



Брюксел, 11 юни 2015 г.
(OR. en)

9565/15

Междуетноститутуционално досие:
2012/0011 (COD)

DATAPROTECT 97
JAI 420
MI 369
DIGIT 49
DAPIX 94
FREMP 133
COMIX 259
CODEC 823

БЕЛЕЖКА

От:	Председателството
До:	Съвета
№ предх. док.:	9398/15
Относно:	Предложение за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (Общ регламент относно защитата на данните) — Изготвяне на общ подход

Въведение

На 25 януари 2012 г. Комисията прие предложение за общ регламент относно защитата на данните (5853/12). Намерението е новият регламент да замени Директива 95/46/ЕО.

Регламентът преследва две цели: да укрепи правата на гражданите в областта на защитата на данните и да подобри възможностите за бизнес, като улесни свободното движение на лични данни в цифровия единен пазар.

Успоредно с предложението за общ регламент относно защитата на данните Комисията прие съобщение относно политиката, в което се излагат целите на Комисията (5852/12), и директива относно обработването на лични данни за целите на правоприлагането (5833/12). Целта на новата директива е да замени рамковото решение относно защитата на данните от 2008 г.

На 12 март 2014 г. Европейският парламент прие позициите си на първо четене по предложенията за регламент и за директива относно защитата на данните.

Компромисен текст

За сближаването на становищата в Съвета по предложението за общ регламент относно защитата на данните в неговата цялост бяха необходими няколко частични общи подхода. Текстът на регламента, който председателството представя за одобрение под формата на общ подход, е поместен в приложението. Всички промени по отношение на първоначалното предложение на Комисията са обозначени с подчертаване, а заличеният текст е обозначен със (...). Преместеният текст е обозначен с *курсив*. Бележките на делегациите по текста на регламента, който към онзи момент не включваше новите предложения на председателството относно съображения 118 и 134, са отразени в документа за резултатите от работата на заседанието на Комитета на постоянните представители на 9 юни 2015 г. (9788/15).

С оглед на заседанието на Комитета на постоянните представители на 9 юни 2015 г. председателството внесе две промени.

Право на обезщетение и отговорност за причинени вреди — член 77 и съображение 118

Председателството предлага съображение 118 да се промени, за да стане ясно, че основната цел на член 77 и съображение 118 е да се гарантира пълното и действително обезщетение на субекта на данните за причинени вреди. Като се има предвид, че правните системи на държавите членки се различават, що се отнася до отговорността за причинени вреди, субектът на данните може да получи такова обезщетение от администратор или обработващ лични данни, който носи отговорност за цялата вреда, или в държавите членки, чиито системи позволяват обединяване на производства, такова обезщетение може да бъде разделено между повече от един администратор или обработващ лични данни.

За да се осигури достатъчна правна сигурност за администраторите и обработващите лични данни, чиито текущи обработки на лични данни съответстват на Директива 95/46/ЕО, председателството предлага приложното поле на регламента да бъде пояснено в съображение 134.

Заключение

За да възложи на председателството мандат за преговори с представителите на Европейския парламент, Съветът се приканва да одобри текста на общия регламент относно защитата на данните, поместен в приложението под формата на общ подход.

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

**относно защитата на физическите лица във връзка с обработването на лични данни
и относно свободното движение на такива данни (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, параграф 2 (...) от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет,

след консултация с Европейския надзорен орган по защита на данните,

в съответствие с обикновената законодателна процедура,

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 и член 16, параграф 1 от Договора постановяват, че всеки има право на защита на личните данни, отнасящи се до него.
- 2) (...) Принципите и правилата относно защитата на физическите лица във връзка с обработването на личните им данни следва, независимо от гражданството или местопребиваването на физическите лица, да са съобразени с техните основни права и свободи и по-конкретно правото на защита на личните им данни. Това следва да допринася за създаването на пространство на свобода, сигурност и правосъдие и на икономически съюз, за постигането на икономически и социален прогрес, 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 от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни е да се хармонизира защитата на основните права и свободи на физическите лица по отношение на дейностите по обработване на данни и да се гарантира свободното движение на лични данни между държавите членки.
- (3а) Правото на защита на личните данни не е абсолютно право, то 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 принципите, възприети в Хартата на основните права на Европейския съюз, както е залегнало в Договорите, по-специално правото на зачитане на личния и семейния живот, дома и комуникациите, правото на защита на личните данни, свободата на мисълта, съвестта и вероизповеданието, свободата на изразяване и на информацията, свободата на стопанската инициатива, правото на ефективни правни средства за защита и на справедлив съдебен процес, както и правото на културно, религиозно и езиково многообразие.

- 4) Икономическата и социалната интеграция, произтичаща от функционирането на вътрешния пазар, доведе до съществено увеличение на трансграничните потоци от данни. Нарасна обменът на данни между (...) публични и частни участници, включително лица и предприятия в Съюза. Националните органи в държавите членки са задължени от правото на Съюза 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.
- 5) Бързото технологично развитие и глобализацията изправиха защитата на личните данни пред нови предизвикателства. Забележително нарасна мащабът на обмена и събирането на данни. Технологиите позволяват на частните дружества и публичните органи да използват лични данни в безпрецедентни мащаби, за да упражняват дейността си. Хората все по-често предоставят лична информация в публичното и световното пространство. Технологиите преобработиха както икономическия, така и социалния живот и следва да улесняват още повече свободното движение на данни в Съюза и предаването на данни до трети държави и международни организации, като същевременно се гарантира високо ниво на защита на личните данни.
- 6) Тези промени изискват (...) стабилна и по-съгласувана рамка за защита на данните в Съюза, подкрепена от силно правоприлагане, като се има предвид значението на изграждането на доверие, което ще позволи на цифровата икономика да се развива на вътрешния пазар. Физическите лица следва да имат контрол върху собствените си лични данни, а правната и практическата сигурност за физическите лица, икономическите оператори и публичните органи следва да бъдат засилени.
- (6a) Когато настоящият регламент предвижда спецификации или ограничения на своите правила от правото на държавите членки, държавите членки могат, доколкото това е необходимо с оглед на съгласуваността и разбираемостта на националните разпоредби за лицата, по отношение на които те се прилагат, да включат елементи на регламента в съответното национално право.

- 7) Целите и принципите на Директива 95/46/ЕО остават стабилни, но това не предотврати фрагментарния начин, по който се осъществява защитата на данни в Съюза, нито правната несигурност и широко разпространеното обществено схващане, че съществуват значителни рискове за защитата на физическите лица, свързани особено с дейностите онлайн. Разликите в осигуреното в държавите членки ниво на защита на правата и свободите на физическите лица, особено на правото на защита на личните данни, във връзка с обработването на лични данни могат да възпрепятстват свободното движение на лични данни в рамките на Съюза. Поради това тези разлики може да се превърнат в препятствие за осъществяването на икономически дейности на равнището на Съюза, да нарушат 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 в изпълнението и прилагането на Директива 95/46/ЕО.
- 8) За да се гарантира съгласувано 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. Необходимо е да се гарантира съгласувано и еднакво 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 законово задължение, за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, предоставени на администратора на лични данни, на държавите членки следва да се позволи да запазят или да въведат национални разпоредби, които да уточняват реда за прилагане на правилата на настоящия регламент. Наред с общите и хоризонтални актове относно защитата на данните, с които се изпълнява Директива 95/46/ЕО, държавите членки имат и специално секторно законодателство в области, които се нуждаят от по-специални разпоредби. Настоящият регламент оставя и свобода на действие на държавите членки да конкретизират собствените си правила. В рамките на предоставената им свобода на действие държавите членки следва да могат да запазят специфичното секторно законодателство, прието за изпълнение на Директива 95/46/ЕО.

