, осигурявано от дадена трета държава, територия или конкретен сектор в тази трета държава, или международна организация; стандартни клаузи за защита; формати и процедури за обмена на информация чрез електронни средства между администраторите, обработващите лични данни и надзорните органи за задължителните фирмени правила; взаимопомощ; и договорености за обмена на информация чрез електронни средства между надзорните органи, както и между надзорните органи и Комитета по защита на данните.

(169) Комисията следва да приеме актове за изпълнение с незабавно приложение, когато

наличните доказателства свидетелстват, че трета държава, територия или конкретен сектор в тази трета държава, или международна организация не осигуряват адекватно ниво на защита, и наложителни причини за спешност изискват това.

(170) Доколкото целта на настоящия регламент, а именно осигуряване на еквивалентно ниво на защита на физическите лица и свободното движение на лични данни навсякъде в Съюза, не може да бъде постигната в достатъчна степен от държавите членки, а поради обхвата или последиците от предвиденото действие, може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в **член 5 от Договора за Европейския съюз** (**ДЕС**). В съответствие с принципа на пропорционалност, уреден в същия член, настоящият регламент не надхвърля необходимото за постигането на тази цел.

(171) **Директива 95/46/ЕО** следва да бъде отменена с настоящия регламент. Обработването, което вече е в ход към датата на прилагане на настоящия регламент, следва да се приведе в съответствие с него в срок от две години, след като регламентът влезе в сила. Когато обработването на данни се основава на съгласие по силата на **Директива 95/46/ЕО**, не е необходимо субектът на данни да дава отново съгласие, ако начинът, по който е заявено съгласието, съответства на условията в настоящия регламент, за да може администраторът да продължи обработването на данни след датата на прилагане на настоящия регламент. Приетите от Комисията решения и разрешенията на надзорните органи въз основа на **Директива 95/46/ЕО** остават в сила, докато не бъдат изменени, заменени или отменени.

(172) В съответствие с **член 28, параграф 2 от Регламент (ЕО) № 45/2001** беше проведена консултация с Европейския надзорен орган по защита на данните и той даде становище на 7 март 2012 г.(**17**).

(173) Настоящият регламент следва да се прилага спрямо всички въпроси, свързани със защитата на основните права и свободи по отношение на обработването на лични данни, които не са предмет на специалните задължения със същата цел, установени с **Директива 2002/58/ЕО на Европейския парламент и на Съвета**(**18**), включително задълженията на администратора и правата на физическите лица. За да се изясни връзката между настоящия регламент и **Директива 2002/58/ЕО** , директивата следва да бъде съответно изменена. След приемането на настоящия регламент **Директива 2002/58/ЕО** следва да се преразгледа, по-специално за гарантиране на съгласуваност с настоящия регламент.

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА 1
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, както и правилата по отношение на свободното движение на лични данни.

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

3. Свободното движение на лични данни в рамките на Съюза не се ограничава, нито се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни.

Член 2

Материален обхват

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

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

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

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

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

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

3. При обработването на лични данни от институциите, органите, службите и агенциите на Съюза се прилага **Регламент (ЕО) № 45/2001**. **Регламент (ЕО) № 45/2001** и другите правни актове на Съюза, приложими към подобна обработка на лични данни, се адаптират към принципите и правилата на настоящия регламент в съответствие с **член 98**.

4. Настоящият регламент не засяга прилагането на **Директива 2000/31/ЕО**, и по-специално разпоредбите относно отговорностите на междинните доставчици на услуги в членове 12—15 от посочената директива.

Член 3

Териториален обхват

1. Настоящият регламент се прилага за обработването на лични данни в контекста на дейностите на дадено място на установяване на администратор или обработващ лични данни в Съюза, независимо дали обработването се извършва в Съюза или не.

2. Настоящият регламент се прилага за обработването на лични данни на субекти на данни, които се намират в Съюза, от администратор или обработващ лични данни, който не е установен в Съюза, когато дейностите по обработване на данни са свързани със:

а) предлагането на стоки или услуги на такива субекти на данни в Съюза, независимо дали от субекта на данни се изисква плащане; или

б) наблюдението на тяхното поведение, доколкото това поведение се проявява в рамките на Съюза.

3. Настоящият регламент се прилага за обработването на лични данни от администратор, който не е установен в Съюза, но е установен на място, където се прилага правото на държава членка по силата на международното право.

Член 4

Определения

За целите на настоящия регламент:

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, умствената, икономическата, културната или социална идентичност на това физическо лице;

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

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

4) „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;

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

6) „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;

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

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

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

10) „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;

11) „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;

12) „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;

13) „генетични данни“ означава лични данни, свързани с наследени или придобити генетичните 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;

14) „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;

15) „данни за здравословното състояние“ означава лични данни, свързани с физическото или психическото здраве на физическо лице, включително предоставянето на здравни услуги, които

дават информация за здравословното му състояние;

16) „основно място на установяване“ означава:

а) по отношение на администратор, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, освен в случаите, когато решенията по отношение на целите и средствата за обработването на лични данни се вземат на друго място на установяване на администратора в Съюза и на това място на установяване има правомощия за прилагане на тези решения, в който случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване;

б) по отношение на обработващ лични данни, установен в повече от една държава членка — мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващия лични данни в Съюза, където се осъществяват основните дейности по обработването в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно настоящия регламент;

17) „представител“ означава физическо или юридическо лице, установено в Съюза, което, назначено от администратора или обработващия лични данни в писмена форма съгласно **член 27**, представлява администратора или обработващия лични данни във връзка със съответните им задължения по настоящия регламент;

18) „дружество“ означава физическо или юридическо лице, което осъществява икономическа дейност, независимо от правната му форма, включително партньорствата или сдруженията, които редовно осъществяват икономическа дейност;

19) „група предприятия“ означава контролиращо предприятие и контролираните от него предприятия;

20) „задължителни фирмени правила“ означава политики за защита на личните данни, които се спазват от администратор или обработващ лични данни, установен на територията на държава членка, при предаване или съвкупност от предавания на лични данни до администратор или обработващ лични данни в една или повече трети държави в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност;

21) „надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно **член 51**;

22) „засегнат надзорен орган“ означава надзорен орган, който е засегнат от обработването на лични данни, тъй като:

а) администраторът или обработващият лични данни е установен на територията на държавата членка на този надзорен орган;

б) субектите на данни с местопребиваване в държавата членка на този надзорен орган са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването; или

в) до този надзорен орган е подадена жалба;

23) „трансгранично обработване“ означава или:

а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обработващ лични данни в Съюза, като администраторът или обработващият лични данни е установен в повече от една държава членка; или

б) обработване на лични данни, което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващ лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка;

24) „относимо и обосновано възражение“ означава възражение срещу проект на решение относно това дали е налице нарушение на настоящия регламент или не, или дали предвиденото действие по отношение на администратора или обработващия лични данни отговаря на изискванията на настоящия регламент, което ясно доказва, че проектът за решение води до значителни рискове за основните права и свободи на субектите на данни и, където е приложимо, за свободното движение на лични данни в рамките на Съюза;

25) „услуга на информационното общество“ означава услуга по смисъла на **член 1, параграф 1, точка б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета**(19);

26) „международна организация“ означава организация и нейните подчинени органи, регламентирани от международното публично право, или друг орган, създаден чрез или въз основа на споразумение между две или повече държави.

ГЛАВА 2
Принципи

Член 5

Принципи, свързани с обработването на лични данни

1. Личните данни са:

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

б) събирани за конкретни, изрично указани и легитимни цели и не се обработват по-нататък по начин, 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 89, параграф 1**, за несъвместимо с първоначалните цели („ограничение на целите“);

в) подходящи, свързани със и ограничени до необходимото във връзка с целите, за които се обработват („свеждане на данните до минимум“);

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

д) съхранявани във форма, която да позволява идентифицирането на субекта на данните за период, не по-дълъг от необходимото 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 89, параграф 1**, 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) обработвани 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 и е в състояние да докаже спазването на параграф 1 („отчетност“).

Член 6

Законосъобразност на обработването

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

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

б) 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;

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

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

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-

специално когато субектът на данните е дете.

Буква е) на първа алинея не се прилага за обработването, което се извършва от публични органи при изпълнението на техните задачи.

2. Държавите членки могат да запазят или въведат по-конкретни разпоредби, за да адаптират прилагането на правилата на настоящия регламент по отношение на обработването, необходимо за спазването на параграф 1, букви в) и д), като установят по-конкретно специални изисквания за обработването и други мерки, за да се гарантира законосъобразно и добросъвестно обработване, включително за други особени случаи на обработване на данни, предвидени в глава IX.

3. Основанието за обработването, посочено в параграф 1, букви в) и д), е установено от:

а) правото на Съюза или

б) правото на държавата членка, което се прилага спрямо администратора.

Целта на обработването се определя в това правно основание или доколкото се отнася до обработването по параграф 1, буква д), то трябва да е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора. Това правно основание може да включва конкретни разпоредби за адаптиране на прилагането на разпоредбите на настоящия регламент, inter alia общите условия, които определят законосъобразността на обработването от администратора, видовете данни, които подлежат на обработване, съответните субекти на данни; образуванията, пред които могат да бъдат разкривани лични данни, и целите, за които се разкриват; ограниченията по отношение на целите на разкриването; периодът на съхранение и операциите и процедурите за обработване, включително мерки за гарантиране на законосъобразното и добросъвестно обработване, като тези за други конкретни случаи на обработване съгласно предвиденото в глава IX. Правото на Съюза или правото на държавата членка се съобразява с обществения интерес и е пропорционално на преследваната легитимна цел.

4. 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 или правото на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на целите по **член 23, 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 9** или се обработват лични данни, отнасящи се до присъди и нарушения, съгласно **член 10**;

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 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 бива информиран за това. Оттеглянето на съгласие 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 6, параграф 1, буква а**), във връзка с прякото предлагане на услуги на информационното общество на деца, обработването на данни на дете е законосъобразно, ако детето е поне на 16 години. Ако детето е под 16 години това обработване е законосъобразно само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето.

Държавите членки могат да предвидят в правото си по-ниска възраст за същите цели при условие че тази по-ниска възраст не е под 13 години.

2. В такива случаи администраторът полага разумни усилия за удостоверяване, че съгласието е дадено или разрешено 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

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 синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

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 или правото на държава членка 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 или правото на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните;

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

г) обработването се извършва при подходящи гаранции в хода на законните дейности на фондация, сдружение или друга структура с нестопанска цел, с политическа, философска, религиозна или синдикална цел, при условие че обработването е свързано единствено с членовете или бившите членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че личните данни не се разкриват без съгласието на субектите на данните;

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

е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;

ж) обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната 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, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на Съюза или правото на държава членка 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, въз основа на правото на Съюза или правото на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна;

й) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно **член 89, параграф 1**, на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната 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, могат 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 професионална тайна по силата на правото на Съюза или правото на държавата членка или правилата, установени от националните компетентни органи или от друго лице, също обвързано от задължение за тайна по силата на правото на Съюза или правото на държавата членка или правилата, установени от националните компетентни органи.

4. Държавите членки могат да запазят или да въведат допълнителни условия, включително и ограничения, по отношение на обработването на генетични данни, биометрични данни или данни за здравословното състояние.

Член 10

Обработване на лични данни, свързани с присъди и нарушения

Обработването на лични данни, свързани с присъди и нарушения или със свързаните с тях мерки за сигурност, въз основа на **член 6, параграф 1**, се извършва само под контрола на официален орган или когато обработването е разрешено от правото на Съюза или правото на държава членка, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни. Пълен регистър на присъдите по наказателни дела се поддържа само под контрола на официален орган.

Член 11

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 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 15—20** не се прилагат, освен когато субектът на данни, с цел да упражни правата си по тези членове, предостави допълнителна информация, позволяваща неговото идентифициране.

ГЛАВА 3
Права на субекта на данни

РАЗДЕЛ 1
Прозрачност и условия

Член 12

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

1. Администраторът предприема необходимите мерки за предоставяне на всякаква информация по **членове 13** и **14** и на всякаква комуникация по **членове 15—22** и **член 34**, която се отнася до обработването, на субекта на данните 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 положение че идентичността на субекта на данните е доказана с други средства.

2. Администраторът съдейства за упражняването на правата на субекта на данните по **членове 15—22**. В случаите, посочени в **член 11, параграф 2**, администраторът не отказва да предприеме действия по искане на субекта на данните за упражняване на правата му по **членове 15—22**, 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 15—22**, 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 взема предвид сложността и броя 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 не 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 надзорен орган и търсене на защита по съдебен ред.

5. Информацията по **членове 13** и **14** и всяка комуникация и действия по **членове 15—22** и **член 34** се предоставят безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може или:

а) да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или комуникацията или предприемането на исканите действия, или

б) 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 11**, когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искане по **членове 15—21**, администраторът 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 13** и **14**, 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. На Комисията се предоставя правомощието да приема делегирани актове в съответствие с **член 92** с цел определяне на информацията, която да бъде представена под формата на икони, и на процедурите за предоставяне на стандартизирани икони.

РАЗДЕЛ 2
Информация и достъп до лични данни

Член 13

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) данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;

б) координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

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

основание за обработването;

г) когато обработването се извършва въз основа на **член 6, параграф 1, буква е**), законните интереси, преследвани от администратора или от трета страна;

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 отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно посоченото в **членове 46** или **47**, или **член 49, параграф 1**, втора алинея 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 право да се направи възражение срещу обработването, както и правото на преносимост на данните;

в) когато обработването се основава на **член 6, параграф 1, буква а**) или **член 9, 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 жалба до надзорен орган;

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

е) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в **член 22**, 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 по-нататък да обработва 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 14

Информация, предоставяна, когато личните данни идват от субекта на данните

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

а) данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;

б) координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

в) целите на обработването, за което личните данни са предназначени, 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 данните на трета държава или на международна организация, и наличието или отсъствието на решение на Комисията относно адекватното ниво на защита или в случай на предаване на данни съгласно **член 46** или **47**, или **член 49, параграф 1**, втора алинея с 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 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) когато обработването се извършва въз основа на **член 6, параграф 1, буква е**), законните интереси, преследвани от администратора или от трета страна;

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

г) когато обработването се основава на **член 6, параграф 1, буква а**) или **член 9, 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;

д) правото на жалба до надзорен орган;

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

ж) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в **член 22**, 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 личните данни по-нататък 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.