- 9) 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, но също и еквивалентни правомощия за наблюдение и гарантиране на спазването на правилата за защита на личните данни, както и еквивалентни санкции за нарушителите в държавите членки.
- 10) В член 16, параграф 2 от Договора се възлага мандат 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.
- 11) 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 данни в рамките на вътрешния пазар, е необходим регламент, който да осигурява правна сигурност и прозрачност на икономическите оператори, включително на микропредприятията, 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 гарантира съгласувано наблюдение на обработването на лични данни, еквивалентни санкции във всички държави членки и ефективно сътрудничество от страна на надзорните органи на различните държави членки. За доброто функциониране на вътрешния пазар се изисква 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. (...)

С цел да се отчете особеното положение на микропредприятията, малките и средните предприятия в настоящия регламент са включени редица дерогации. Освен това институциите и органите на Съюза, държавите членки и техните надзорни органи се приканват да вземат предвид специфичните нужди на микропредприятията, малките и средните предприятия при прилагането на настоящия регламент. Разбирането на понятието за микропредприятия, малки и средни предприятия следва да се основава на Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микропредприятия, малките и средните предприятия.

- 12) Защитата, осигурена с настоящия регламент, се отнася за физическите лица, независимо от тяхното гражданство или местопребиваване, във връзка с обработването на лични данни. Що се отнася до обработването на данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и координатите за връзка на юридическото лице, никое от посочените лица не следва да търси защита по силата на настоящия регламент. (...)
- 13) Защитата на физическите лица следва да бъде технологично неутрална и да не зависи от използваната техника, тъй като в противен случай това би създавало сериозен риск от заобикаляне на закона. Защитата на физическите лица следва да се прилага за обработването на лични данни с автоматични средства, както и за ръчното им обработване, ако данните се съхраняват или са предназначени да се съхраняват в регистър на лични данни. Досиетата или групите от досиета, както и заглавните им страници, които не са структурирани съгласно специфични критерии, не следва да попадат в приложното поле на настоящия регламент.
- 14) Настоящият регламент не урежда въпроси по отношение на защитата на основните права и свободи или свободното движение на данни, свързани с дейности, които са извън приложното поле на правото на Съюза, например дейности в областта на националната сигурност, (...) нито урежда обработването на лични данни от държавите членки, когато извършват дейности във връзка с общата външна политика и политиката на сигурност на Съюза.
- (14a) Регламент (ЕО) № 45/2001 се прилага към обработването на лични данни от институциите, органите, службите и агенциите на Съюза. Регламент (ЕО) № 45/2001 и другите законодателни актове на Съюза, приложими към подобна обработка на лични данни, следва да бъдат адаптирани към принципите и правилата на настоящия регламент.
- 15) Регламентът не следва да се прилага спрямо обработването на лични данни от физическо лице в рамките на лична или домашна дейност, което следователно няма връзка с професионална или търговска дейност. Личните и домашните дейности включват участието в социални мрежи и онлайн дейности, предприети в контекста на тези лични и домашни дейности. Настоящият регламент (...) следва да се прилага обаче за администратори или обработващи лични данни, които осигуряват средствата за обработване на лични данни за такива лични или домашни дейности.

- 16) 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, изпълнението на наказателни санкции или предпазването от и предотвратяването на заплахи за обществената сигурност, и свободното движение на такива данни са предмет на специален правен инструмент на равнището на Съюза.

Следователно настоящият регламент не следва да се прилага спрямо дейностите по обработване на лични данни за такива цели. Обработването на данни от стана на публичните органи по силата на настоящия регламент обаче следва да бъде уредено с по-специфичен правен инструмент на равнището на Съюза (Директива XX/YYYY), когато данните се използват за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции. Държавите членки може да възложат на компетентните органи по смисъла на Директива XX/УУУ други задачи, чието изпълнение не е свързано задължително с целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, изпълнението на наказателни санкции или предпазването от и предотвратяването на заплахи за обществената сигурност, така че обработването на лични данни за тези цели, дотолкова, доколкото то попада 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 общия регламент относно защитата на данните, държавите членки може да запазят или да въведат по-конкретни разпоредби, за да адаптират прилагането на разпоредбите на общия регламент относно защитата на данните. Подобни разпоредби може 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 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 и наказателното преследване на престъпления. Това е от значение например в рамките на дейностите срещу изпирането на пари или на дейностите на съдебно-медицинските лаборатории.

(16a) Макар настоящият регламент да се прилага и спрямо дейностите на съдилищата и други съдебни органи, съгласно правото на Съюза или на държавите членки може да се определят конкретно операциите и процедурите по обработване на лични данни от съдилищата и другите съдебни органи. Компетентността на надзорните органи следва да не 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. Надзорът на такива операции по обработване на данни може да бъде поверен на специални органи в рамките на съдебната система на държавата членка, които по-конкретно да контролират спазването на правилата на настоящия регламент, да повишават осведомеността на съдебното съсловие за неговите задължения по силата на настоящия регламент и да се занимават с жалбите във връзка с това обработване.

17) Директива 2000/31/ЕО не се прилага за въпроси, свързани с услугите на информационното общество, обхванати от настоящия регламент. 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. Настоящият регламент не следва да засяга нейното прилагане. Поради това настоящият регламент следва да се прилага, без да се 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.

18) (...)

19) 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 или не. 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.

- 20) 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 с местопребиваване в Съюза от администратор, 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 или не с плащане, осъществявано в Съюза. За да се установи дали този администратор предлага стоки или услуги на такива субекти на данни в Съюза, следва да бъде уточнено дали администраторът възнамерява да развива стопанска дейност със субекти на данни, пребиваващи в една или повече държави членки на Съюза. Като се има предвид, че достъпността на уебсайт на администратора или на негов посредник в Съюза или на електронен адрес и други данни за контакт или използването на език, който по правило се използва в третата държава, където е установен администраторът, са недостатъчни, за да бъде уточнено подобно намерение, фактори като използване на език или валута, които по правило се използват в една или повече държави членки, с възможност за поръчване на стоки и услуги на този друг език и/или споменаването на потребители или ползватели, пребиваващи в Съюза, могат да спомогнат да бъде уточнено дали администраторът възнамерява да предлага стоки или услуги на такива субекти на данни в Съюза.
- 21) Обработването на лични данни на субекти на данни, пребиваващи в Съюза, от администратор, който не е установен в Съюза, следва също да се урежда от настоящия регламент, когато е свързано с наблюдението на тяхното поведение, осъществявано в 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 са следени в интернет посредством техники за обработване на данни, които се състоят в профилиране на дадено физическо лице, по-специално с цел да се вземат решения относно него или да се анализират или предугаждат неговите лични предпочитания, поведение и начин на мислене.
- 22) Когато националното право на дадена държава членка се прилага по силата на международното публично право, настоящият регламент се прилага също спрямо администратор, който не е установен в Съюза, като например дипломатическа мисия на държава членка или консулска служба.

23) 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. Данните, съдържащи псевдонимизирани данни, 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 лице може да бъде идентифицирано, следва да се вземат предвид всички средства, с които е вероятно да си послужи администраторът или което и да е друго лице, за да идентифицира пряко или непряко даденото физическо лице. За да се уточни дали има разумна вероятност дадени средства да бъдат използвани за идентифициране на лицето, следва да се вземат предвид всички обективни фактори, като разходите и количеството време, необходими за идентифицирането, като се отчитат както наличните към момента на обработване на данните технологии, така и тяхното развитие. Поради това принципите на защита на данните не следва да се прилагат по отношение на анонимна информация, т.е. информация, която не е свързана с идентифицирано или подлежащо на идентифициране физическо лице, или по отношение на данни, които са анонимизирани по такъв начин, че субектът на данните 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.