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, при спазване на условията и гаранциите по **член 89, параграф 1**, 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 тези случаи администраторът взема подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните, което включва и предоставяне на публичен достъп до информацията;

в) получаването или разкриването е изрично разрешено от правото на Съюза или правото на държавата членка, което се прилага спрямо администратора и в което се предвиждат също подходящи мерки за защита на легитимните 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 или право на държава членка, включително законово задължение за поверителност.

Член 15

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 жалба до надзорен орган;

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 22**, 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 46** във връзка с предаването.

3. Администраторът предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, администраторът може да наложи разумна такса въз основа на административните разходи. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не 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 16

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 добавяне на декларация.

Член 17

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 посочените по-долу 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 6, параграф 1, буква а**) или **член 9, параграф 2, буква а**), и няма друго правно основание за обработването;

в) субектът на данните възразява срещу обработването съгласно **член 21, параграф 1** и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването съгласно **член 21, параграф 2**;

г) личните данни са били обработвани незаконосъобразно;

д) личните данни трябва да бъдат изтрити с цел спазването на правно задължение по правото на Съюза или правото на държава членка, 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, 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 изисква обработване, предвидено в правото

на Съюза или правото на държавата членка, 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 9, параграф 2**, букви з) и и), както и **член 9, параграф 3**;

г) за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно **член 89, параграф 1**, доколкото съществува вероятност правото, установено 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 18

Право на ограничаване на обработването

1. Субектът на данните има право да изиска от администратора ограничаване на обработването, когато се прилага едно от следното:

а) точността на личните данни се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността 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 21, параграф 1** в очакване на проверка дали законните основания на администратора имат преимущество 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 лице или поради важни основания 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.

Член 19

Задължение за уведомяване при коригиране или изтриване на лични данни или

ограничаване на обработването

Администраторът съобщава за всяко извършено в съответствие с **член 16**, **член 17, параграф 1** и **член 18** 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 20

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 6, параграф 1, буква а**) или **член 9, параграф 2, буква а**) или на договорно задължение съгласно **член 6, параграф 1, буква б**); и

б) обработването се извършва по автоматизиран начин.

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, когато това е технически осъществимо.

3. Упражняването на правото, посочено в параграф 1 от настоящия член не засяга **член 17**. 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 21

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 6, параграф 1, буква д) или буква е**), включително профилиране, основаващо

се на посочените разпоредби. Администраторът прекратява обработването на личните данни, освен ако не 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. Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възражение срещу обработване на лични данни, отнасящо се до него за този вид маркетинг, което включва и профилиране, доколкото то е свързано с директния маркетинг.

3. Когато субектът на данни възрази срещу обработване за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява.

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

5. В контекста на използването на услугите на информационното общество и независимо от **Директива 2002/58/ЕО**, субектът на данните може да упражнява правото си на възражение чрез автоматизирани средства, като се използват технически спецификации.

6. Когато лични данни се обработват за целите на научни или исторически изследвания или за статистически цели съгласно **член 89, параграф 1**, 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 публичен интерес.

Член 22

Автоматизирано вземане на индивидуални решения, включително профилиране

1. Субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последствия за субекта на данните 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 субект на данни и администратор;

б) е разрешено от правото на Съюза или правото на държава членка, което се прилага спрямо администратора, и в което се предвиждат също подходящи мерки за защита на правата и свободите, и легитимните 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 и свободите и легитимните 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 не се основават на специалните категории лични данни, посочени в **член 9, параграф 1**, освен ако не се прилага **член 9, параграф 2, буква а) или буква ж**) и не са въведени подходящи мерки за защита на правата и свободите и легитимните интереси на субекта на данните.

РАЗДЕЛ 5
Ограничения

Член 23

Ограничения

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

а) националната сигурност;

б) отбраната;

в) обществената сигурност;

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

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

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

ж) предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

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

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

й) изпълнението по гражданскоправни искове.

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

а) целите на обработването или категориите обработване;

б) категориите лични данни;

в) обхвата на въведените ограничения;

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

д) спецификацията на администратора или категориите администратори;

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

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

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

ГЛАВА 4
Администратор и обработващ лични данни

РАЗДЕЛ 1
Общи задължения

Член 24

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 кодекси за поведение, посочени в **член 40** или одобрени механизми за сертифициране, посочени в **член 42** може да се използва като елемент за доказване на спазването на задълженията на администратора.

Член 25

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, периода 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. Одобреният механизъм за сертифициране съгласно **член 42** може да се използва като елемент, за да се докаже спазването на изискванията, предвидени в параграфи 1 и 2 от настоящия член.

Член 26

Съвместни администратори

1. Когато двама или повече администратори съвместно определят целите и средствата на обработването, те са съвместни администратори. Те определят по прозрачен начин съответните си отговорности за изпълнение на задълженията по настоящия регламент, по-специално що се отнася до упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информацията, посочена в **членове 13** и **14**, посредством договореност помежду си, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на Съюза или правото на държава членка, което се прилага спрямо администраторите. В договорността може да се посочи точка за контакт за субектите на данни.

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

3. Независимо от условията на договорността, 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 27

Представители на администратори и обработващи лични данни, които не са установени в Съюза

1. В случаите когато се прилага **член 3, параграф 2**, администраторът или обработващият личните данни определя писмено представител в Съюза.

2. Задължението, установено в параграф 1 от настоящия член, не се прилага за:

а) обработване, което е спорадично, не включва мащабно обработване на специални категории данни по **член 9, параграф 1**, нито обработване на лични данни, свързани с присъди и нарушения, посочени в **член 10**, и няма вероятност да породи риск за правата и свободите на физическите лица, като се имат предвид естеството, контекстът, обхватът и целите на обработването; или

б) публичен орган или структура.

3. Представителят е установен в една от държавите членки, в която се намират субектите на данни, чиито лични данни се обработват във връзка с предлагането на стоки или услуги или чието поведение се наблюдава.

4. Администраторът или обработващият лични данни предоставя на представителя мандат, съгласно който по-специално надзорните органи и субектите на данни могат освен или вместо към администратора или обработващия лични данни да се обръщат към представителя по всички въпроси, свързани с обработването, с цел да се гарантира спазване на настоящия регламент.

5. Определянето на представител от администратора или обработващия лични данни не засяга правните действия, които биха могли да бъдат предприети срещу самия администратор или обработващ личните данни.

Член 28

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 осигурява защита на правата на субектите на данни.

2. Обработващият данни не включва друг обработващ данни без предварителното конкретно или общо писмено разрешение на администратора. В случай на общо писмено разрешение, обработващият данни винаги информира администратора за всякакви планирани

промени за включване или замяна на други лица, обработващи данни, като по този начин даде 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 по силата на правото на Съюза или правото на държава членка, което се прилага спрямо обработващия лични данни, като в този 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 32**;

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 32—36**, 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 не 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. Придържането на обработващия лични данни към одобрен кодекс за поведение, посочен в **член 40** или одобрен механизъм за сертифициране, посочен в **член 42** 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 администратора или обработващия лични данни съгласно **членове 42** и **43**.

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 93, параграф 2**.

8. Надзорният орган може да приема стандартни договорни клаузи по въпросите, посочени в параграфи 3 и 4 от настоящия член, и в съответствие с механизма за съгласуваност, посочен в **член 63**.

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

10. Без да се засягат **членове 82**, **83** и **84**, 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 29

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 не се изисква от правото на Съюза или правото на държава членка.

Член 30

Регистри на дейностите по обработване

1. Всеки администратор и — когато това е приложимо — представител на 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 и — когато това е приложимо — на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива;

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 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, а в случай на предаване на данни, посочено в **член 49, параграф 1**, втора алинея, 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 32, параграф 1**.

2. Всеки обработващ лични данни и — когато това е приложимо — представителят на обработващия 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 и на всеки администратор, от чието име действа обработващият лични данни и — когато това е приложимо —на представителя на администратора или обработващия лични данни и на длъжностното лице по 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, а в случай на предаване на данни, посочено в **член 49, параграф 1**, втора алинея, документация за подходящите гаранции;

г) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в **член 32, параграф 1**.

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

4. При поискване, администраторът или обработващият лични данни и — когато това е приложимо — представителят на администратора или на обработващия личните данни, осигуряват достъп до регистъра на надзорния орган.

5. Задълженията, посочени в параграфи 1 и 2, не се прилагат по отношение на предприятие или дружество с по-малко от 250 служители, освен ако има вероятност извършваното от тях обработване да породи риск за правата и свободите на субектите на данни, ако обработването не е спорадично или включва специални категории данни по **член 9, параграф 1** или лични данни, свързани с присъди и нарушения, по **член 10**.

Член 31

Сътрудничество с надзорния орган

При поискване администраторът и обработващият лични данни и — когато това е приложимо — техните представители си сътрудничат с надзорния орган при изпълнението на неговите задължения.

РАЗДЕЛ 2
Сигурност на личните данни

Член 32

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. Придържането към одобрен кодекс за поведение, посочен в **член 40** или одобрен механизъм за сертифициране, посочен в **член 42** може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграф 1 от настоящия член.

4. 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 не се изисква да прави това по силата на правото на Съюза или правото на държава членка.

Член 33

Уведомяване на надзорния орган 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 надзорния орган, компетентен в съответствие с **член 55**, освен ако не съществува вероятност нарушението на сигурността на личните данни да породи риск за правата и свободите на физическите лица. Уведомлението до надзорния орган 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, ако е възможно, категориите и приблизителният брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на лични данни;

б) посочване на името и координатите за връзка на длъжностното лице по защита на данните или на друга точка за контакт, от която може да се получи повече информация;

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 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 надзорния орган да провери дали е спазен настоящият член.

Член 34

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 33, параграф 3**, букви б), в) и г).

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

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 материализира 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, надзорният орган 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.

РАЗДЕЛ 3
Оценка на въздействието върху защитата на данните и предварителни консултации

Член 35

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, когато такова е определено.

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

а) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично 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 9, параграф 1** или на лични данни за присъди и нарушения по **член 10**; или

в) систематично мащабно наблюдение на публично достъпна зона.

4. Надзорният орган съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно параграф 1. Надзорният орган съобщава тези списъци на Комитета, посочен в **член 68**.

5. Надзорният орган може също да състави и оповести списък на видовете операции по обработване, за които не се изисква оценка на въздействието върху защитата на данните. Надзорният орган съобщава тези списъци на Комитета.

6. Преди приемането на списъците, посочени в параграфи 4 и 5, компетентният надзорен орган прилага посочения в **член 63** механизъм за съгласуваност, ако тези списъци включват дейности за обработване, свързани с предлагането на стоки или услуги на субекти на данни или с наблюдението на тяхното поведение в няколко държави членки или могат съществено да засегнат свободното движение на лични данни в рамките на Съюза.

7. Оценката съдържа най-малко:

а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

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 осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

8. При оценката на въздействието на операциите по обработване, извършвани от администраторите и обработващите лични данни, надлежно се отчита и спазването от тяхна страна на одобрените кодекси за поведение, посочени в член 340 особено 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 търговските или обществените интереси или сигурността на операциите по обработване.

10. Когато обработването съгласно **член 6, параграф 1, буква в**) или д) има правно основание в правото на Съюза или в правото на държавата членка, под чиято юрисдикция е администраторът, и това право 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 в контекста на приемането на това правно основание, параграфи 1—7 не се прилагат, освен ако държавите членки не сметнат за необходимо да направят такава оценка преди започването на дейностите за обработване.

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 36

Предварителна консултация

1. Администраторът се консултира с надзорния орган преди обработването, когато оценката на въздействието върху защитата на данните съгласно **член 35** покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска.

2. Когато надзорният орган 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, надзорният орган в срок до осем седмици след получаване на искането за консултация дава писмено становище на администратора или на обработващия лични данни, когато е приложимо, 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. Надзорният орган 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 може да спрат да текат, докато надзорният орган получи всяка евентуално поискана от него информация за целите на консултацията.

3. Когато се консултира с надзорния орган съгласно параграф 1, администраторът предоставя на надзорния орган следната информация:

а) където е приложимо — информация за съответните отговорности на администратора, съвместните администратори и обработващите лични данни, които се занимават с обработването, по-конкретно при обработване на данни в рамките на група предприятия;

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) където е приложимо, координатите за връзка на длъжностното лице по защита на данните;

д) оценката на въздействието върху защитата на данните по **член 35**; както и

е) всякаква друга информация, поискана от надзорния орган.

4. Държавите членки се консултират с надзорния орган по време на изготвянето на предложения за законодателни мерки, които да бъдат приети от националните парламенти, или на регулаторни мерки, основани на такива законодателни мерки, които се отнасят до обработването.

5. Без да се засяга параграф 1, правото на държавите членки може да изисква от администраторите да се консултират с надзорния орган и да получават предварително разрешение от него във връзка с обработването от администратор за изпълнението на задача, осъществявана от администратора в полза на обществения интерес, включително обработване във връзка със социалната закрила и общественото здраве.

РАЗДЕЛ 4
Длъжностно лице по защита на данните

Член 37

Определяне на длъжностното лице по защита на данните

1. Администраторът и обработващият лични данни определят длъжностно лице по защита на данните във всички случаи, когато:

а) обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;

б) основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или

в) основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни съгласно **член 9** и на лични данни, свързани с присъди и нарушения, по **член 10**.

2. Група предприятия може да назначи едно длъжностно лице по защита на данните, при условие че от всяко предприятие има лесен достъп до длъжностно лице по защита на данните.

3. Когато администраторът или обработващият лични данни е обществен орган или структура, едно длъжностно лице по защита на данните може да бъде назначено за няколко такива органа или структури, като се отчита организационната им структура и размер.

4. В случаи, различни от посочените в параграф 1, администраторът или обработващият лични данни или сдружения и други структури, представляващи категории администратори или обработващи лични данни, могат да определят — или ако това се иска от правото на Съюза или право на държава членка определят — длъжностно лице по защита на данните. Длъжностното лице по защита на данните може да действа в полза на такива сдружения и други структури, представляващи администратори или обработващи лични данни.

5. 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 39**.

6. Длъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни или да изпълнява задачите въз основа на договор за услуги.

7. Администраторът или обработващият лични данни публикува данните за контакт с длъжностното лице по защита на данните и ги съобщава на надзорния орган.

Член 38

Длъжност на длъжностното лице по защита на данните

1. Администраторът и обработващият лични данни гарантират, че длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни.

2. Администраторът и обработващият лични данни подпомагат длъжностното лице по защита на данните при изпълнението на посочените в **член 39** 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. Администраторът и обработващият лични данни правят необходимото 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 е длъжно да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държава членка.