(23aa) Принципите на защитата на данните следва да не се прилагат за починали лица. Националното право на държава членка може да предвиди правила във връзка с обработването на данни на починали лица.

(23a) Прилагането на псевдонимизиране на личните данни може да намали рисковете за съответните субекти на данни и да помогне на администраторите и на обработващите лични данни в изпълнението на техните задължения за защита на данните. Изричното въвеждане на „псевдонимизацията“ чрез членовете на настоящия регламент следователно не е предназначено да изключи всички други мерки за защита на данните.

(236)(...)

(23в) С цел да се създадат стимули за прилагане на псевдонимизацията при обработването на лични данни, мерките за псевдонимизация, като същевременно се даде възможност за цялостен анализ, следва да са възможни при един и същи администратор на данни, когато той е взел всички необходими технически и организационни мерки за осигуряване изпълнението на разпоредбите на настоящия регламент, като се вземе предвид съответното обработване на данни и бъде направено необходимото допълнителната информация, свързваща личните данни с конкретен субект на данните, да бъде пазена отделно. Администраторът, който обработва данните, се обръща и към упълномощени лица в рамките на един и същи администратор на данни. В такъв случай обаче администраторът на данните следва да се увери, че лицето(ата), извършващо(и) псевдонимизацията, не е(са) посочено(и) в метаданните.

24) При използването на онлайн услуги физическите лица могат да са свързани с онлайн идентификатори, предоставени от техните устройства, приложения, инструменти и протоколи, като адресите по интернет протокол (IP адреси) или идентификаторите, наричани „бисквитки“. По този начин могат да бъдат оставени следи, които, съчетани с уникалните идентификатори и с друга информация, получена от сървърите, могат да се използват за създаването на профили на физическите лица и за тяхното идентифициране. Идентификационните номера, данните за местоположението, онлайн идентификаторите или други специфични фактори като такива не следва (...) непременно да се считат за лични данни, ако не идентифицират или не спомагат за идентифицирането на дадено лице.

25) Съгласие следва да се дава недвусмислено по всеки подходящ начин, позволяващ даването на свободно изразено, конкретно и информирано указание за волята на субекта на данни въз основа на писмено, в т.ч. електронно, или устно изявление, или ако се налага поради особени обстоятелства, чрез всякакво друго ясно потвърждаващо действие от страна на субекта на данни, удостоверяващо неговото съгласие за обработването на свързани с него лични данни. Това може да включва отбелязване с отметка в поле при посещението на уебсайт в интернет или всякакво друго указание или поведение, което ясно показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Мълчанието или липсата на действие следователно не следва да представлява съгласие. Когато е технически възможно и ефективно, съгласието на субекта на данните за обработването може да бъде давано посредством подходящи настройки на браузъра или друго приложение. В такива случаи е достатъчно субектът на данни да получи информацията, необходима за свободното заявяване на конкретно и информирано съгласие при започване на използването на услугата. (...). 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 недвусмислено 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.

- (25a) Генетичните данни следва да се определят като лични данни, които са свързани с наследени или придобити генетични белези на дадено физическо лице и са получени в резултат от анализ на биологична проба от въпросното физическо лице, по-специално чрез анализ на дезоксирибонуклеиновата киселина (ДНК) или на рибонуклеиновата киселина (РНК) или анализ на всеки друг елемент, позволяващ получаване на равностойна информация.
- (25aa) Често в момента на събиране на данните целта за обработване на данни за научни цели не може да бъде напълно идентифицирана. Поради това субектите на данни могат да дадат съгласие за определени области на научни изследвания при спазване на признатите етични норми, отнасящи се за научните изследвания. Субектите на данни следва да имат възможност да дадат своето съгласие само за определени области на научни изследвания или части от научноизследователски проекти, доколкото позволява преследваната цел и при условие, че това не е свързано с непропорционални усилия с оглед на целта за защита.
- 26) Личните данни, отнасящи се до здравето, следва да обхващат (...) данни, свързани със здравословното състояние на субекта на данните, които разкриват информация за физическото или менталното здраве на субекта на данните в миналото, настоящето или бъдещето; включително информацията относно регистрацията на физическото лице за целите на предоставянето на здравно обслужване (...); номер, символ или характеристика, присвоени на 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 генетични данни и биологични проби; (...) или всякаква информация, като например за заболяване, увреждане, риск от заболяване, медицинска история, клинично лечение или текущо физиологично или биомедицинско състояние на субекта на данните, независимо от източника на информация, например лекар или друг медицински специалист, болница, медицинско изделие или ин витро диагностично изследване.

27) Основното място на установяване на администратор на данни в Съюза следва да бъде мястото в Съюза, където се намира главната му администрация, 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 такъв случай последното 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 в действителност 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 такова 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 главното му управление в Съюза, а ако няма главно 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 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, следва да не се считат за засегнати надзорни органи, ако 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.

- 28) 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. Централно предприятие, което осъществява надзор на обработването на лични данни в свързани с него предприятия, образува заедно с тях образувание, което може да се третира като „група предприятия“.
- 29) На децата (...) се полага специална защита на личните данни, тъй като те не познават достатъчно добре рисковете, последиците, гаранциите и своите права, свързани с обработването на лични данни. (...) Това се отнася 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 на деца при ползване на услуги, предоставяни пряко на деца.
- 30) Всяко обработване на лични данни следва да бъде законосъобразно и добросъвестно. (...) Физическите лица следва да знаят, че личните им данни се събират, използват, от тях се извлича информация или се обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данни. Принципът на прозрачност изисква всяка информация както за обществеността, така и за субекта на данни, да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки. Това 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 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 данните, следва да бъдат ясни и законни и определени към момента на събирането на данните. Личните данни следва да са подходящи и релевантни (...) за целите, за които данните се обработват; това налага, по-специално, да се гарантира, че събраните данни не надхвърлят необходимото и че срокът, за който данните се съхраняват, е ограничен до строг минимум. (...) Личните данни следва да се обработват единствено ако целта на обработването не може логично да бъде постигната с други средства. С цел да се гарантира, че срокът на съхранение на данните не е по-дълъг от необходимия, администраторът следва да установи срокове за тяхното заличаване 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 подобаваща степен на сигурност и поверителност на личните данни, включително предотвратяване на неправомерен достъп до или използване на лични данни или оборудване за тяхното обработване.

31) За да бъде обработването законосъобразно, личните данни следва да бъдат обработвани въз основа на съгласието на съответното лице или на друго легитимно правно основание, установено по законодателен път било в настоящия регламент или в друг правен акт на Съюза или на държава членка, както е посочено в настоящия регламент, включително необходимостта от спазване на законовото задължение, наложено на администратора на лични данни, или необходимостта от изпълнение на договор, по който субектът на данни е страна, или за да бъдат предприети стъпки по искане на субекта на данни преди встъпване в договорни отношения.

(31a) Когато в настоящия регламент се прави позоваване на правно основание или законодателна мярка, това не налага непременно приемането на законодателен акт от парламент, без 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 да бъде предвидимо за правните субекти, както изисква съдебната практика на Съда на Европейския съюз и на Европейския съд по правата на човека.

(32) 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. Следва да бъде предоставена предварително съставена от администратора декларация за съгласие в разбираема и лесно достъпна форма, на ясен и прост език, като съдържанието ѝ не следва да звучи необичайно в общия контекст. За да бъде дадено съгласие 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, 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.

(33) (...)