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

Член 39

Задачи на длъжностното лице по защита на данните

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

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка;

б) да наблюдава спазването на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка 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) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно **член 35**;

г) да си сътрудничи с надзорния орган;

д) да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в **член 36**, и по целесъобразност да се консултира по всякакви други въпроси.

2. При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

РАЗДЕЛ 5
Кодекси за поведение и сертифициране

Член 40

Кодекси за поведение

1. Държавите членки, надзорните органи, Комитетът и Комисията насърчават изготвянето на кодекси за поведение, които имат за цел да допринесат за правилното прилагане на настоящия регламент, като се отчитат специфичните характеристики на различните обработващи данни сектори и конкретните нужди на микропредприятията, малките и средните предприятия.

2. Сдруженията и други структури, представляващи категории администратори или обработващи лични данни, могат да изготвят кодекси за поведение или да изменят или допълват такива кодекси с цел да бъде уточнено прилагането на настоящия регламент, като по отношение на:

а) добросъвестното и прозрачно обработване;

б) законните интереси, преследвани от администраторите в конкретни аспекти;

в) събирането на лични данни;

г) псевдонимизацията на лични данни;

д) информирането на обществеността и на субектите на данни;

е) упражняването на правата на субектите на данни;

ж) информирането и закрилата на децата и начина за получаване на съгласие от носещите родителска отговорност за детето;

з) мерките и процедурите, посочени в **членове 24** и **25**, и мерките за осигуряване на посочената в **член 32** сигурност на обработването;

и) уведомяването на надзорните органи за нарушения на сигурността на личните данни и съобщаването за такива нарушения на сигурността на личните данни на субектите на данни;

й) предаването на лични данни на трети държави или международни организации; или

к) извънсъдебните производства и другите процедури за разрешаване на спорове между администраторите и субектите на данни по отношение на обработването, без да се засягат правата на субектите на данни съгласно **членове 77** и **79**.

3. Освен спазването на настоящия регламент от администратора или обработващия лични данни, към които се прилага настоящият регламент, кодекси за поведение, одобрени съгласно параграф 5 от настоящия член и общовалидни съгласно параграф 9 от настоящия член, могат също така да се прилагат към администратори или обработващи лични данни, непопадащи в обхвата на настоящия регламент съгласно **член 3**, с цел да се осигурят подходящи гаранции в рамките на предаването на лични данни на трети държави или международни организации съгласно условията, посочени в **член 46, параграф 2, буква д**). Тези администратори или обработващи лични данни поемат задължителни ангажименти с изпълнителна сила, чрез договорни или други инструменти със

задължителен характер, да прилагат тези подходящи гаранции, включително по отношение на правата на субектите на данни.

4. Кодексът за поведение, посочен в параграф 2 от настоящия член съдържа механизми, които позволяват на посочения в **член 41, параграф 1** орган да извършва задължителното наблюдение на спазването на неговите разпоредби от администраторите или обработващите лични данни, които приемат да го прилагат, без да се засягат задълженията и правомощията на надзорните органи, компетентни по силата на **член 55** или **56**.

5. Сдруженията и другите структури, посочени в параграф 2 от настоящия член, които възнамеряват да изготвят кодекс за поведение или да изменят или допълнят съществуващ кодекс, представят проекта на кодекс, негово изменение или допълнение на надзорния орган, който е компетентен съгласно **член 55** Надзорният орган дава становище дали проектът за кодекс, негово изменение или допълнение съответстват на настоящия регламент и одобрява този проект на кодекс, негово изменение или допълнение, ако установи, че той осигурява достатъчно подходящи гаранции.

6. Когато проектът на кодекс, негово изменение или допълнение е одобрено в съответствие с параграф 5 и когато съответният кодекс за поведение няма отношение към дейности по обработване в няколко държави членки, надзорният орган регистрира и публикува кодекса.

7. Ако проект на кодекс за поведение има отношение към дейности по обработване в няколко държави членки, надзорният орган, който е компетентен съгласно **член 55**, преди одобряването на проекта на кодекс, негово изменение или допълнение, го представя, по посочената в **член 63** процедура, на Комитета, който дава становище дали проектът на кодекс, негово изменение или допълнение съответстват на настоящия регламент, или, в случаите, посочени в параграф 3 от настоящия член, осигуряват подходящи гаранции.

8. Ако посоченото в параграф 7 становище потвърди, че проектът на кодекс, негово изменение или допълнение съответстват на настоящия регламент или, в случаите, посочени в параграф 3, осигуряват подходящи гаранции, Комитетът представя становището си на Комисията.

9. Комисията може чрез актове за изпълнение да реши дали одобрения кодек за поведение, негово изменение или допълнение, който ѝ е представен по силата на параграф 8 от настоящия член, е общовалиден в рамките на Съюза. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

10. Комисията осигурява подходяща публичност на одобрените кодекси, за които е решено, че са общовалидни в съответствие с параграф 9.

11. Комитетът събира всички одобрени кодекси за поведение, техните изменения и допълнения в регистър и ги прави обществено достъпни чрез всички подходящи средства.

Член 41

Наблюдение на одобрените кодекси за поведение

1. Без да се засягат задачите и правомощията на компетентния надзорен орган по

членове 57 и **58**, наблюдението на спазването на даден кодекс за поведение съгласно **член 40** може да се осъществява от орган, който има съответното ниво на опит във връзка с предмета на кодекса и е акредитиран за тази цел от компетентния надзорен орган.

2. Посоченият в параграф 1 орган може да бъде акредитиран да наблюдава съответствието с кодекс за поведение, ако:

а) е доказал в задоволителна степен пред компетентния надзорен орган своята независимост и опит във връзка с предмета на кодекса;

б) е установил процедури, даващи му възможност да направи оценка на допустимостта на съответните администратори и обработващи лични данни да прилагат кодекса, да наблюдава дали те спазват разпоредбите на кодекса и периодично да прави преглед на неговото функциониране;

в) е установил процедури и структури за обработване на жалби за нарушения на кодекса или за начина, по който кодексът е бил приложен или се прилага от администратор или обработващ лични данни, и за прозрачното довеждане на тези процедури и структури до знанието на субектите на данни и обществеността; и

г) демонстрира в задоволителна степен пред компетентния надзорен орган, че задачите и задълженията му не водят до конфликт на интереси.

3. Компетентният надзорен орган представя проектокритериите за акредитацията на орган по параграф 1 от настоящия член на Комитета в съответствие с посочения в **член 63** механизъм за съгласуваност.

4. Без да се засягат задачите и правомощията на компетентния надзорен орган и разпоредбите на глава VIII, при наличие на адекватни предпазни мерки орган, посочен в параграф 1 от настоящия член, предприема съответните действия в случай на нарушение на кодекса от страна на администратор или обработващ лични данни, включително като суспендира членството в кодекса или изключва от него съответния администратор или обработващ лични данни. Той информира компетентния надзорен орган за тези действия и за мотивите, с които са предприети.

5. Компетентният надзорен орган анулира акредитацията на орган по параграф 1, ако условията за акредитация не са били спазени или вече не се спазват или ако предприетите от органа действия нарушават настоящия регламент.

6. Настоящият член не се прилага по отношение на обработване, извършвано от публичните власти и органи.

Член 42

Сертифициране

1. Държавите членки, надзорните органи, Комитетът по защита на данните и Комисията насърчават, особено на равнището на Съюза, създаването на механизми за сертифициране за защита на данните и на печати и маркировки за защита на данните с цел да се демонстрира спазването на

настоящия регламент при операциите по обработване от страна на администраторите и обработващите лични данни. Отчитат се конкретните нужди на микропредприятията, на малките и средните предприятия.

2. Освен спазването на настоящия регламент от администратора или обработващия лични данни, към които се прилага настоящият регламент, може да се установяват механизми за сертифициране, печати или маркировки за защита на данните, одобрени съгласно параграф 5 от настоящия член, с цел да се демонстрира наличието на подходящи гаранции, осигурени от администраторите и обработващите лични данни, които не са обект на настоящия регламент съгласно **член 3**, в рамките на предаването на лични данни на трети държави или международни организации съгласно условията, посочени в **член 46, параграф 2, буква е**). Тези администратори или обработващи лични данни поемат задължителни ангажименти с изпълнителна сила, чрез договорни или други инструменти със задължителен характер, да прилагат тези подходящи гаранции, включително по отношение на правата на субектите на данни.

3. Сертифицирането е доброволно и е достъпно чрез процедура, която е прозрачна.

4. Сертифицирането по настоящия член не води до намаляване на отговорността на администратора или на обработващия лични данни за спазване на настоящия регламент и не засяга задачите и правомощията на надзорните органи, които са компетентни съгласно **член 55** или **член 56** .

5. Сертифицирането по силата на настоящия член се издава от сертифициращите органи, посочени в **член 43**, или от компетентния надзорен орган, въз основа на критериите, одобрени от компетентния надзорен орган съгласно **член 58, параграф 3**, или, от Комитета съгласно **член 63**. Когато критериите са одобрени от Комитета, това може да доведе до единно сертифициране — „Европейски печат за защита на данните“.

6 Администраторът или обработващият лични данни, който подлага своето обработване на механизма за сертифициране, осигурява на сертифициращия орган, посочен в **член 43**, или ако е приложимо — на компетентния надзорен орган, цялата информация и достъп до своите дейности по обработване, които са необходими за извършване на процедурата по сертифициране.

7. Сертификатът се издава на администратора или обработващия лични данни за максимален срок от три години и може да бъде подновен при същите условия, ако съответните изисквания продължават да са спазени. Сертификатът се оттегля, ако е приложимо, от сертифициращите органи, посочени в **член 43**, или от компетентния надзорен орган, ако изискванията за сертифицирането не са спазени или вече не се спазват.

8. Комитетът обединява всички механизми за сертифициране и всички печати и маркировки за защита на данните в регистър и осигурява публичен достъп до тях по подходящ начин.

Член 43

Сертифициращи органи

1. Без да се засягат задачите и правомощията на компетентния надзорен орган съгласно **членове 57** и **58**, сертифициращите органи, притежаващи подходящ опит в областта на защитата на данните, след уведомяване на надзорния орган с цел, ако е необходимо, той да може да упражни правомощията си съгласно **член 58, параграф 2, буква з**), издават и подновяват сертификат.Държавите членки гарантират, че тези сертифициращи органи се акредитират от един или двама от следните органи:

а) надзорния орган, който е компетентен съгласно **член 55** или **56**;

б) националния орган по акредитация, посочен в съответствие с **Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета**(**20**) в съответствие с EN-ISO/IEC 17065/2012 и с допълнителните изисквания, определени от надзорния орган, който е компетентен съгласно **член 55** или **56**.

2. Сертифициращите органи, посочени в параграф 1, се акредитират в съответствие с посочения параграф само ако:

а) са доказали в задоволителна степен пред компетентния надзорен орган своята независимост и опит във връзка с предмета на сертифицирането;

б) са поели ангажимент да спазват критериите, посочени в **член 42, параграф 5**, и одобрени от надзорния орган, който е компетентен съгласно **член 55** или **56**, или, от Комитета съгласно **член 63**;

в) са установили процедури за издаването, периодичния преглед и отнемането на сертификат, печати и маркировки за защита на данните;

г) са установили процедури и структури за обработване на жалби за нарушения на сертификата или за начина, по който сертификатът е бил приложен или се прилага от администратора или обработващия лични данни, и за прозрачното довеждане на тези процедури и структури до знанието на субектите на данни и обществеността; и

д) демонстрират в задоволителна степен пред компетентния надзорен орган, че задачите и задълженията им не водят до конфликт на интереси.

3. Акредитирането на сертифициращите органи, посочени в параграфи 1 и 2 от настоящия член, се извършва на базата на критериите, одобрени от надзорния орган, който е компетентен съгласно **член 55** или **56**, или, от Комитета съгласно **член 63**. В случай на акредитация съгласно параграф 1, буква б) от настоящия член, тези изисквания допълват изискванията, предвидени в **Регламент (ЕО) № 765/2008** и техническите правила, които описват методите и процедурите на сертифициращите органи.

4. Сертифициращият органи, посочени в параграф 1 отговарят за правилната оценка, която води до сертифициране или отнемане на издаден сертификат, без да се засяга отговорността на администратора или обработващия лични данни за спазването на настоящия регламент. Акредитацията се издава за максимален срок от пет години и може да бъде подновена при същите условия, ако сертифициращият орган отговаря на изискванията, установени в настоящия член.

5. Сертифициращите органи, посочени в параграф 1 представят на компетентните надзорни органи мотивите за издаване или отнемане на съответния сертификат.

6. Изискванията, посочени в параграф 3 от настоящия член, и критериите, посочени в **член 42, параграф 5**, се оповестяват от надзорния орган в леснодостъпна форма. Надзорните органи също така информират Комитета относно тези изисквания и критерии. Комитетът обединява всички механизми за сертифициране и всички печати за защита на данните в регистър и осигурява публичен достъп до тях по подходящ начин.

7. Без да се засяга глава VIII, компетентният надзорен орган или националният орган по акредитация анулира акредитация на сертифициращ орган, посочен в параграф 1 от настоящия член, ако не са били спазени или вече не се спазват условията за акредитация, или ако предприетите от сертифициращия орган действия нарушават настоящия регламент.

8. На Комисията се предоставя правомощие да приема делегирани актове в съответствие с **член 92** с цел уточняване на изискванията, които трябва да бъдат взети предвид по отношение на механизмите за сертифициране за защита на данните, посочени в **член 42, параграф 1**.

9. Комисията може чрез актове за изпълнение да определя технически стандарти за механизмите за сертифициране и за печатите и маркировките за защита на данните, както и механизми за насърчаване и признаване на тези механизми и на печатите и маркировките. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

ГЛАВА 5
Предаване на лични данни на трети държави или международни организации

Член 44

Общ принцип на предаването на данни

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

Член 45

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

1. Предаване на лични данни на трета държава или международна организация може да има, ако Комисията реши, че тази трета държава, територия или един или повече конкретни сектори

в тази трета държава, или въпросната международна организация осигуряват адекватно ниво на защита. За такова предаване не се изисква специално разрешение.