- 34) За да се гарантира, че съгласието е дадено свободно, съгласието не следва да представлява валидно правно основание за обработването на лични данни в конкретна ситуация, когато е налице очевидна неравнопоставеност между субекта на данните и администратора и поради тази неравнопоставеност не изглежда вероятно съгласието да е дадено свободно във всички обстоятелства на конкретната ситуация. Смята се, че съгласието не е изразено свободно, ако то не дава възможност да бъде дадено отделно съгласие за различни операции по обработване на данни, макар да е подходящо в конкретния случай, или ако изпълнението на даден договор се поставя в зависимост от даването на съгласие, въпреки че това не е необходимо за това изпълнение, и субектът на данните не може в разумни граници да получи същите услуги от друг източник, без да даде съгласие.
- 35) Обработването на данни следва да е законосъобразно, когато то е необходимо в контекста на договор или при намерение за сключване на договор.
- (35a) Настоящият регламент предвижда общи правила относно защитата на данните, както и че в някои особени случаи държавите членки имат право да определят и национални правила относно защитата на данните. Следователно регламентът не изключва правни актове на държавите членки, които определят характеристиките на специални случаи на обработване, включително които определят по-точно условията, при които обработването на лични данни е законосъобразно. В националното право може да се предвидят също специални условия за обработването в определени сектори и за обработването на специални категории данни.
- (36) Когато обработването се извършва в съответствие със законово 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 националното право на държава членка. (...) Правото на Съюза или националното право следва да определя също и целите на обработването. В това (...) основание биха могли да се посочат общите условия на регламента, които определят законосъобразността на обработването на данни, да се установяват спецификациите за определянето на администратора на лични данни, видът данни, които подлежат на обработване, съответните субекти на данни, образуванията, пред които могат да бъдат разкривани данни, ограниченията по отношение на целите, периодът на съхранение и други мерки за гарантиране на законосъобразното и добросъвестно обработване.

Също така законодателството на Съюза или националното законодателство следва да 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 или частното право, като например професионално сдружение, когато това е оправдано поради съображения от обществен интерес, включително за здравни цели, например общественото здраве и социалната закрила и управлението на здравните служби.

- 37) Обработването на лични данни следва също да се счита за законосъобразно, когато е необходимо, за да се защити интерес от основно значение за живота на субекта на данните или на друго лице. (...) Някои видове обработване на данни могат да обслужват както важни области от обществен интерес, така и жизненоважните интереси на субекта на данните, като 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 бедствия.
- 38) Законните интереси на даден администратор, включително на администратор, пред когото може да бъдат разкрити 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. Законен интерес може да е налице, когато например между субекта на данни и администратора на лични данни съществува съответна определена връзка, като 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, в т.ч. дали субектът на данни може по времето и в контекста на събирането на данни да очаква, че може да се осъществи обработване на данните за тази цел. Тази преценка трябва по-специално да отчита дали субектът на данни е дете, като се има предвид, че на децата се полага специална защита. Субектът на данни следва да има право на възразение срещу обработването въз основа на конкретното си положение и безплатно. За да се гарантира прозрачността, администраторът следва да бъде задължен изрично да информира субекта на данни относно преследваните законни интереси и относно правото на възразение и също така да бъде задължен да документира тези законни интереси. (...)

(38a) Администратори, които представляват част от група предприятия или институция, свързана с централен орган, могат да имат законен интерес да предадат личните данни в рамките на групата предприятия за вътрешни административни цели, включително 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.

39) Обработването на данни в степен, която е строго необходима за целите на гарантирането на мрежовата и информационната сигурност, т.е. способността на дадена мрежа или информационна система да издържа, на дадено равнище на доверие, на случайни събития или неправомерни или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхраняваните или предаваните 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, екипи за реагиране при инциденти с компютърната сигурност, 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, разпространение на зловреден софтуер, спиране на атаки с цел отказване на услугите и вреди за компютрите и електронните съобщителни системи. 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.

40) Обработването на лични данни за цели, различни от тези, за които първоначално са събрани данните, следва да бъде разрешено единствено когато обработването е съвместимо с целите, за които първоначално са събрани данните. В такъв случай не се изисква отделно правно основание, различно от това, с което е било разрешено събирането на данните. (...) Ако обработването е необходимо за изпълнението на задача, осъществявана в обществен интерес или свързана с упражняването на официални правомощия, които са предоставени на администратора на лични данни, в правото на Съюза или правото на държава членка могат да бъдат определени и уточнени задачите и целите, за които допълнителното обработване се счита за законосъобразно. Допълнителното обработване (...) с цел архивиране от обществен интерес или за статистически, научни или исторически (...) цели (...), или с оглед на бъдещо решаване на спорове, следва да се разглежда като съвместими законосъобразни операции по обработване. Правното основание, предвидено в правото на Съюза или на държавите членки за събирането и обработването на лични данни, може да бъде и правно основание за допълнително обработване за други цели, ако тези цели са в съответствие с възложената задача и администраторът на данните има право законно да събира данни за тези други цели.

За да установи дали дадена цел на допълнително обработване е съвместима с целта, за която първоначално са събрани данните, 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 допълнително обработване, в какъв контекст са събрани данните, включително основателните очаквания на субекта на данните по отношение на тяхното по-нататъшно използване, естеството на личните данни, последствията от предвиденото допълнително обработване на данни за субектите на данни и съществуването на подходящи гаранции при операциите по първоначалното и предвиденото допълнително обработване. Ако набеязаната друга цел не е съвместима с първоначалната, за която са събрани данните, администраторът следва да получи съгласието на субекта на данните за тази допълнителна цел или следва да основе обработването на друго законно основание за законосъобразно обработване, особено когато това е предвидено в правото на Съюза или в правото на държавата членка, което се прилага спрямо администратора. (...)

Във всеки случай прилагането на принципите, установени с 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. (...) Посочването от администратора на данни на евентуални престъпни деяния или заплахи за обществената сигурност и предаването на тези данни на компетентен орган следва да се разглеждат като част от законния интерес, преследван от администратора. Въпреки това, подобно предаване, което е от законен интерес на администратора, или допълнително 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.

- 41) 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 може да създаде значителни рискове за основните права и свободи. Тези данни следва да включват и личните данни, разкриващи расов или етнически произход, като използването на понятието „расов произход“ в настоящия регламент не означава, че Европейският съюз приема теориите, които се опитват да установят съществуването на отделни човешки раси. Тези данни не следва да се обработват, освен ако обработването не е разрешено в конкретни 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 правилата, залегнали в настоящия регламент, за спазване на законово задължение или за изпълнение на задача, осъществявана в 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, в частност 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.

Специални категории лични данни могат също да бъдат обработвани, ако данните явно са направени обществено достояние или доброволно и по искане на субекта на данните са предадени на администратора за конкретна цел, посочена от субекта на данните, когато обработването се извършва в негов интерес.

В правото на държавите членки и на Съюза може да бъде предвидено общата забрана за обработване на такива специални категории лични данни в определени случаи да не може да бъде вдигната посредством изричното съгласие на субекта на данни.

- 42) Дерогация от забраната за обработване на чувствителни категории данни следва бъде разрешена и ако такава е предвидена в правото на Съюза или на държава членка и при подходящи гаранции, така че да бъдат защитени личните данни и останалите основни права, когато (...) съображения, свързани с обществен интерес, оправдават това, по-специално обработването на данни в областта на трудовото право, правото в областта на социалната сигурност и социалната закрила, включително пенсиите, иза целите на сигурността, наблюдението и предупреждението във връзка със здравеопазването, предотвратяването или контрола на заразните болести и други сериозни заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и услуги, както и на лекарствените продукти или медицинските изделия, или за целите на оценката на обществените политики в областта на здравеопазването, както и чрез изготвянето на показатели за качеството и активността.

Това 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 архивиране в обществен интерес или за исторически, статистически и научни (...) цели.

Чрез дерогация следва да се даде възможност да се обработват и такива 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.

(42a) 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 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 предупреждението във връзка със здравеопазването, или за целите на архивирането в обществен интерес, за исторически, статистически или научни цели, както и за целите на проучванията в областта на общественото здраве, провеждани в интерес на обществото. Поради това настоящият регламент следва да предвижда хармонизирани условия за обработването на специални категории лични данни, свързани със здравето, 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 на държавите членки следва да предвижда конкретни и подходящи мерки за защита на основните права и личните данни на всяко лице. (...)

(42б) 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. Това обработване е предмет на подходящи и конкретни мерки с оглед защита на правата и свободите на отделните лица. В този контекст понятието „обществено здраве“ следва да се тълкува по смисъла на 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 и означава всички елементи, свързани със здравето, а именно здравно състояние, включително заболяемост и инвалидност, решаващи фактори, които оказват влияние върху това здравно 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 лични 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, застрахователни дружества или банки.

- 43) Освен това обработването на лични данни от официални органи за постигането на цели, определени в конституционното право или в международното публично право, на официално признати религиозни сдружения се извършва по съображения от обществен интерес.
- 44) Когато демократичната система в дадена държава членка предполага по време на предизборна дейност политическите партии да събират 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.
- 45) Ако обработваните от администратора 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 подкрепя упражняваните от него права.
- 46) Принципът на прозрачност изисква всяка информация както за обществеността, така и за субекта на данните да бъде лесно достъпна и разбираема 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 и в електронна форма, например чрез уебсайт, когато е адресирана до обществеността. Това важи в особена степен за ситуации, като например онлайн рекламите, където увеличеният брой участници и технологичната сложност на тази практика трудно позволяват на субекта на данни да знае и да разбира дали се събират свързани с него лични данни, от кого и с каква цел. 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 такива ясни и недвусмислени формулировки, които да бъдат лесно разбираеми за детето.

- 47) Следва да бъдат осигурени условия за улесняване на упражняването на правата на субектите на данни, предоставени с настоящия регламент, включително механизми за (...) искане на достъп до данни, коригиране, заличаване и упражняване на правото на възразение. Затова 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 отговори на исканията на субекта на данни незабавно и най-късно в рамките на фиксиран срок от един месец, както и да посочи причините, ако не възнамерява да изпълни искането на субекта на данни.

Въпреки това, ако исканията са очевидно неоснователни или прекомерни, като например когато субектът на данни необосновано и многократно иска информация, или когато субектът на данните злоупотребява с правото си да получава информация, например чрез предоставяне на фалшива или подвеждаща информация при подаване на искането, администраторът би могъл да откаже да предприеме действия по искането.

- 48) 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 предоставя на субекта на данни всякаква допълнителна информация, необходима за гарантирането на добросъвестно и прозрачно обработване. Освен това субектът на данни следва да бъде информиран, че се извършва профилиране и за последствията от подобно профилиране. Когато от субекта на данни се събират данни, той следва да бъде информиран и относно това дали е задължен да предостави данните и относно последствията, ако не предостави тези данни.

- 49) Информацията за обработването на лични данни, свързани със субекта на данните, следва да му се предоставя в момента на събирането или, когато данните не са събрани от субекта на данните, в рамките на разумен срок, в зависимост от обстоятелствата в конкретния случай. В случаите, когато данните могат да бъдат законно разкрити на друг получател, субектът на данните следва да бъде информиран, когато данните се разкриват за първи път на получателя. Когато администраторът на данни възнамерява да обработва данните за цел, различна от тази, за която са събрани, той следва да предостави на субекта на данните преди това допълнително обработване информация за въпросната друга цел и друга необходима информация. Когато на субекта на данните не може да се предостави информация за произхода на данните, поради използването на различни източници, информацията се представя по обобщен начин.

- 50) Не е необходимо обаче да се налага такова задължение, когато субектът на данни вече разполага с тази информация, когато записването или разкриването на данните 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 на данни се извършва за целите на архивирането в обществен интерес, за исторически, статистически или научни (...) цели; в този контекст може да бъде взет предвид броят на субектите на данни, актуалността на данните и всички установени гаранции.
- 51) Всяко физическо лице следва да има право на достъп до събраните 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 физическите лица на достъп до личните данни за здравословното им състояние, например данните в техните медицински досиета, които съдържат такава информация като диагноза, 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 това за какви цели се обработват данните, когато е възможно — за какъв срок, кои са получателите на данните, каква е логиката на автоматичното обработване на данните и какви биха могли да бъдат последствията от такова обработване, най-малкото когато става дума за създаване на профили. Това право не следва да влияе неблагоприятно върху правата и свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право, закрилящо софтуера. Тези съображения обаче не следва да водят до отказ на всякаква информация на съответния субект на данни. Когато администраторът обработва голямо количество информация относно субекта на данни, администраторът може да поиска преди да предаде информацията субектът на данните да посочи точно за коя информация или за кои дейности по обработването се отнася искането.
- 52) 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. (...) 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. Администраторът не следва да запазва лични данни с единствената цел да може да отговори на потенциални искания.

- 53) Всяко физическо лице следва да има право на коригиране на личните данни, свързани с него, както и правото „да бъде забравено“, когато запазването на тези данни не е в съответствие с настоящия регламент или с правото на Съюза или на държавата членка, под чиято юрисдикция е администраторът на данните. По-специално, субектите на данни следва да имат право личните им данни да се заличават и да не бъдат обработвани повече, когато данните престанат да бъдат необходими с оглед на целите, за които са били събрани или обработвани по-друг начин, когато субектите на данните са оттеглили своето съгласие за обработването им, когато възразяват срещу обработването на лични данни, свързани с тях, или когато обработването на личните им данни по друг начин не е в съответствие с настоящия регламент. Това право е особено важно, когато субектът на данни е дал съгласието си като дете, когато 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 данните обаче следва да бъде законно, ако е необходимо за упражняване на правото на свобода на изразяване или правото на информация, за привеждане в съответствие с правно задължение, за изпълнението на задача, извършвана в интерес на обществото или при изпълнението на официални функции, възложени на администратора, по причини от публичен интерес в областта на общественото здравеопазване, за целите на архивирането в интерес на обществото, за исторически, статистически и научни (...) цели или за установяването, упражняването или защитата на правни искове.
- 54) С цел утвърждаване на „правото да бъдеш забравен“ в онлайн средата, правото на заличаване следва също да бъде разширено, така че администраторът, който е направил личните данни обществено достъпни, следва да бъде задължен да уведоми администраторите, които обработват такива данни, (...) да заличат всякакви връзки към тези лични данни или техните копия или реплики.

С цел да осигури посочената по-горе информация администраторът следва да предприеме (...) разумни мерки, като взема предвид наличните технологии и средствата на разположение на администратора, в това число технически мерки, по отношение на данните, за чието публикуване отговаря. (...)

(54a) Методите за ограничаване на обработването на лични данни биха могли да включват, наред с другото, временно преместване на избраните данни в друга система за обработване или прекратяване на достъпа на ползвателите до тях, или временно премахване на публикуваните данни от уебсайт. В системите за автоматизирано архивиране ограничаването на обработването на лични данни следва по принцип да бъде осигурено с технически средства; фактът, че обработването на лични данни е ограничено, следва да бъде посочен в системата по начин, който ясно показва, че обработването на лични данни подлежи на ограничения.