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

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

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

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

3. След оценка на адекватността на нивото на защита Комисията може чрез акт за изпълнение да реши, че дадена трета държава, територия или един или повече конкретни сектори в тази трета държава, или дадена международна организация осигуряват адекватно ниво на защита по смисъла на параграф 2 от настоящия член. В акта за изпълнение се предвижда механизъм за периодичен преглед най-малко веднъж на четири години, при който се отчитат всички имащи отношение промени в третата държава или международната организация. В акта за изпълнение се уточнява неговото териториално и секторно приложение и, ако е приложимо, се посочват надзорният орган или органи, посочени в параграф 2, буква б) от настоящия член. Актът за изпълнение се приема в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

4. Комисията осъществява постоянно наблюдение на развитието в трети държави и международни организации, което би могло да повлияе на действието на решенията, приети съгласно параграф 3 от настоящия член, и на решенията, приети въз основа на **член 25, параграф 6 от Директива 95/46/ЕО**.

5. Ако е налице съответната информация, по-специално след прегледа по параграф 3 от настоящия член, Комисията решава, че дадена трета държава, територия, или един или повече конкретни сектори в трета държава, или дадена международна организация е престанала да осигурява адекватно ниво на защита по смисъла на параграф 2 от настоящия член, при което Комисията в необходимата степен отменя, изменя или спира прилагането на решението по параграф 3 от настоящия член чрез акт за изпълнение без обратна сила. Тези актове за изпълнение се приемат

в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

При надлежно обосновани императивни причини по спешност Комисията незабавно приема приложими актове за изпълнение в съответствие с процедурата, посочена в **член 93, параграф 3**.

6. Комисията започва консултации с третата държава или международната организация с цел да коригира положението, довело до решението, взето по силата на параграф 5.

7. Решението по параграф 5 от настоящия член не засяга предаването на лични данни на третата държава, територия или един или повече конкретни сектори в тази трета държава, или на въпросната международна организация съгласно **членове 46—49**.

8. Комисията публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита.

9. Решенията, приети от Комисията въз основа на **член 25, параграф 6 от Директива 95/46/ЕО**, остават в сила, докато не бъдат изменени, заменени или отменени с решение на Комисията, прието в съответствие с параграфи 3 или 5 от настоящия член.

Член 46

Предаване на данни с подходящи гаранции

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

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

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

б) задължителни фирмени правила в съответствие с **член 47**;

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

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

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

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

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

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

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

4. Надзорният орган прилага механизма за съгласуваност по **член 63** в случаите, посочени в параграф 3 от настоящия член.

5. Разрешенията, издадени от държава членка или надзорен орган въз основа на **член 26, параграф 2 от Директива 95/46/ЕО**, остават валидни, докато не бъдат изменени, заменени или отменени, ако е необходимо, от надзорния орган. Решенията, приети от Комисията въз основа на **член 26, параграф 4 от Директива 95/46/ЕО**, остават в сила, докато не бъдат изменени, заменени или отменени, ако е необходимо, с решение на Комисията, прието в съответствие с параграф 2 от настоящия член.

Член 47

Задължителни фирмени правила

1. Компетентният надзорен орган одобрява задължителни фирмени правила в съответствие с механизма за съгласуваност, определен в **член 63**, ако те:

а) са със задължителен характер, прилагат се спрямо и се привеждат в изпълнение от всеки съответен член на групата предприятия или групата дружества, участващи в съвместна стопанска дейност, включително техните служители;

б) изрично предоставят на субектите на данни приложими права по отношение на обработването на техните лични данни; и

в) изпълняват изискванията, установени в параграф 2.

2. В посочените в параграф 1 задължителни фирмени правила се уточнява най-малко следното:

а) структурата и координатите за връзка на групата предприятия или групата дружества, участващи в съвместна стопанска дейност и на всеки техен член;

б) предаването или съвкупността от предавания на данни, включително категориите лични данни, видът на обработването и неговите цели, видът на засегнатите субекти на данни, и се посочва въпросната трета държава или държави;

в) тяхното правно обвързващо естество както на вътрешно, така и на външно равнище;

г) прилагането на общите принципи за защита на данните, по-специално ограничението на целите, свеждането на данните до минимум, ограничените периоди на съхранение, качеството на данните, защитата на данните на етапа на проектирането и по подразбиране, правното основание за обработването, обработването на специални категории лични данни, мерките за гарантиране сигурността на данните, както и изискванията по отношение на последващото предаване на данни на образувания, които не са обвързани от задължителните фирмени правила;

д) правата на субектите на данни по отношение на обработването и средствата за упражняване на тези права, включително правото на субекта на данни да не бъде обект на решения, основани единствено на автоматизирано обработване, включително профилиране в съответствие с **член 22**, правото на подаване на жалба до компетентния надзорен орган и до компетентните съдилища на държавите членки в съответствие с **член 79**, както и правото на съдебна защита, и когато е приложимо — на обезщетение за нарушаване на задължителните фирмени правила;

е) поемането от администратора или обработващия лични данни, установен на територията на държава членка, на отговорност за всяко нарушение на задължителните фирмени правила от който и да е член на съответната група, който не е установен в Съюза; администраторът или обработващият лични данни е изцяло или частично освободен от такава отговорност само ако докаже, че този член не носи отговорност за събитието, довело до причиняването на вреда;

ж) начинът, по който информацията относно задължителните фирмени правила, по-специално относно разпоредбите, посочени в букви г), д) и е) от настоящия параграф, се предоставя на субектите на данни в допълнение към информацията по **членове 13** и **14**;

з) задачите на всяко длъжностно лице за защита на данните, определено в съответствие с **член 37**, или всяко друго лице или образувание, натоварено да наблюдава спазването на задължителните фирмени правила в рамките на групата предприятия или групата дружества, участващи в съвместна стопанска дейност, както и да наблюдава обучението и разглеждането на жалбите;

и) процедурите по отношение на жалбите;

й) механизмите в рамките на групата предприятия или групата дружества, участващи в съвместна стопанска дейност за осигуряване на проверка на спазването на задължителните фирмени правила. Тези механизми включват одити на защитата на данните и методи за осигуряване на коригиращи действия за защита на правата на субекта на данни. Резултатите от тази проверка следва да се съобщават на лицето или образуването, посочено в буква з), и на управителния съвет на контролиращото предприятие на групата предприятия или на групата дружества, участващи в съвместна стопанска дейност, и следва при поискване да се предоставят на компетентния надзорен орган;

к) механизмите за докладване и записване на промени в правилата и докладването на надзорния орган за тези промени;

л) механизмът за сътрудничество с надзорния орган с цел осигуряване на спазването на правилата от всеки член на групата предприятия или на групата дружества, участващи в съвместна стопанска дейност, по-специално чрез предоставяне на надзорния орган на резултатите от проверките на мерките, посочени в буква й);

м) механизмите за докладване на компетентния надзорен орган за всякакви правни изисквания, приложими към член на групата предприятия или групата дружества, участващи в съвместна стопанска дейност, в трета държава, които е вероятно да доведат до значими неблагоприятни последици за гаранциите, предоставяни от задължителните фирмени правила; както и

н) подходящото обучение за защита на данните за персонала, който постоянно или редовно има достъп до лични данни.

3. Комисията може да определя формáта и процедурите за обмена на информация между администраторите, обработващите лични данни и надзорните органи относно задължителните фирмени правила по смисъла на настоящия член. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

Член 48

Предаване или разкриване на данни, което не е разрешено от правото на Съюза

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 или негова държава членка, без да се засягат другите основания за предаване на данни съгласно настоящата глава.

Член 49

Дерогации в особени случаи

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

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

б) предаването е необходимо за изпълнението на договор между субекта на данните и

администратора или за изпълнението на преддоговорни мерки, взети по искане на субекта на данните;

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

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

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

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

ж) предаването се извършва от регистър, която съгласно правото на Съюза или правото на държавите членки е предназначена да предоставя информация на обществеността и е достъпна за справка от обществеността по принцип или от всяко лице, което може да докаже, че има законен интерес за това, но само доколкото условията за справка, установени в правото на Съюза или правото на държавите членки, са изпълнени в конкретния случай.

Когато предаването не може да се основава на разпоредба на **членове 45** или **46**, включително разпоредби относно задължителни фирмени правила, и не е приложима нито една от дерогациите в особени случаи, посочени в първата алинея на настоящия параграф, предаването на данни на трета държава или международна организация може да се извършва само ако предаването не е повторяемо, засяга само ограничен брой субекти на данни, необходимо е за целите на неоспоримите законни интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данни и администраторът е оценил всички обстоятелства, свързани с предаването на данните, и въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни. Администраторът уведомява надзорния орган за предаването на данни. В допълнение към предоставянето на информацията, посочена в **членове 13** и **14**, администраторът информира субекта на данни за предаването, както и за преследваните неоспоримите законни интереси.

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

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

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

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

организация. Държавите членки съобщават тези разпоредби на Комисията.

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

Член 50

Международно сътрудничество за защита на личните данни

По отношение на трети държави и международни организации Комисията и надзорните органи предприемат подходящи стъпки 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 6
Независими надзорни органи

РАЗДЕЛ 1
Независим статут

Член 51

Надзорен орган

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

2. Всеки надзорен орган допринася за последователното прилагане на настоящия

регламент в рамките на Съюза. За тази цел надзорните органи си сътрудничат помежду си и с Комисията в съответствие с глава VII.

3. Когато в дадена държава членка е създаден повече от един надзорен орган, тази държава членка определя надзорния орган, който представлява тези органи в Комитета, и определя механизма за осигуряване на спазването от другите органи на правилата, отнасящи се до механизма за съгласуваност, посочен в **член 63**.

4. Всяка държава членка уведомява Комисията за разпоредбите в своето законодателство, които приема по силата на настоящата глава, най-късно до 25 май 2018 г. и я уведомява без забавяне за всяко последващо изменение, което ги засяга.

Член 52

Независимост

1. Всеки надзорен орган 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 членът или членовете на надзорния орган остават независими от външно влияние, било то пряко или непряко, и нито търсят, нито приемат инструкции от когото и да било.

3. Член или членовете на всеки надзорен орган се въздържат от всякакви несъвместими със задълженията им действия и по време на своя мандат не се ангажират с никакви несъвместими функции, независимо дали срещу възнаграждение или безвъзмездно.

4. Всяка държава членка гарантира, че на всеки надзорен орган са предоставени човешки, технически и финансови ресурси, помещения и инфраструктура, необходими за ефективното изпълнение на неговите задачи и упражняването на неговите правомощия, включително на тези, които ще бъдат изпълнявани в контекста на взаимопомощта, сътрудничеството и участието в Комитета.

5. Всяка държава членка гарантира, че всеки надзорен орган избира и разполага със свой собствен персонал, който е подчинен изключително на члена или членовете на засегнатия надзорен орган.

6. Всяка държава членка гарантира, че всеки надзорен орган подлежи на финансов контрол, който не засяга неговата независимост и че той има отделен, публичен годишен бюджет, който може да бъде част от общия държавен или национален бюджет.

Член 53

Общи условия за членовете на надзорния орган

1. Държавите членки предвиждат, че всеки член на техните надзорни органи се назначава по прозрачна процедура от:

— парламента;

— правителството;

— държавния глава; или

— независим орган, който съгласно правото на държавата членка е натоварен да извършва назначенията.

2. Всеки член трябва да има квалификациите, опита и уменията, по-специално в областта на защитата на личните данни, необходими, за да изпълнява своите задължения и да упражнява своите правомощия.

3. Задълженията на даден член приключват при изтичането на мандата му, подаването на оставка или задължителното му пенсиониране в съответствие с правото на съответната държава членка.

4. Член на надзорния орган се освобождава само в случай на тежко провинение или ако престане да отговаря на необходимите условия за изпълнение на задълженията.

Член 54

Правила за създаването на надзорния орган

1. Всяка държава членка урежда със закон всичко от по-долу посоченото:

а) създаването на всеки надзорен орган;

б) необходимите квалификации и условия за допустимост за назначаването на членовете на всеки надзорен орган;

в) правилата и процедурите за назначаването на член или членовете на всеки надзорен орган;

г) продължителността на мандата на члена или членовете на всеки надзорен орган, която е не по-малко от четири години, с изключение на първите назначения след 24 май 2016 г., някои от които може да са за по-кратък срок, когато това е необходимо, за да се защити независимостта на надзорния орган посредством процедура за постепенно назначаване;

д) дали и ако да — за колко мандата — се допуска преназначаване на члена или членовете на всеки надзорен орган;

е) условията, регламентиращи задълженията на члена или членовете и на персонала на всеки надзорен орган, забранените действия, функции и облаги, които са несъвместими с тези задължения по време на мандата и след неговото приключване, и правилата, от които се ръководи прекратяването на трудовите правоотношения.

2. Както по време на мандата си, така и след неговото приключване, членът или членовете и персоналът на всеки надзорен орган, в съответствие с правото на Съюза или правото на държава членка, са обвързани от задължението за опазване на професионална тайна по отношение на всяка поверителна информация, която е стигнала до тяхното знание в хода на изпълнението на техните задачи или упражняването на техните правомощия. По време на техния мандат това задължение за опазване на професионалната тайна се прилага по-специално по отношение на подаването на сигнали от физически лица за нарушения на настоящия регламент.

РАЗДЕЛ 2
Компетентност, задачи и правомощия

Член 55

Компетентност

1. Всеки надзорен орган е компетентен да изпълнява задачите и да упражнява правомощията, възложени му в съответствие с настоящия регламент, на територията на своята собствена държава членка.

2. Когато обработването се извършва от публични органи или частни организации на основание **член 6, параграф 1, буква в**) или д), компетентен е надзорният орган на съответната държава членка. В тези случаи **член 56** не се прилага.

3. Надзорните органи не са компетентни да осъществяват надзор на дейностите по обработване, извършвани от съдилищата при изпълнение на съдебните им функции.

Член 56

Компетентност на водещия надзорен орган

1. Без да се засяга **член 55**, надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни е компетентен да действа като водещ надзорен орган за трансграничното обработване, извършвано от посочения администратор или обработващ лични данни в съответствие с процедурата по **член 60**.

2. Чрез дерогация от параграф 1 всеки надзорен орган е компетентен да разглежда внесена при него жалба или евентуални нарушения на настоящия регламент, ако случаят се отнася единствено до място на установяване в държавата членка на надзорния орган или засяга в значителна степен субекти на данни единствено в тази държава членка.

3. В посочените в параграф 2 от настоящия член случаи надзорният орган незабавно уведомява за тях водещия надзорен орган. В срок от три седмици след като е бил уведомен, водещият надзорен орган взема решение за това дали той самият ще разгледа или не случая в съответствие с процедурата, предвидена в **член 60**, като отчита дали администраторът или обработващият лични данни е установен в държавата членка на надзорния орган, който го е

уведомил.