55) С цел допълнително укрепване на контрола над собствените данни (...), когато обработването на лични данни става по автоматичен начин, субектът на данните следва да има и правото да получаваотнасящите се до него лични данни, които той е предоставил на администратора, в структуриран, широко използван и пригоден за машинно четене формат, и да я предава на друг администратор.

Това право следва да се прилага, когато субектът на данни е предоставил личните данни по собствено съгласие или по 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 по-специално не следва да се прилага, когато обработването на личните данни е необходимо за спазване на законово задължение, което се прилага спрямо администратора, или за изпълнението на задача от обществен интерес, или при упражняването на официално правомощие, предоставено на администратора.

Правото на субекта на данни да предава лични данни не създава задължение за администраторите да възприемат или поддържат технически съвместими системи за обработване на данни.

Когато в определен пакет от лични данни е засегнат повече от един субект на данни, правото данните да бъдат предавани не следва да засяга изискванията за законосъобразност на обработването на лични данни във връзка с друг субект на данни в съответствие с настоящия регламент. Това право не следва да засяга и правото на субекта на данни на заличаване на лични данни и ограниченията на това право, както е посочено в настоящия регламент, и по-специално не следва да включва заличаването на лични данни относно субекта на данните, които той е предоставил в изпълнение на договор в степента и за сроковете, необходими за изпълнението на този договор. (...)

- 56) В случаите, когато личните данни биха могли да бъдат законно обработвани (...), 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 при все това да има право на възражение срещу обработването на 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.
- 57) Когато се обработват лични данни за целите на директния маркетинг, субектът на данните следва да има право на възражение срещу такова обработване, независимо дали първоначално или допълнително, безплатно и по начин, който може лесно и ефективно да се използва.

- 58) Субектът на данни следва да има правото да не бъде обект на решение, с което се прави оценка на свързани с него лични аспекти (...) въз основа единствено на автоматично обработване, пораждащо правни последиствия за него или го засяга в значителна степен, като например автоматичен отказ на онлайн искания за кредит или електронни практики за набиране на персонал без човешка намеса. Това обработване включва и „профилирането“, състоящо се от всякакви форми на автоматично 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, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението, местоположението или движенията, доколкото това поражда правни последиствия по отношение на лицето или го засяга значително. Въпреки това вземането на решения въз основа на такова обработване, включително профилиране, следва да бъде позволено, когато е разрешено от правото на Съюза или на държава членка, под чиято юрисдикция е администраторът, включително за целите на наблюдението и предотвратяването на измамите и укриването на данъци 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, включително конкретното информиране на субекта на данните и правото на човешка намеса, правото на субекта на изразяване на неговото мнение, на получаване на обяснение за решението, взето в резултат на такава оценка, както и правото на обжалване на решението. 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-конкретно за да гарантира, че факторите, които водят до неточности в данните, 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, наред с другото, ефект на дискриминация за лицата въз основа на тяхната раса или етнически произход, политически възгледи, вероизповедание или убеждения, членство в синдикални организации, генетичен или здравен статус, 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.

(58a) Профилирането като такова се подчинява на (общите) правила на настоящия регламент относно обработването на лични данни (правни основания за обработването, принципи за защитата на данни и т.н.), с конкретни гаранции (например задължението за провеждане на оценка на въздействието в някои случаи или разпоредбите за предоставяне на конкретна информация на заинтересованото лице). Европейският комитет по защита на данните следва да може да издава насоки в това отношение.

59) Ограничения върху специфични принципи и върху правото на информация, достъп, коригиране и заличаване или върху правото на преносимост на данните, на възражение, на мерки, основани на създаване на профили, както и уведомяването на субект на данни за нарушение на сигурността на данни и на определени свързани с това задължения на администраторите на лични данни, могат да бъдат налагани от правото на Съюза или на държава членка, доколкото 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 нарушения на етичните кодекси при регламентирания професии, други обществени интереси 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, допълнителното 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 хуманитарни цели, като изпълнението на задача, възложена на Международното движение на Червения кръст и Червения полумесец (...). Тези ограничения следва да бъдат в съответствие с изискванията, определени в Хартата на основните права на Европейския съюз и в Европейската конвенция за защита на правата на човека и основните свободи.

59a) Никоя разпоредба на настоящия регламент не следва да засяга (...) предоставената на Международния комитет на Червения кръст съгласно международното право привилегия за неразкриване на поверителна информация, която е приложима при съдебни и административни производства. (...)

60) Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-конкретно администраторът следва (...) да е длъжен да прилага подходящи мерки и да бъде в състояние да докаже, че (...) дейностите по обработването съответстват на настоящия регламент (...). Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на лицата.

(60a) Такива рискове, с различна вероятност и тежест, могат да произтичат от обработване на данни, което би могло да доведе до физически, материални или морални 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 данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация, или други значителни икономически или социални неблагоприятни последици; 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 или на данни, отнасящи се до здравето или сексуалния живот или до присъди и престъпления или свързани с тях мерки за сигурност; когато се оценяват лични аспекти, по-конкретно анализиране и 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; когато обработването включва голям обем лични данни и засяга голям брой субекти на данни; (...).

60b) Вероятността и тежестта на риска следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването на данни. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до висок риск. Високият риск е специфичен риск, който засяга правата и свободите на лицата (...).

(60в) 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 техния 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 Европейския комитет по защита на данните или чрез указания, предоставени от длъжностното лице за защита на данните. Европейският комитет по защита на данните 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 лицата, и да даде указания какви мерки могат да бъдат достатъчни в такива случаи за преодоляването на такъв риск. (...)

61) Защитата на правата и свободите на лицата с оглед на обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира, че са изпълнени изискванията на настоящия регламент. С цел да се гарантира и докаже съответствие с настоящия регламент администраторът следва да приеме вътрешни политики и да предприеме подходящи мерки, които отговарят по-специално на принципите за защита на данните още при проектирането и по подразбиране. Такива мерки могат да се изразяват, наред с другото, 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 най-новите постижения, да се уверят, че администраторите и обработващите лични данни са в състояние да изпълнят своите задължения за защита на данните.

62) 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.

63) Когато даден администратор, който не е установен в Съюза, обработва лични данни на субекти на данни с местопребиваване в Съюза и дейностите му по обработването са свързани с предлагането на стоки или услуги на такива субекти на данни или с наблюдението на тяхното поведение в Съюза, (...) администраторът следва да определи представител освен ако (...) извършването от него обработване има случаен характер и е слабо вероятно да породява риск за правата и свободите на субектите на данни, предвид естеството, обхвата, контекста и целите на обработването, или ако администраторът е публичен орган или структура (...). Представителят следва да действа от името на администратора, а надзорният орган може да се обръща към него. Представителят следва да бъде посочен изрично от администратора с писмен мандат да действа от негово име във връзка с неговите задължения съгласно настоящия регламент. Посочването на представител не засяга отговорностите и задълженията на администратора съгласно настоящия регламент. Този представител следва да изпълнява задачите си в съответствие с получения от администратора мандат, включително да си сътрудничи с компетентните надзорни органи при всяко действие, което се предприема, за да се осигури спазването на настоящия регламент. Посоченият представител следва да бъде обект на правоприлагащи мерки, в случай на нарушение от страна на администратора.

(63a) 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 обработващи лични данни, които предоставят достатъчни гаранции, особено по отношение на експертни знания, надеждност и ресурси, че ще предприемат технически и организационни мерки, които да 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 на държава членка, който обвързва обработващия лични данни с администратора, регламентира предмета и срока на действие 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, или които са част от сертифициране, предоставено по механизма за сертифициране. След приключване на обработването от името на администратора, обработващият личните данни следва да ги върне или изтрие, освен ако не е налице изискване за съхраняване на данните по силата на правото на Съюза или на държава членка, което се прилага спрямо обработващия лични данни.