4. Когато водещият надзорен орган реши да разгледа случая, се прилага процедурата по **член 60**. Надзорният орган, уведомил водещия надзорен орган, може да му предостави на проект за решение. Водещият надзорен орган отчита в максимална степен този проект при изготвянето на проекта за решение, посочен в **член 60, параграф 3**.

5. Ако водещият надзорен орган реши да не разгледа случая, надзорният орган, уведомил водещия надзорен орган, го разглежда в съответствие с **членове 61** и **62**.

6. За трансграничното обработване, което извършва, администраторът или обработващият лични данни комуникира единствено с водещия надзорен орган.

Член 57

Задачи

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

а) наблюдава и осигурява прилагането на настоящия регламент;

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) дава становища, в съответствие с правото на държавата членка, на националния парламент, правителството и други институции и органи относно законодателните и административните мерки, свързани със защитата на правата и свободите на физическите лица по отношение на обработването;

г) насърчава информираността на администраторите и обработващите лични данни за задълженията им по силата на настоящия регламент;

д) при поискване предоставя информация на всеки субект на данни във връзка с упражняването на правата му по силата на настоящия регламент и ако е необходимо, си сътрудничи за тази цел с надзорните органи в други държави членки;

е) разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение в съответствие с **член 80**, и разследва предмета на жалбата, доколкото това е целесъобразно, и информира жалбоподателя за напредъка и резултатите от разследването в разумен срок, особено ако е необходимо по-нататъшно разследване или координиране с друг надзорен орган;

ж) сътрудничи си с други надзорни органи, включително чрез обмен на информация и взаимопомощ, с оглед осигуряване на съгласувано прилагане и изпълнение на настоящия регламент;

з) извършва проучвания относно прилагането на настоящия регламент, включително въз

основа на информация, получена от друг надзорен или публичен орган;

и) наблюдава съответното развитие, по-специално в областта на информационните и комуникационни технологии и търговските практики, дотолкова доколкото то оказва влияние върху защитата на личните данни;

й) приема стандартните договорни клаузи, посочени в **член 28, параграф 8** и **член 46, параграф 2, буква г**);

к) съставя и поддържа списък във връзка с изискването за оценка на въздействието върху защитата на данните съгласно **член 35, параграф 4**;

л) дава становища по операциите за обработване на данни, посочени в **член 36, параграф 2**;

м) насърчава съставянето на кодекси за поведение съгласно **член 40** и предоставя становище и одобрява кодексите за поведение, които осигуряват достатъчно гаранции съгласно **член 40, параграф 5**;

н) насърчава създаването на механизми за сертифициране за защита на данните и на печати и маркировки за защита на данните съгласно **член 42, параграф 1**, и одобрява критериите за сертифициране съгласно **член 42, параграф 5**;

о) когато е приложимо, извършва периодичен преглед на сертификатите, издадени в съответствие с **член 42, параграф 7**;

п) изготвя и публикува критериите за акредитация на органите за наблюдение на кодексите за поведение съгласно **член 41** и на сертифициращите органи съгласно **член 43**;

р) извършва акредитацията на органите за наблюдение на кодексите за поведение съгласно **член 41** и на сертифициращите органи съгласно **член 43**;

с) дава разрешение за договорните клаузи и разпоредбите, посочени в **член 46, параграф 3**;

т) одобрява задължителните фирмени правила съгласно **член 47**;

у) допринася за дейностите на Комитета;

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

х) изпълнява други задачи, свързани със защитата на лични данни.

2. Всеки надзорен орган улеснява подаването на жалбите, посочени в параграф 1, буква е), чрез мерки като например 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 задачите от страна на всеки надзорен орган е безплатно за субекта на данни и — когато това е приложимо — за длъжностното лице за защита на данните.

4. Когато исканията са очевидно неоснователни или прекомерни, по-специално поради своята повторяемост, надзорният орган може да наложи разумна такса, основана на административните разходи, или да откаже да предприеме действия по искането. Надзорният орган носи тежестта на доказване на очевидно неоснователния или прекомерния характер на искането.

Член 58

Правомощия

1. Всеки надзорен орган има всички от посочените по-долу правомощия за разследване:

а) да разпорежда на администратора и на обработващия лични данни и, когато е приложимо — на представителя на администратора или 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 извършва преглед на сертификатите, издадени в съответствие с **член 42, параграф 7**;

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

д) 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;

е) да получава достъп до всички помещения на администратора и обработващия лични данни, включително до всяко оборудване и средство за обработване на данни, в съответствие с правото на Съюза или процесуалното право на държавата членка.

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

а) да отправя предупреждения до администратора или обработващия лични данни, когато има вероятност операции 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 разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;

г) 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;

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

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

ж) да разпорежда коригирането, или изтриването на лични данни или ограничаването на обработването им съгласно **членове 16**, **17** и **18**, както и уведомяването за тези действия на получатели, пред които личните данни са били разкрити съгласно **член 17, параграф 2** и **член 19**;

з) да отнема сертификат или да разпорежда на сертифициращия орган да отнеме сертификат, издаден съгласно **членове 42** и **43**, или да разпорежда на сертифициращия орган да не издава сертификат, ако изискванията за сертифицирането не са спазени или вече не се спазват;

и) да налага административно наказание „глоба“ или „имуществена санкция“ съгласно **член 83**, в допълнение към мерките, посочени в настоящия параграф, или вместо тях, в зависимост от особеностите на всеки отделен случай;

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

3. Всеки надзорен орган има всички от посочените по-долу правомощия да дава разрешения и становища:

а) да дава становища на администратора в съответствие с процедурата по предварителна консултация, посочена в **член 36**;

б) да издава по собствена инициатива или при поискване становища до националния парламент, правителството на държавата членка или, в съответствие с правото на държавата членка — до други институции и органи, както и до обществеността по всякакви въпроси, свързани със защитата на лични данни;

в) да дава разрешение за обработването, посочено в **член 36, параграф 5**, ако съгласно правото на държавата членка се изисква такова предварително разрешение;

г) да дава становища и да одобрява проекти на кодекси за поведение съгласно **член 40, параграф 5**;

д) да акредитира сертифициращи органи съгласно **член 43**;

е) да издава сертификати и да одобрява критериите за сертифициране в съответствие с **член 42, параграф 5**;

ж) да приема стандартните клаузи за защита на данните, посочени в **член 28, параграф 8** и в **член 46, параграф 2, буква г**);

з) да дава разрешение за договорните клаузи, посочени в **член 46, параграф 3, буква а**);

и) да дава разрешение за административните договорености, посочени в **член 46, параграф 3, буква б**);

й) да одобрява задължителните фирмени правила съгласно **член 47**.

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

5. Всяка държава членка урежда със закон нейният надзорен орган да има правомощието да довежда нарушенията на настоящия регламент до знанието на съдебните органи и по целесъобразност да инициира или по друг начин да участва в съдебни производства, с цел осигуряване на изпълнението на настоящия регламент.

6. Всяка държава членка може да урежда със закон нейният надзорен орган да има допълнителни правомощия освен посочените в параграфи 1, 2 и 3. Упражняването на тези правомощия не нарушава ефективното действие на глава VII.

Член 59

Доклади за дейността

Всеки надзорен орган изготвя годишен доклад за своята дейност, който може да включва списък на видовете нарушения, за които е бил уведомен и на видовете мерки, взети в съответствие с **член 58, параграф 2**. Тези доклади се предоставят на националния парламент, правителството и други органи, посочени в правото на държавата членка. До тях се осигурява достъп на обществеността, на Комисията, и на Комитета.

ГЛАВА 7
Сътрудничество и съгласуваност

РАЗДЕЛ 1
Сътрудничество

Член 60

Сътрудничество между водещия надзорен орган и другите засегнати надзорни органи

1. Водещият надзорен орган си сътрудничи с другите засегнати надзорни органи в съответствие с настоящия член и се стреми към постигането на консенсус. Водещият надзорен орган и засегнатите надзорни органи обменят всяка имаща отношение информация помежду си.

2. Водещият надзорен орган може да поиска по всяко време от другите засегнати надзорни органи да предоставят взаимопомощ съгласно **член 61** и може да провежда съвместни операции съгласно **член 62**, по-специално за да извършва разследвания или да наблюдава изпълнението на мярка, засягаща администратор или обработващ лични данни, установен в друга държава членка.

3. Водещият надзорен орган незабавно предава информация за това на другите засегнати надзорни органи. Водещият надзорен орган незабавно представя на другите засегнати надзорни органи проект за решение, за да получи тяхното становище и да вземе надлежно предвид вижданията им.

4. Ако някой от другите засегнати надзорни органи изрази относимо и обосновано възражение срещу проекта за решение в срок от четири седмици, след като е било поискано мнението му в съответствие с параграф 3 от настоящия член, водещият надзорен орган, в случай че не приема относимото и обосновано възражение или счита, че това възражение не е относимо или обосновано, отнася въпроса до механизма за съгласуваност, посочен в **член 63**.

5. Ако водещият надзорен орган възнамерява да приеме направено относимо и обосновано възражение, той изпраща на другите засегнати надзорни органи преработен проект за решението, за да получи тяхното становище. За този преработен проект на решението се следва процедурата, посочена в параграф 4, за срок от две седмици.

6. Когато нито един от другите засегнати органи не е възразил срещу проекта на решение, представен от водещия надзорен орган в посочения в параграфи 4 и 5 срок, се счита, че водещият надзорен орган и засегнатите надзорни органи са съгласни с този проект на решение и са обвързани от него.

7. Водещият надзорен орган приема решението и уведомява за него основното място на установяване или единственото място на установяване на администратора или обработващия лични данни, според случая, и информира другите засегнати надзорни органи и Комитета за въпросното решение, като включва резюме на съответните факти и основания. Надзорният орган, до когото е била подадена жалбата, информира жалбоподателя за решението.

8. Чрез дерогация от параграф 7, когато дадена жалба е оставена без разглеждане или отхвърлена, надзорният орган, до който е била подадена жалбата, приема решението и уведомява жалбоподателя за него, като информира и администратора

9. Когато водещият надзорен орган и засегнатите надзорни органи постигнат съгласие определени части от жалбата да бъдат оставени без разглеждане или отхвърлени, а по други части от тази жалба да се предприемат действия, за всяка от тези части се приема отделно решение. Водещият надзорен орган приема решението относно частта, за която се предприемат действия във връзка с администратора, уведомява за него основното място на установяване или единственото място на установяване на администратора или обработващия лични данни на територията на неговата държава членка и информира жалбоподателя за това, а надзорният орган по жалбата приема решението относно частта, с която е свързано оставянето без разглеждане или отхвърлянето на тази жалба, уведомява за него жалбоподателя и информира за това администратора или обработващия лични данни.

10. След като е бил уведомен за решението на водещия надзорен орган съгласно параграфи 7 и 9, администраторът или обработващият лични данни взема необходимите мерки, за да осигури съответствие с решението по отношение на дейностите по обработването на всички места, на които е установен в Съюза. Администраторът или обработващият лични данни уведомява водещия надзорен орган за мерките, взети с цел осигуряване на съответствие с решението, а водещият орган информира другите засегнати надзорни органи.

11. Когато при изключителни обстоятелства засегнат надзорен орган има основания да счита, че са необходими спешни действия, за да се защитят интересите на субекти на данни, се прилага процедурата по спешност по **член 66**.

12. Водещият надзорен орган и другите засегнати надзорни органи си предават информацията, изисквана съгласно настоящия член, по електронен път, използвайки стандартизиран формат.

Член 61

Взаимопомощ

1. Надзорните органи си предоставят взаимно значима информация и помощ, за да изпълняват и прилагат настоящия регламент по съгласуван начин, и въвеждат мерки за ефективно сътрудничество помежду си. Взаимопомощта обхваща по-специално искания за информация и мерки за надзор, например искания за предоставяне на предварителни разрешения или провеждане на предварителни консултации, проверки и разследвания.

2. Всеки надзорен орган предприема всички подходящи мерки, които са необходими, за да се отговори на искането на друг надзорен орган без ненужно забавяне и не по-късно от един месец след получаване на искането. Такива мерки могат да включват, по-специално, предаване на значима информация относно хода на дадено разследване.

3. Исканията за помощ съдържат цялата необходима информация, включително целта на искането и причините за него. Обменената информация се използва единствено за целите, за които е поискана.

4. Надзорен орган, до който е отправено искане, няма право да откаже да го изпълни, освен ако:

а) не е компетентен относно предмета на искането или мерките, които се изисква да изпълни; или

б) удовлетворяването на искането би било в нарушение на настоящия регламент или правото на Съюза или правото на държава членка, което се прилага спрямо надзорния орган, до който е отправено искането.

5. Надзорният орган, до който е отправено искането, информира искащия надзорен орган за резултатите или, в зависимост от случая, за напредъка на предприетите мерки в отговор на искането. Надзорният орган, до който е отправено искането, излага мотивите си в случай на отказ да

изпълни искането по силата на параграф 4.

6. Надзорните органи, до които са отправени искания, по правило предоставят информацията, поискана от други надзорни органи, по електронен път, като използват стандартизиран формат.

7. Надзорните органи, до които са отправени искания, не събират такси за действията, които са предприели в отговор на искане за взаимопомощ. Надзорните органи могат да постигнат съгласие с други надзорни органи относно правила за предоставяне на обезщетение един на друг за конкретни разходи, свързани с предоставянето на взаимопомощ при извънредни обстоятелства.

8. Когато в рамките на един месец от получаване на искането на друг надзорен орган надзорният орган не предостави информацията, посочена в параграф 5 от настоящия член, искащият надзорен орган може да приеме временна мярка на територията на своята държава членка в съответствие с **член 55, параграф 1**. В този случай се счита, че са необходими спешни действия съгласно **член 66, параграф 1**, което изисква спешно решение със задължителен характер от страна на Комитета в съответствие с **член 66, параграф 2**.

9. Комисията може посредством актове за изпълнение да определи формата и процедурите за взаимопомощ по настоящия член, както и договореностите за обмена на информация по електронен път между надзорните органи и между надзорните органи и Комитета, и по-специално стандартизирания формат, посочен в параграф 6 от настоящия член. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

Член 62

Съвместни операции на надзорни органи

1. Когато е целесъобразно, надзорните органи провеждат съвместни операции, включително съвместни разследвания и съвместни мерки за изпълнение, в които участват членове или персонал на надзорни органи от други държави членки.