64) (...)

65) За да докаже съответствие с настоящия регламент, администраторът или обработващият данни следва да поддържа документация за всички категории дейности по обработване, за които той е отговорен. Всеки администратор и обработващ лични данни следва да бъде длъжен да си сътрудничи с надзорния орган и да му предоставя тази документация при поискване, за да може да бъде използвана за наблюдение на тези операции по обработване.

- 66) 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. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид наличните технологии 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 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 морални вреди.
- (66a) За да се повиши спазването на настоящия регламент, в случаите, в които е вероятно операциите по обработването да доведат до висок риск за правата и свободите на лицата, 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 подходящите мерки, за да се докаже, че обработването на лични данни е в съответствие с 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.

- 67) Нарушаването на сигурността на лични данни може, ако не бъде овладяно по подходящ и навременен начин, да доведе до (...) физически, материални или морални вреди, 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, накръняване на репутацията, нарушаване на поверителността на данни, защитени от професионална тайна, или някакви други икономически или социални неблагоприятни последици за засегнатите лица. (...) Поради това, веднага след като администраторът установи наличието на (...) нарушение на сигурността на лични данни, което може да доведе до (...) физически, материални или морални вреди, той следва да уведоми за него надзорния орган без излишно забавяне и когато това е осъществимо — в срок от 72 часа. Когато уведомлението не може да бъде подадено в срок от 72 часа, то следва да бъде придружено от обяснение относно причините за забавянето. Физическите лица, чиито права и свободи могат да бъдат сериозно накрънени от такива нарушения, следва да бъдат уведомени без излишно забавяне с цел предприемане на 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. Субектите на данни следва да бъдат уведомявани веднага щом това е разумно осъществимо и в тясно сътрудничество с надзорния орган, като се спазват насоките, предоставени от него или от други релевантни органи (например правоприлагащи 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 данните или срещу подобни нарушения би оправдало по-дълги срокове.
- 68) (...) Трябва 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 намеса на надзорния орган в съответствие със задачите и правомощията, които са му предоставени с настоящия регламент.

(68a) Не следва да се изисква уведомяване на субекта на данни за нарушение на сигурността на личните данни, ако администраторът е предприел подходящи технологични мерки за защита и тези мерки са били приложени спрямо данните, засегнати от нарушението на сигурността на личните данни. Такива технологични мерки за защита следва да включват мерки, които правят данните неразбираеми за всяко лице, което няма разрешение за достъп до тях, по-специално като кодират личните данни(...).

69) При установяване на подробни правила за формата и процедурите, приложими за уведомяването за нарушения на сигурността на личните данни, следва да се отдаде необходимото внимание на обстоятелствата, свързани с нарушението на сигурността, 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 в случаи, когато ранното разкриване може ненужно да попречи при разследването на обстоятелствата, свързани с нарушението на сигурността.

70) 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, но невинаги допринася за подобряването на защитата на личните данни. Ето защо тези общи задължения за безразборно уведомяване следва да бъдат премахнати и заменени с ефективни процедури и механизми, които са съсредоточени върху тези видове операции по обработване, за които има вероятност да доведат до висок риск за правата и свободите на лицата поради своето естество, обхват, *контекст* и цели (...). Такива видове операции по обработване могат да бъдат тези, които по-конкретно включват използването на нови технологии, или са нов вид технологии и когато преди това не е извършена оценка на въздействието върху защитата на данните от администратора, или когато възниква необходимост от тях във връзка с времето, което е изминало от първоначалното обработване.

(70a) 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 този висок риск, като се вземат предвид естеството, обхвата, контекстът и целите на обработването и източниците на рисковете, като тази оценка включва по-специално предвидените мерки, гаранциите и механизмите за ограничаване на тези рискове, с които се осигурява защитата на личните данни и се доказва съответствието с настоящия регламент.

71) 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 в случаи, когато данните се обработват с цел вземане на решения относно конкретни 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 престъпления 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 оптично-електронни 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 те 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, независимо от обема или естеството на данните, не следва да се счита за широкомащабно, ако обработването на такива данни е защитено с професионална тайна (...), като обработването на лични данни на пациенти или клиенти от личен лекар, здравен работник, болница или адвокат. В такива случаи оценката на въздействието върху защитата на данните не следва да бъде задължителна.

- 72) 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.
- 73) Оценките за въздействието върху защитата на личните данни може да се извършват от обществен орган или обществена структура, ако такава оценка вече не е направена в контекста на приемането на националния закон, на чието основание общественият орган или обществената структура изпълнява своите задачи и който урежда въпросната специална операция или набор от операции по обработване на данни.
- 74) Когато в оценката на въздействието върху защитата на данните е указано, че въпреки предвидените гаранции, мерки за сигурност и ограничаване на риска обработването бидовело до висок риск за правата и свободите на лицата (...), 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. Такъв висок (...) риск може да бъде породен от определен вид обработване на данни и от определена степен и честота на обработване, които могат да доведат също до нанасяне на (...) вреди или до (...) намеса в правата и свободите на субекта на данни. Надзорният орган следва да отговори на искането за консултация в определен срок. Въпреки това отсъствието на отговор от надзорния орган в рамките на този срок не следва да засяга 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 процеса на консултации на надзорния орган може да се представи резултатът от оценка на въздействието върху защитата на данните, извършена по отношение на въпросното обработване съгласно член 33., и по-конкретно мерките, предвидени за ограничаване на възможните рискове за правата и свободите на лицата.
- (74a) 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.

(74б) Надзорният орган следва да бъде консултиран и при изготвяне на законодателна или регулаторна мярка, която предвижда обработване на лични данни, (...) за да се гарантира, че планираното обработване съответства на настоящия регламент, и по-специално за да се ограничат рисковете, свързани със субекта на данни.

75) В случаите, когато обработването на данни се извършва в публичния сектор или когато в частния сектор обработването се извършва от голямо предприятие или когато основните дейности на предприятието, независимо от размера му, включват операции по обработване, които изискват редовно и систематично наблюдение, администраторът или обработващият лични данни може да бъде подпомаган при наблюдението на вътрешното съответствие с настоящия регламент от лице с експертни познания в областта на законодателството и практиките за защита на данните. Тези служители по защита на данните, независимо от това дали са наети от администратора, следва да бъдат в състояние да изпълняват своите задължения и задачи независимо.

76) 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-конкретно 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 лицата.

(76а) 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.

77) 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.

- 78) Трансграничните 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 създаде нови предизвикателства и опасения по отношение на 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, следва да не 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 глава V, при спазване на другите разпоредби на настоящия регламент.
- 79) 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 сключат международни споразумения, които включват предаването на лични данни на трети държави или международни организации, доколкото тези споразумения не засягат настоящия регламент или други разпоредби от правото на ЕС и доколкото включват гаранции за защита на правата на субектите на данни.