2. Когато администраторът или обработващият лични данни е установен в няколко държави членки или когато има вероятност от операции по обработване на данни да бъдат засегнати съществено значителен брой субекти на данни в повече от една държава членка, надзорният орган на всяка от тези държави членки има право да участва в съвместни операции. Надзорният орган, който е компетентен съгласно **член 56, параграф 1 или параграф 4**, кани надзорния орган на всяка от тези държави членки да участва в съответните съвместни операции и отговаря незабавно на искането на даден надзорен орган за участие.

3. В съответствие с правото на държавата членка и с разрешението на командироващия надзорен орган надзорният орган може да предостави правомощия, в това число правомощия за разследване, на членовете или персонала на командироващия надзорен орган, участващи в съвместни операции, или, доколкото правото на държавата членка на надзорния орган домакин позволява, да разреши на членовете или персонала на командироващия надзорен орган да упражняват своите правомощия за разследване в съответствие с правото на държавата членка на командироващия надзорен орган. Тези правомощия за разследване могат да се упражняват единствено под

ръководството и в присъствието на членове или персонал на надзорния орган домакин. Спрямо членовете и персонала на командироващия надзорен орган се прилага правото на държавата членка на надзорния орган домакин.

4. Когато в съответствие с параграф 1 персонал на командироващ надзорен орган участва в операция в друга държава членка, държавата членка на надзорния орган домакин носи отговорност за действията на този персонал, включително отговорност за всякакви вреди, нанесени от него по време на операцията, в съответствие с правото на държавата членка, на чиято територия се провежда операцията.

5. Държавата членка, на чиято територия е нанесена вредата, поправя тази вреда при условията, приложими към вреди, нанесени от собствения ѝ персонал. Държавата членка на командироващия надзорен орган, чиито служители са причинили вреди на лице на територията на друга държава членка, възстановява изцяло сумите, които последната е изплатила от тяхно име на лицата, които са имали правото да ги получат.

6. Без да се засяга упражняването на правата ѝ по отношение на трети страни и с изключение на параграф 5, всяка държава членка се въздържа в случая, предвиден в параграф 1, да иска обезщетение от друга държава членка за вредите, посочени в параграф 4.

7. Когато се планира съвместна операция и в срок от един месец даден надзорен орган не изпълни задължението, предвидено във второто изречение на параграф 2 от настоящия член, другите надзорни органи могат да приемат временна мярка на територията на своята държава членка в съответствие с **член 55**. В този случай се счита, че са необходими спешни действия съгласно **член 66, параграф 1**, което изисква становище или спешно решение със задължителен характер от страна на Комитета в съответствие с **член 66, параграф 2**.

РАЗДЕЛ 2
Съгласуваност

Член 63

Механизъм за съгласуваност

С цел да допринесат за съгласуваното прилагане на настоящия регламент в целия Съюз, надзорните органи си сътрудничат помежду си и, ако е целесъобразно, с Комисията чрез механизъм за съгласуваност, както е определено в настоящия раздел.

Член 64

Становище на Комитета

1. Комитетът дава становище, когато компетентен надзорен орган възнамерява да приеме някоя от мерките, изброени по-долу. За тази цел компетентният надзорен орган предава проекта за решение на Комитета, когато то:

а) има за цел приемане на списък на операциите по обработване, които подлежат на изискването за оценка на въздействието по отношение на защитата на лични данни в съответствие с **член 35, параграф 4**;

б) се отнася до въпрос съгласно **член 40, параграф 7** дали проект на кодекс на поведение, негово изменение или допълнение съответства на настоящия регламент;

в) има за цел одобряване на критериите за акредитиране на орган съгласно **член 41, параграф 3** или на орган по сертифициране съгласно **член 43, параграф 3**;

г) има за цел определяне на стандартните клаузи за защита на данните, посочени в **член 46, параграф 2, буква г**) и в **член 28, параграф 8**;

д) има за цел даване на разрешение за договорните клаузи, посочени в **член 46, параграф 3, буква а**); или

е) има за цел одобряване на задължителни фирмени правила по смисъла на **член 47**.

2. Всеки надзорен орган, председателят на Комитета или Комисията може да поиска разглеждането на въпрос с общо приложение или с последици в повече от една държава членка от Комитета с цел получаване на становище, по-специално когато даден компетентен надзорен орган не изпълнява задълженията за взаимопомощ съгласно **член 61** или за съвместни операции съгласно **член 62**.

3. В случаите, посочени в параграфи 1 и 2, Комитетът дава становище по отнесения до него въпрос, при условие че все още не е давал становище по същия въпрос. Това становище се приема в срок от осем седмици с обикновено мнозинство от членовете на Комитета. Този срок може да бъде удължен с още шест седмици с оглед на сложността на въпроса. По отношение на посочения в параграф 1 проект за решение, разпространен до членовете на Комитета в съответствие с параграф 5, за член, който не е представил възражение в посочения от председателя разумен срок, се счита, че е съгласен с проекта за решение.

4. Надзорните органи и Комисията предоставят без ненужно забавяне на Комитета, по електронен път и посредством стандартизиран формат, всяка информация, която е от значение, включително, според случая, обобщение на фактите, проекта за решение, основанията, които налагат приемането на такава мярка, и становищата на други засегнати надзорни органи.

5. Председателят на Комитета без ненужно забавяне информира по електронен път:

а) членовете на Комитета и Комисията за всяка значима информация, която му е била съобщена, като използва стандартизиран формат. При необходимост секретариатът на Комитета предоставя писмен превод на съответната информация; и

б) надзорния орган, посочен, според случая, в параграфи 1 и 2, и Комисията за становището и го оповестява публично.

6. Компетентният надзорен орган не приема проекта си за решение по параграф 1 в

рамките на посочения в параграф 3 срок.

7. Надзорният орган, посочен в параграф 1, в най-голяма степен взема предвид становището на Комитета и в срок от две седмици след получаване на становището информира председателя на Комитета по електронен път дали ще запази или ще измени своя проект за решение и му представя изменения проект за решение, ако има такъв, като използва стандартизиран формат.

8. Когато засегнатият надзорен орган информира председателя на Комитета в посочения в параграф 7 от настоящия член срок, че възнамерява изцяло или отчасти да не се съобрази със становището на Комитета, като представи съответните основания, се прилага **член 65, параграф 1**.

Член 65

Разрешаване на спорове от Комитета

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

а) когато в случаи по **член 60, параграф 4** засегнат надзорен орган е повдигнал относимо и обосновано възражение срещу проект за решение на водещия орган или водещият орган е отхвърлил възражението като неотносимо или необосновано. Решението със задължителен характер се отнася за всички въпроси, които са предмет на относимото и обосновано възражение, особено когато има нарушение на настоящия регламент;

б) когато има противоречиви виждания за това кой от засегнатите надзорни органи е компетентен за основното място на установяване;

в) когато компетентният надзорен орган не е поискал становището на Комитета в случаите, посочени в **член 64, параграф 1**, или не се е съобразил със становището на Комитета, дадено по член 564. В този случай всеки засегнат надзорен орган или Комисията може да отнесе въпроса до Комитета.

2. Посоченото в параграф 1 решение се приема в срок от един месец от отнасянето на въпроса от мнозинство от две трети от членовете на Комитета. Посоченият срок може да бъде удължен с още един месец с оглед на сложността на въпроса. Решението по параграф 1 е обосновано, адресирано е до водещия надзорен орган и всички засегнати надзорни органи и е със задължителен характер за тях.

3. Когато Комитетът не е бил в състояние да приеме решение в срока, посочен в параграф 2, той приема решението си в срок от две седмици от изтичането на втория месец, споменат в параграф 2, с обикновено мнозинство от членовете на Комитета. Когато членовете на Комитета са разделени поравно на две, решението се приема с решаващия глас на председателя.

4. Засегнатите надзорни органи не приемат решение по отнесения до Комитета въпрос съгласно параграф 1 в рамките на сроковете, посочени в параграфи 2 и 3.

5. Председателят на Комитета уведомява без ненужно забавяне засегнатите надзорни

органи за решението, посочено в параграф 1. Той уведомява и Комисията за него. Решението се публикува на уебсайта на Комитета без забавяне след като надзорният орган е уведомил за окончателното си решение, посочено в параграф 6.

6. Водещият надзорен орган или, според случая, надзорният орган, до който е била подадена жалбата, приема окончателното си решение въз основа на решението, посочено в параграф 1 от настоящия член, без ненужно забавяне и най-късно един месец след като Комитетът е уведомил за решението си. Водещият надзорен орган или, според случая, надзорният орган, до който е била подадена жалбата, информира Комитета за датата, на която администраторът или обработващият лични данни и субектът на данни са били уведомени за неговото окончателно решение. Окончателното решение на засегнатите надзорни органи се приема по реда на **член 60**, параграфи 7, 8 и 9. Окончателното решение се позовава на решението, посочено в параграф 1 от настоящия член, и в него се уточнява, че посоченото в посочения параграф решение ще бъде публикувано на уебсайта на Комитета в съответствие с параграф 5 от настоящия член. Към окончателното решение се прилага решението, посочено в параграф 1 от настоящия член.

Член 66

Процедура по спешност

1. При извънредни обстоятелства, когато засегнат надзорен орган счита, че е налице спешна необходимост да се действа в защита на правата и свободите на субектите на данни, той може чрез дерогация от механизма за съгласуваност, предвиден в **членове 63**, **64** и **65**, или процедурата, предвидена в **член 60**, да приеме незабавно временни мерки, водещи до правни последици на собствената му територия, с определен срок на валидност, който не надвишава три месеца. Надзорният орган съобщава незабавно тези мерки и мотивите за приемането им на другите засегнати надзорни органи, на Комитета и на Комисията.

2. Когато надзорен орган е предприел мярка съгласно параграф 1 и счита, че е необходимо спешно да бъдат приети окончателни мерки, той може да поиска от Комитета спешно становище или спешно решение със задължителен характер, като изтъкне причини за искането на такова становище или решение.

3. Всеки надзорен орган може да поиска спешно становище или спешно решение със задължителен характер, според случая, от Комитета, когато компетентен надзорен орган не е предприел подходящи мерки в ситуация, в която е налице спешна необходимост от предприемане на действия с цел защита на правата и свободите на субектите на данни, като посочи причините за искането на такова становище или решение, както и за спешната нужда от предприемане на действия.

4. Чрез дерогация от **член 64, параграф 3** и **член 65, параграф 2**, в срок от две седмици с обикновено мнозинство от членовете на Комитета се приема спешно становище или спешно решение със задължителен характер, както са посочени в параграфи 2 и 3 от настоящия член.

Член 67

Обмен на информация

Комисията може да приема актове за изпълнение с общ обхват за да уточни договореностите за обмен на информация по електронен път между надзорните органи, както и между надзорните органи и Комитета, по-специално стандартизирания формат, посочен в **член 64**.

Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в **член 93, параграф 2**.

РАЗДЕЛ 3
Европейски комитет по защита на данните

Член 68

Европейски комитет по защита на данните

1. Създава се Европейски комитет по защита на данните („Комитетът“), който е орган на Съюза и притежава правосубектност.

2. Комитетът се представлява от своя председател.

3. Комитетът е съставен от ръководителите на по един надзорен орган от всяка държава членка и Европейския надзорен орган по защита на данните, или от съответните им представители.

4. Когато в дадена държава членка повече от един надзорен орган отговаря за наблюдението на прилагането на разпоредбите съгласно настоящия регламент, в съответствие с правото на тази държава членка се назначава общ представител.

5. Комисията има право да участва в дейностите и заседанията на Комитета без право на глас. Комисията посочва свой представител. Председателят на Комитета уведомява Комисията за дейностите на Комитета.

6. В случаите, посочени с **член 65**, Европейският надзорен орган по защита на данните има право на глас само във връзка с решения, които се отнасят до принципите и правилата, приложими за институциите, органите, службите и агенциите на Съюза, които съответстват по същество на предвидените в настоящия регламент.

Член 69

Независимост

1. Комитетът действа независимо при изпълнението на задачите си или упражняването на правомощията си съгласно **членове 70** и **71**.

2. Без да се засягат исканията на Комисията, посочени в **член 70, параграф 1, буква б**) и **член 70, параграф 2**, Комитетът не търси и не приема указания от никого при изпълнението на

своите задачи или упражняването на своите правомощия.

Член 70

Задачи на Комитета

1. Комитетът осигурява съгласуваното прилагане на настоящия регламент. За тази цел Комитетът по своя собствена инициатива или, ако е целесъобразно, по искане на Комисията, по-специално:

а) наблюдава и гарантира правилното прилагане на настоящия регламент в случаите, предвидени в **членове 64** и **65**, без да се засягат задачите на националните надзорни органи;

б) консултира Комисията по всеки въпрос, свързан със защитата на личните данни в Съюза, включително относно всяко предложено изменение на настоящия регламент;

в) консултира Комисията относно формàта и процедурите за обмен на информация между администраторите, обработващите лични данни и надзорните органи за задължителните фирмени правила;

г) издава насоки, препоръки и най-добри практики относно процедурите за изтриване на връзки, копия или преписи на лични данни от обществено достъпни съобщителни услуги, както е посочено в **член 17, параграф 2**;

д) разглежда по своя собствена инициатива, по искане на някой от своите членове или по искане на Комисията всеки въпрос, който се отнася до прилагането на настоящия регламент, и издава насоки, препоръки и най-добри практики с цел насърчаване на съгласуваното прилагане на настоящия регламент;

е) издава насоки, препоръки и най-добри практики в съответствие с буква д) от настоящия параграф за допълнително уточняване на критериите и условията във връзка с решенията, основани на профилиране на данни съгласно **член 22, параграф 2**;

ж) издава насоки, препоръки и най-добри практики в съответствие с буква д) от настоящия параграф за установяване на нарушения на сигурността на данните и определяне на ненужното забавяне по **член 33**, параграфи 1 и 2, както и за определяне на конкретните обстоятелства, при които от администратора или обработващия лични данни се изисква да уведомяват за нарушението на сигурността на личните данни;

з) издава насоки, препоръки и най-добри практики в съответствие с буква д) от настоящия параграф по отношение на обстоятелствата, при които нарушение на сигурността на личните данни има вероятност да доведе до висок риск за правата и свободите на физическите лица, посочени в **член 34, параграф 1**;

и) издава насоки, препоръки и най-добри практики в съответствие с буква д) от настоящия параграф за целите на допълнително уточняване на критериите и изискванията за предаване на лични данни въз основа на задължителни фирмени правила, които се спазват от

администраторите, и задължителни фирмени правила, които се спазват от обработващите лични данни, както и на необходимите допълнителни изисквания за осигуряване на защита на личните данни на съответните субекти на данни, посочени в **член 47**;

й) издава насоки, препоръки и най-добри практики в съответствие с буква д) от настоящия параграф за целите на допълнително уточняване на критериите и изискванията за предаване на лични данни въз основа на **член 49, параграф 1**;

к) изготвя насоки за надзорните органи относно прилагането на мерките, посочени в **член 58**, параграфи 1, 2 и 3, и определянето на размера на административните наказания „глоба“ или „имуществена санкция“ съгласно **член 83**;

л) извършва преглед на практическото прилагане на насоките, препоръките и най-добрите практики, посочени в букви д) и е);

м) издава насоки, препоръки и най-добри практики в съответствие с буква д) от настоящия параграф за установяване на общи процедури за подаване на сигнали от физически лица за нарушения на настоящия регламент съгласно **член 54, параграф 2**;

н) насърчава изготвянето на кодекси на поведение и установяването на механизми за сертифициране за защита на данните и печати и маркировки за защита на данните съгласно **членове 40** и **42**;

о) извършва акредитацията на сертифициращи органи и периодичния ѝ преглед съгласно **член 43** и поддържа публичен регистър на акредитираните органи съгласно **член 43, параграф 6** и на акредитираните администратори и обработващи лични данни, установени в трети държави, съгласно **член 42, параграф 7**;

п) уточнява изискванията, посочени в **член 43, параграф 3**, с оглед на акредитацията на сертифициращи органи съгласно **член 42**;

р) предоставя на Комисията становище относно изискванията за сертифициране, посочени в **член 43, параграф 8**;

с) предоставя на Комисията становище относно иконите, посочени в **член 12, параграф 7**;

т) предоставя на Комисията становище за оценка на адекватността на нивото на защита на данните в трета държава или международна организация, включително за оценка на това дали третата държава, територията или един или повече конкретни сектори в рамките на тази трета държава, или международната организация, са престанали да осигуряват адекватно ниво на защита. За тази цел Комисията предоставя на Комитета цялата необходима документация, включително кореспонденцията с правителството на третата държава, по отношение на тази трета държава, територия или конкретен сектор или с международната организация;

у) дава становища по проекти за решения на надзорните органи по силата на механизма за съгласуваност, посочен в **член 64, параграф 1**, по въпроси, изпратени съгласно **член 64, параграф 2** и приема решения със задължителен характер съгласно **член 65**, включително по

въпроси, разглеждани съгласно **член 66**;

ф) насърчава сътрудничеството и ефективния двустранен и многостранен обмен на информация и добрите практики между надзорните органи;

х) насърчава общите програми за обучение и улеснява обмена на персонал между надзорните органи и — когато това е целесъобразно —с надзорните органи на трети държави или международни организации;

ц) насърчава обмена на знания и документация относно законодателството и практиките в областта на защитата на данни с надзорните органи по защита на данните в цял свят;

ч) дава становища по кодексите за поведение, съставяни на равнището на Съюза в съответствие с **член 40, параграф 9**; и

ш) поддържа обществено достъпен електронен регистър на решенията, взети от надзорните органи и съдилищата по въпроси, разглеждани в рамките на механизма за съгласуваност.

2. Когато Комисията поиска съвет от Комитета, тя може да посочи срок, като се взема предвид спешността на въпроса.

3. Комитетът изпраща своите становища, насоки, препоръки и най-добри практики на Комисията и на комитета, посочен в **член 93**, и ги прави обществено достояние.

4. Комитетът се консултира по целесъобразност със заинтересованите страни и им предоставя възможност да направят коментари в рамките на разумен срок. Без да се засягат разпоредбите на **член 76**, Комитетът оповестява публично резултатите от процедурата на консултации.

Член 71

Доклади

1. Комитетът изготвя годишен доклад относно защитата на физическите лица по отношение на обработването в Съюза и, когато е от значение — в трети държави и международни организации. Докладът се оповестява публично и се предава на Европейския парламент, на Съвета и на Комисията.

2. В годишния доклад се включва преглед на практическото прилагане на насоките, препоръките и най-добрите практики, посочени в **член 70, параграф 1, буква л**), както и на решенията със задължителен характер, посочени в **член 65**.

Член 72

Процедура

1. Комитетът взема решения с обикновено мнозинство на членовете си, освен ако не е

предвидено друго в настоящия регламент.

2. Комитетът приема свой процедурен правилник с мнозинство от две трети от своите членове и определя своите методи на работа.

Член 73

Председател

1. Комитетът избира с обикновено мнозинство председател и двама заместник-председатели измежду своите членове.

2. Мандатът на председателя и на заместник-председателите е пет години и може да бъде подновяван еднократно.

Член 74

Задачи на председателя

1. Председателят има следните задачи:

а) да свиква заседанията на Комитета и да изготвя дневния ред;

б) да уведомява водещия надзорен орган и засегнатите надзорни органи за решенията, приети от Комитета съгласно член 58а;

в) да осигурява своевременното изпълнение на задачите на Комитета, по-специално във връзка с механизма за съгласуваност, посочен в **член 63**.

2. Комитетът определя разпределението на задачите между председателя и заместник-председателите в своя процедурен правилник.

Член 75

Секретариат

1. Комитетът разполага със секретариат, който се осигурява от Европейския надзорен орган по защита на данните.

2. Секретариатът изпълнява задачите си изключително под ръководството на председателя на Комитета.

3. Служителите на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачи, възложени на Комитета с настоящия регламент, са организационно отделени от служителите, участващи в изпълнението на задачи, възложени на Европейския надзорен орган по защита на данните.

4. Когато е целесъобразно, Комитетът и Европейският надзорен орган по защита на данните изготвят и публикуват меморандум за разбирателство за прилагане на настоящия член, в който се определят условията за сътрудничеството помежду им и който се прилага за служителите на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачи, възложени на Комитета с настоящия регламент.

5. Секретариатът предоставя аналитична, административна и логистична подкрепа на Комитета.

6. Секретариатът отговаря по-специално за:

а) ежедневната работа на Комитета;

б) комуникацията между членовете на Комитета, неговия председател и Комисията;

в) комуникацията с други институции и с обществеността;

г) използването на електронни средства за вътрешна и външна комуникация;

д) превода на значима информация;

е) подготовката на заседанията на Комитета и последващите действия във връзка с тях;

ж) подготовката, изготвянето и публикуването на становища, решения относно уреждането на спорове между надзорни органи и други текстове, приети от Комитета.

Член 76

Поверителност

1. Обсъжданията на Комитета са поверителни, когато Комитетът счита това за необходимо, както е посочено в процедурния му правилник.

2. Достъпът до документи, предоставени на членове на Комитета, експерти и представители на трети страни, се урежда с **Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета**(**21**).

ГЛАВА 8
Средства за правна защита, отговорност за причинени вреди и санкции

Член 77

Право на подаване на жалба до надзорен орган

1. Без да се засягат които и да било други административни или съдебни средства за

правна защита, всеки субект на данни има право да подаде жалба до надзорен орган, по-специално в държавата членка на обичайно местопребиваване, място на работа или място на предполагаемото нарушение, ако субектът на данни счита, че обработването на лични данни, отнасящи се до него,нарушава разпоредбите на настоящия регламент.

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

Член 78

Право на ефективна съдебна защита срещу надзорен орган

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

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

3. Производствата срещу надзорен орган се образуват пред съдилищата на държавата членка, в която е установен надзорният орган.

4. Когато се образува производство срещу решението на надзорен орган, което е било предхождано от становище или решение на Комитета в съответствие с механизма за съгласуваност, надзорният орган предава това становище или решение на съда.

Член 79

Право на ефективна съдебна защита срещу администратор или обработващ лични данни

1. Без да се засягат които и да било налични административни или несъдебни средства за защита, включително правото на подаване на жалба до надзорен орган съгласно **член 77**, всеки субект на данни има право на ефективна съдебна защита, когато счита, че правата му по настоящия регламент са били нарушени в резултат на обработване на личните му данни, което не е в съответствие с настоящия регламент.

2. Производствата срещу даден администратор или обработващ лични данни се образуват пред съдилищата на държавата членка, в която администраторът или обработващият лични данни има място на установяване. Като алтернативен вариант такива производства могат да се образуват пред съдилищата на държавата членка, в която субектът на данните има обичайно местопребиваване, освен ако администраторът или обработващият лични данни е публичен орган на държава членка, действащ в изпълнение на публичните си правомощия.

Член 80

Представителство на субектите на данни

1. Субектът на данни има право да възложи на структура, организация или сдружение с нестопанска цел, което е надлежно учредено в съответствие с правото на държава членка,, има уставни цели, които са в обществен интерес и действа в областта на защитата на правата и свободите на субекта на данни по отношение на защитата на неговите лични данни, да подаде жалба от негово име и да упражни от негово име правата по **членове 77**, **78** и **79**, както и правото на обезщетение по **член 82**, когато то е предвидено в правото на държавата членка.

2. Държавите членки могат да предвидят всяка структура, организация и сдружение по параграф 1 от настоящия член, независимо от възложения от субекта на данни мандат, да има право да подаде в съответната държава членка жалба до надзорния орган, който е компетентен съгласно **член 73**, и да упражни правата по **членове 78** и **79**, ако счита, че правата на субект на данни съгласно настоящия регламент са били нарушени в резултат на обработването на лични данни.

Член 81

Прекратяване на производството

1. Когато компетентен съд на държава членка има информация, че производство, засягащо същия въпрос по отношение на обработване от същия администратор или обработващ лични данни, е висящо пред съд на друга държава членка, той установява контакт със съда в другата държава членка, за да потвърди наличието на такова производство.

2. Когато производство, засягащо същия въпрос по отношение на обработване от същия администратор или обработващ личните данни е висящо пред съд на друга държава членка, всеки компетентен съд, освен първия сезиран съд, може да преустанови производството, което води.

3. Когато тези производства са висящи пред първоинстанционни съдилища, всеки съд, освен първия сезиран съд, може също да се откаже от компетентност по молба на една от страните, при условие че първият сезиран съд е компетентен по отношение на въпросните искове и правото му допуска тяхното съединяване.

Член 82

Право на обезщетение и отговорност за причинени вреди

1. Всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на настоящия регламент, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди.

2. Администраторът, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава настоящия регламент. Обработващият лични данни носи отговорност за вреди, произтичащи от извършеното обработване,

само когато не е изпълнил задълженията по настоящия регламент, конкретно насочени към обработващите лични данни, или когато е действал извън законосъобразните указания на администратора или в противоречие с тях.

3. Администраторът или обработващият лични данни се освобождава от отговорност съгласно параграф 2, ако докаже, че по никакъв начин не е отговорен за събитието, причинило вредата.

4. Когато в една и съща операция по обработване участват повече от един администратор или обработващ лични данни или участват и администратор, и обработващ лични данни, и когато те са отговорни по параграфи 2 и 3 за вреда, причинена от обработването, всеки администратор или обработващ лични данни носи отговорност за цялата вреда, за да се гарантира действително обезщетение на субекта на данни.

5. Когато администратор или обработващ лични данни е изплатил съгласно параграф 4 пълното обезщетение за причинената вреда, той има право да поиска от другите администратори или обработващи лични данни, участвали в същата операция по обработване на лични данни, да му възстановят част от платеното обезщетение, съответстваща на тяхната част от отговорността за причинената вреда в съответствие с условията по параграф 2.

6. Съдебните производства във връзка с упражняването на правото на обезщетение се образуват пред съдилища, компетентни съгласно правото на държавата членка, посочена в **член 79, параграф 2**.

Член 83

Общи условия за налагане на административни наказания „глоба“ или „имуществена санкция“

1. Всеки надзорен орган гарантира, че наложените административни наказания „глоба“ или „имуществена санкция“ в съответствие с настоящия член за извършени нарушения на настоящия регламент, посочени в параграфи 4, 5 и 6, във всеки конкретен случай са ефективни, пропорционални и възпиращи.

2. В зависимост от обстоятелствата във всеки конкретен случай административните наказания „глоба“ или „имуществена санкция“ се налагат в допълнение към мерките, посочени в **член 58, параграф 2**, букви а)—з) и й), или вместо тях. Когато се взема решение дали да бъде наложено административно наказание „глоба“ или „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) дали нарушението е извършено умишлено или по небрежност;

в) действията, предприети от администратора или обработващия лични данни за

смекчаване на последиците от вредите, претърпени от субектите на данни;

г) степента на отговорност на администратора или обработващия лични данни като се вземат предвид технически и организационни мерки, въведени от тях в съответствие с **членове 25** и **32**;

д) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни;

е) степента на сътрудничество с надзорния орган с цел отстраняване на нарушението и смекчаване на евентуалните неблагоприятни последици от него;

ж) категориите лични данни, засегнати от нарушението;

з) начина, по който нарушението е станало известно на надзорния орган, по-специално дали и до каква степен администраторът или обработващият лични данни е уведомил за нарушението;

и) когато на засегнатия администратор или обработващ лични данни преди са налагани мерки, посочени в **член 58, параграф 2**, във връзка със същия предмет на обработването, дали посочените мерки са спазени;

й) придържането към одобрени кодекси на поведение съгласно **член 40** или одобрени механизми за сертифициране съгласно **член 42**; и

к) всякакви други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая, като пряко или косвено реализирани финансови ползи или избегнати загуби вследствие на нарушението.

3. Ако администратор или обработващ лични данни умишлено или по небрежност наруши няколко разпоредби на настоящия регламент при една и съща операция по обработване или при свързани операции, общият размер на административната глоба или имуществената санкция не може да надвишава сумата, определена за най-тежкото нарушение.

4. Нарушенията на посочените по-долу разпоредби подлежат, в съответствие с параграф 2, на административно наказание „глоба“ или „имуществена санкция“ в размер до 10 000 000 EUR или, в случай на предприятие — до 2 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока:

а) задълженията на администратора и обработващия лични данни съгласно **членове 8**, **11**, **25—39** и **42** и **43**;

б) задълженията на сертифициращия орган съгласно **членове 42** и **43**;

в) задълженията на органа за наблюдение съгласно **член 41, параграф 4**.

5. Нарушенията на посочените по-долу разпоредби подлежат, в съответствие с параграф 2, на административно наказание „глоба“ или „имуществена санкция“ в размер до 20 000 000 EUR

или, в случай на предприятие — до 4 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока:

а) основните принципи за обработване на лични данни, включително условията, свързани с даването на съгласие, в съответствие с **членове 5**, **6**, **7** и **9**;

б) правата на субектите на данни съгласно **членове 12—22**;

в) предаването на лични данни на получател в трета държава или международна организация съгласно **членове 44—49**;

г) всички задължения, произтичащи от правото на държавите членки, приети съгласно глава IX;

д) неспазване на разпореждане, или на временно или окончателно ограничаване във връзка с обработването или на наложено от надзорния орган преустановяване на потоците от данни съгласно **член 58, параграф 2** или непредоставяне на достъп в нарушение на **член 58, параграф 1**.

6. Неспазването на разпореждане на надзорния орган, както е посочено в **член 58, параграф 2**, подлежи, в съответствие с параграф 2 от настоящия член, на административно наказание „глоба“ или „имуществена санкция“ в размер до 20 000 000 EUR или, в случай на предприятие — до 4 % от общия му годишен световен оборот за предходната финансова година, която от двете суми е по-висока.

7. Без да се засягат корективните правомощия на надзорните органи съгласно **член 58, параграф 2**, всяка държава членка може да определя правила за това дали и до каква степен могат да бъдат налагани административни наказания „глоба“ или „имуществена санкция“ на публични органи и структури, установени в тази държава членка.

8. Упражняването от надзорния орган на правомощията му по настоящия член зависи от съответните процедурни гаранции в съответствие с правото на Съюза и правото на държавата членка, включително ефективна съдебна защита и справедлив съдебен процес.

9. Когато в правната система на държавата членка не са предвидени административни наказания „глоба“ или „имуществена санкция“, настоящият член може да се прилага по такъв начин, че глобата да се инициира от компетентния назорен орган и да се налага от компетентните национални съдилища, като в същото време се гарантира, че тези правни средства за защита са ефективни и имат ефект, равностоен на административните наказания „глоба“ или „имуществена санкция“, налагани от надзорните органи. Във всички случаи наложените глоби или имуществени санкции са ефективни, пропорционални и възпиращи. Посочените държави членки уведомяват Комисията за разпоредбите в правото си, които примат съгласно настоящия параграф, най-късно до 25 май 2018 г., и я уведомяват незабавно за всеки последващ закон за изменение или за всяко изменение, които ги засягат.

Член 84

Санкции

1. Държавите членки определят правила за други санкции, приложими за нарушения на настоящия регламент по-специално за нарушения, които не подлежат на административно наказание „глоба“ или „имуществена санкция“ съгласно **член 83**, и вземат всички необходими мерки за гарантиране на тяхното прилагане. Тези санкции са ефективни, пропорционални и възпиращи.

2. Всяка държава членка уведомява Комисията за тези разпоредби в своето право, които приема съгласно параграф 1 до 25 май 2018 г., и я уведомява незабавно за всяко последващо, свързано с тях изменение.

ГЛАВА 9
Разпоредби, свързани с особени ситуации на обработване

Член 85

Обработване и свобода на изразяване и информация

1. Държавите членки съгласуват със закон правото на защита на личните данни в съответствие с настоящия регламент с правото на свобода на изразяване и информация, включително обработването за журналистически цели и за целите на академичното, художественото или литературното изразяване.

2. За обработването, извършвано за журналистически цели и за целите на академичното, художественото или литературното изразяване, държавите членки предвиждат изключения или дерогации от глава II (принципи), глава III (права на субекта на данни), глава IV (администратор и обработващ лични данни), глава V (предаване на лични данни на трети държави и международни организации), глава VI (независими надзорни органи), глава VII (сътрудничество и съгласуваност) и глава IX (особени ситуации на обработване на данни), ако те са необходими за съгласуване на правото на защита на личните данни със свободата на изразяване и информация.

3. Всяка държава членка уведомява Комисията за разпоредбите в правото си, които е приела съгласно параграф 2, и я уведомява незабавно за всеки последващ закон за изменение или за всяко изменение, които ги засягат.

Член 86

Обработване и публичен достъп до официални документи

Лични данни в официални документи, държани от публичен орган или публична или частна структура за изпълнение на задача от обществен интерес могат да бъдат разкривани от този орган или структура в съответствие с правото на Съюза или правото на държавата членка, на което се подчинява публичният орган или структура, за да се съгласува публичният достъп до официални документи с правото на защита на личните данни в съответствие с настоящия регламент.

Член 87

Обработване на националния идентификационен номер

Държавите членки могат да определят и специалните условия за обработване на национален идентификационен номер или на всякакъв друг идентификатор с общо приложение. В този случай националният идентификационен номер и всеки друг идентификатор с общо приложение се използват само при подходящи гаранции за правата и свободите на субекта на данните в съответствие с настоящия регламент.

Член 88

Обработване в контекста на трудово или служебно правоотношение

1. Държавите членки могат със закон или с колективни споразумения да предвидят по-конкретни правила, за да гарантират защитата на правата и свободите по отношение на обработването на личните данни на наетите лица по трудово ли служебно правоотношение, по-специално за целите на набирането на персонал, изпълнението на трудовия договор, включително изпълнението на задълженията, установени със закон или с колективни споразумения, управлението, планирането и организацията на работата, равенството и многообразието на работното място, здравословните и безопасни условия на труд, защитата на имуществото на работодателя или на клиента, както и за целите на упражняване и ползване на индивидуална или колективна основа на правата и облагите от заетостта, а също и за целите на прекратяване на трудовото или служебното правоотношение.

2. Тези правила включват подходящи и конкретни мерки за защита на човешкото достойнство, законните интереси и основните права на субекта на данните, по-специално по отношение на прозрачността на обработването, предаването на лични данни в рамките на група предприятия или група дружества, участващи в съвместна стопанска дейност и системите за наблюдение на работното място.

3. Всяка държава членка уведомява Комисията за тези разпоредби в своето право, които приема съгласно параграф 1 до 25 май 2018 г., и я уведомява незабавно за всяко последващо, свързано с тях изменение.

Член 89

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

1. 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 могат 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.

2. Когато личните данни се обработват за научни или исторически изследвания или за статистически цели, правото на Съюза или правото на държава членка може да предвижда дерогации от правата по **членове 15**, **16**, **18** и **21** съобразно условията и гаранциите по параграф 1 от настоящия член, 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.

3. Когато личните данни се обработват за целите на архивирането в обществен интерес, правото на Съюза или правото на държава членка може да предвижда дерогации от правата по **членове 15**, **16**, **18**, **19**, **20** и **21** съобразно условията и гаранциите по параграф 1 от настоящия член, 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 обработването по параграфи 2 и 3 служи едновременно за друга цел, дерогациите се прилагат единствено за обработване, извършвано за посочените в тези параграфи цели.

Член 90

Задължения за опазване на тайна

1. Държавите членки могат да приемат специални правила, за да установят правомощията на надзорните органи съгласно **член 58, параграф 1**, букви д) и е) по отношение на администраторите или обработващите лични данни, които по силата на правото на Съюза или правото на държава членка или на правила, установени от компетентните национални органи, са обвързани със задължение за опазване на професионална тайна или с други равностойни задължения за опазване на тайна, когато това е необходимо и пропорционално за съчетаване на правото на защита на личните данни със задължението за опазване на тайна. Тези правила се прилагат само по отношение на лични данни, които администраторът или обработващият лични данни е получил в хода на дейност, подлежаща на това задължение за опазване на тайна.

2. Всяка държава членка уведомява Комисията за правилата, приети съгласно параграф 1, до 25 май 2018 г., и я уведомява незабавно за всяко последващо, свързано с тях изменение.

Член 91

Съществуващи правила на църкви и религиозни сдружения за защита на данните

1. Когато в дадена държава членка към момента на влизане в сила на настоящия регламент църкви и религиозни сдружения или общности прилагат цялостни правила по отношение на защитата на физическите лица във връзка с обработването, тези съществуващи правила могат да продължат да се прилагат, при условие че са приведени в съответствие с настоящия регламент.

2. Църквите и религиозните сдружения, които прилагат цялостни правила в съответствие

с параграф 1 от настоящия член, подлежат на контрол от страна на независим надзорен орган, който може да е специален, при условие че изпълнява условията, предвидени в глава VI от настоящия регламент.

ГЛАВА 10
Делегирани актове и актове за изпълнение

Член 92

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Делегирането на правомощия, посочено в **член 12, параграф 8** и **член 43, параграф 8**, се предоставя на Комисията за неопределен срок, считано от 24 май 2016 г.

3. Делегирането на правомощия, посочено в **член 12, параграф 8** и **член 43, параграф 8**, може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за отмяна се прекратява посоченото в него делегиране на правомощия. То поражда действие в деня след публикуването му в Официален вестник на Европейския съюз или на по-късна, посочена в решението дата. То не засяга действителността на делегираните актове, които вече са в сила.

4. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и на Съвета.

5. Делегиран акт, приет съгласно **член 12, параграф 8** и **член 43, параграф 8**, влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от три месеца от нотифицирането за акта на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Този срок се удължава с три месеца по инициатива на Европейския парламент или на Съвета.

Член 93

Процедура на комитет

1. Комисията се подпомага от комитет. 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**.

3. При позоваване на настоящия параграф се прилага **член 8 от Регламент (ЕС) № 182/2011** във връзка с член 5 от него.

ГЛАВА 11
Заключителни разпоредби

Член 94

Отмяна на **Директива 95/46/ЕО**

1. **Директива 95/46/ЕО** се отменя, считано от 25 май 2018 г.

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

Член 95

Връзка с **Директива 2002/58/ЕО**

Настоящият регламент не налага допълнителни задължения на физическите или юридическите лица по отношение на обработването във връзка с предоставянето на обществено достъпни електронни съобщителни услуги в обществени съобщителни мрежи в Съюза, по отношение на въпроси, за които са им наложени специални задължения със същата цел, установени в **Директива 2002/58/ЕО**.

Член 96

Връзка с по-рано сключени споразумения

Международните споразумения, включващи предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди 24 май 2016 г и са съобразени с правото на Съюза като приложими преди посочената дата, остават в сила, докато не бъдат изменени, заменени или отменени.

Член 97

Доклади на Комисията

1. До 25 май 2020 г. и на всеки четири години след това, Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент. Докладите са публични.

2. В контекста на оценките и прегледите, посочени в параграф 1, Комисията разглежда по-специално прилагането и функционирането на:

а) глава V относно предаването на лични данни на трети държави или международни организации, особено по отношение на решенията, приети съгласно член 45, параграф 3 от настоящия регламент, и решенията, приети въз основа на **член 25, параграф 6 от Директива 95/46/ЕО**;

б) глава VII относно сътрудничеството и съгласуваността.

3. За целите на параграф 1 Комисията може да поиска информация от държавите членки и от надзорните органи.

4. При извършването на оценките и прегледите по параграфи 1 и 2 Комисията взема предвид позициите и констатациите на Европейския парламент, на Съвета и на други компетентни органи или източници.

5. При необходимост Комисията представя подходящи предложения за изменение на настоящия регламент, като отчита по-специално развитието на информационните технологии и напредъка на информационното общество.

Член 98

Преглед на други правни актове на Съюза за защита на данните

Ако е целесъобразно, Комисията представя законодателни предложения за изменение на други правни актове на Съюза за защита на личните данни, за да гарантира единна и съгласувана защита на физическите лица във връзка с обработването Това се отнася по-специално за правилата по отношение на защитата на физическите лица във връзка с обработването от институции, органи, служби и агенции на Съюза, както и за правилата по отношение на свободното движение на такива данни.

Член 99

Влизане в сила и прилагане

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

2. Прилага се от 25 май 2018 година.

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

Съставено в Брюксел на 27 април 2016 година.

За Европейския парламент

Председател

M. SCHULZ

За Съвета

Председател

J.A. HENNIS-PLASSCHAERT

_____

(1) ОВ C 229, 31.7.2012 г., стр. 90.

(2) ОВ C 391, 18.12.2012 г., стр. 127.

(3) Позиция на Европейския парламент от 12 март 2014 г. (все още непубликувана в Официален вестник) и позиция на Съвета на първо четене от 8 април 2016 г. (все още непубликувана в Официален вестник). Позиция на Европейския парламент от 14 април 2016 г.

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

(5) **Препоръка 2003/361/ЕО** на Комисията от 6 май 2003 г. относно дефиницията на микропредприятията, малките и средните предприятия (C(2003) 1422) (ОВ L 124, 20.5.2003 г., стр. 36).

(6) **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).

(7) **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 наказателни санкции и относно свободното движение на такива данни за отмяна на **Рамково решение 2008/977/ПВР на Съвета** (вж. страница 89 от настоящия брой на Официален вестник).

(8) **Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000** г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар (Директива за електронната търговия) (ОВ L 178, 17.7.2000 г., стр. 1).

(9) **Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011** г. за упражняване на правата на пациентите при трансгранично здравно обслужване (ОВ L 88, 4.4.2011 г., стр. 45).

(10) **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).

(11) **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 (текст от значение за ЕИП) (ОВ L 354, 31.12.2008 г., стр. 70).

(12) **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).

(13) **Регламент (ЕС) № 1215/2012 на Европейския парламент и на Съвета от 12 декември 2012** г. относно компетентността, признаването и изпълнението на съдебни решения по граждански и търговски дела (ОВ L 351, 20.12.2012 г., стр. 1).

(14) **Директива 2003/98/ЕО на Европейския парламент и на Съвета от 17 ноември 2003** г. относно повторната употреба на информацията в обществения сектор (ОВ L 345, 31.12.2003 г., стр. 90).

(15) **Регламент (ЕС) № 536/2014 на Европейския парламент и на Съвета от 16 април 2014** г. относно клиничните изпитвания на лекарствени продукти за хуманна употреба, и за отмяна на **Директива 2001/20/ЕО** (ОВ L 158, 27.5.2014 г., стр. 1).

(16) **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).

(17) ОВ C 192, 30.6.2012 г., стр. 7.

(18) **Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002** г. 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).

(19) **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).

(20) **Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008** г. за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на **Регламент (ЕИО) № 339/93** (ОВ L 218, 13.8.2008 г., стр. 30).

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

Важна правна бележка: Съгласно **Регламент (ЕС) № 216/2013** г. само законодателството на Европейските общности, публикувано в книжното издание до 1 юли 2013 г. и в електронната версия на Официален вестник на Европейския съюз след 1 юли 2013 г. (включително), се счита за автентично и има правна сила.