- 80) Комисията може (...) да реши, с действие по отношение на целия Съюз, че определени трети държави или територия или конкретен сектор, например частният сектор или един или повече конкретни икономически сектори в дадена трета държава, или международна организация, предоставят адекватно ниво на защита на данните, с което се осигуряват правна сигурност и еднообразие навсякъде в Съюза по отношение на третите държави или международните организации, за които се смята, че предоставят такова ниво на защита. В тези случаи предаването на лични данни на тези държави може да се извършва, без да е необходимо някакво специално разрешение.
- 81) 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 територията или на конкретния сектор в третата държава, Комисията следва да вземе предвид как се зачитат в дадената трета държава принципите на правовата държава, достъпът до правосъдие, както и международните норми и стандарти за правата на човека, както и съответното общо и секторно право, включително законодателството в областта на обществената сигурност, отбраната и националната сигурност, а също и обществения ред и наказателното право. При приемането на решение относно адекватността за територия или конкретен сектор в трета държава, следва да се вземат предвид ясни и обективни критерии, като например специфични дейности по обработване и обхвата на приложимите правни стандарти и на действащото законодателство в третата държава. Третата държава следва да предостави гаранции, които осигуряват адекватно ниво на защита, по-специално, когато данните се обработват в един или повече конкретни сектора. Третата държава следва по-специално да осигури ефективен надзор в областта на защитата на данните и да предвиди механизми за сътрудничество с европейските органи по защита на данните, а на субектите на данните следва да бъдат предоставени действителни и приложими права и ефективни средства за административна и съдебна защита.

- (81a) Освен международните ангажменти, които третата държава или международната организация е поела, Комисията също така 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 Европейския комитет по защита на данните при оценяването на нивото на защита в трети държави или международни организации.
- (81б) Комисията следва да наблюдава изпълнението на решенията относно нивото на защита в дадена трета държава или територия или конкретен сектор в трета държава, или в международна организация, включително решения, приети въз основа на член 25, параграф 6 или член 26, параграф 4 от Директива 95/46/ЕО. Комисията следва да направи оценка в рамките на разумен срок на изпълнението на последните решения и да докладва за всякакви отнасящи се до тази оценка констатации на Комитета по смисъла на Регламент (ЕС) № 182/2011, съгласно установеното в настоящия регламент.
- 82) Комисията може (...) да приеме, че дадена трета държава или територия или конкретен сектор в трета държава или дадена международна организация (...) вече не осигуряват 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 членове 42—44. В такъв случай следва да се предвиди провеждането 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.

- 83) При липсата на решение относно адекватността 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 от използването на задължителни фирмени правила, стандартни клаузи за защита на данните, приети от Комисията, стандартни клаузи за защита на данните, приети от надзорния орган или *ad hoc* договорни клаузи, разрешени от надзорния орган, или други уместни и пропорционални мерки, оправдани с оглед на всички обстоятелства около дадена операция по предаване на данни или даден набор от операции по предаване на данни, когато са разрешени от надзорен орган. Тези гаранции следва да осигуряват спазване на изискванията относно защитата на данните и на правата на субектите на данни, включително правото на ефективна административна и съдебна защита. Те следва да се отнасят по-специално до спазването на общите принципи, свързани с обработването на лични данни, наличието на приложими права на субекта на данните и на ефективни правни средства за защита, както и до принципите за защита на данните, още при самото им 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. Следва да има получено разрешение от компетентния надзорен орган, когато гаранциите са предоставени в административни договорености, които нямат задължителен характер.

- 84) 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, включително договор между обработващия лични данни и друг обработващ лични данни, нито да добавят други клаузи или допълнителни гаранции, доколкото 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.
- 85) Дадена корпоративна група или група предприятия, 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 корпоративна група или група предприятия, доколкото такива фирмени правила включват основни принципи и законно приложими права, за да се осигурят подходящи гаранции за предаването или категориите предавания на лични данни.
- 86) Следва да се предвиди възможността да се предават данни при определени обстоятелства, когато субектът на данните е дал изричното си съгласие, когато предаването е в отделен случай във връзка с договор или правна претенция, независимо от това дали е в рамките на съдебна, административна или друга извънсъдебна процедура, включително процедури пред регулатори 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 на държава членка, или когато предаването се извършва от регистрационна система, създадена със закон и предназначена за справки от обществеността или от лица, които имат законен интерес. В този случай предаването не следва да включва всички данни или всички категории данни, съдържащи се в регистрационната система, а когато регистрационната система е предназначена за справка от лица, които имат законен интерес, предаването следва да се извършва единствено по искане на тези лица или ако те са получателите.

- 87) Тези правила 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 адекватността, правото на Съюза или 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. Предаването на международна хуманитарна организация, като например Национално дружество на Червения кръст (...) или Международния комитет на Червения кръст, на лични данни на субект на данни, който е физически или юридически неспособен да даде своето съгласие, с оглед на изпълнението на задача, възложена на Международното движение на Червения кръст и Червения полумесец съгласно Женевските конвенции, и/или на работа за точното прилагане на международното хуманитарно право, приложимо в условията на военни конфликти, може да се счита за необходимо поради важна причина от обществен интерес или от жизненоважен интерес за субекта на данни.

- 88) Предаване на данни, което не може да се окачестви като широкомащабно или често, също може да бъде възможно за целите на законните интереси на администратора или обработващия данни, когато пред тези интереси нямат преимущество интересите или правата и свободите на субекта на данни и когато администраторът или обработващият лични данни е оценил всички обстоятелства около предаването на данните.
- Администраторът или обработващият лични данни следва да обръща специално внимание на естеството на данните, целта и продължителността на предлаганата операция или операции по обработването им, както и на положението в държавата на произход, третата държава или държавата на крайното местоназначение на данните, и на предоставените подходящи гаранции за защита на основните права и свободи на физическите лица при обработването на техните лични данни. За целите на обработването на данни за исторически, статистически и научноизследователски цели следва да се вземат предвид основателните очаквания на обществото за повишаване на познанието. За да се оцени дали дадено предаване е широкомащабно или често, следва да се вземат предвид количеството лични данни и броят на субектите на данни, както и дали предаването се осъществява в отделни случаи или редовно.

- 89) Във всеки случай, когато Комисията не е взела решение относно адекватното ниво на защита на данните в дадена трета държава, администраторът или обработващият данни следва да използва решения, които гарантират на субектите на данни, че ще продължат да се ползват от основните права и гаранциите по отношение на обработването на техните данни в Съюза след предаването на тези данни.
- 90) Някои трети държави прилагат закони, подзаконови актове и други законодателни инструменти, които имат за цел пряко да регулират дейностите по обработване на данни на физически и юридически лица под юрисдикцията на държавите членки. Извънтериториалното прилагане на тези закони, подзаконови актове и други законодателни инструменти 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. Това може, наред с другото, да бъде случаят, когато разкриването е необходимо поради важно основание от обществен интерес, признато в правото на Съюза или на държава членка, на което е подчинен администраторът. (...)
- 91) Трансграничното движение на лични данни извън Съюза може да увеличи риска физическите лица да не могат да упражнят правата на защита на данните, за 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 също 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 разпоредбите на настоящия регламент, включително разпоредбите, установени в глава V.

- 92) Създаването в държавите членки на надзорни органи, оправомощени да изпълняват задачите и упражняват своите правомощия при пълна независимост, е съществен елемент от защитата на физическите лица във връзка с обработването на личните им данни. Държавите членки могат да създават повече от един надзорен орган, за да бъде отразена тяхната конституционна, организационна и административна структура.
- 92a) 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 пък означава, че надзорните органи не могат да бъдат обект на съдебен контрол.
- 93) 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 единно звено за контакт, за да гарантира ефективното участие на тези органи в механизма, както и бързото и безпрепятствено сътрудничество с други надзорни органи, Европейския комитет по защита на данните и Комисията.
- 94) Всеки надзорен орган следва да получи (...) финансовите 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. За всеки надзорен орган следва да има отделен годишен бюджет, който може да е част от общия държавен или национален бюджет.
- 95) Общите условия за члена или членовете на надзорния орган следва да бъдат определени със закон във всяка държава членка и по-специално да предвиждат, че тези членове следва да се назначават от парламента и/или от правителството или от държавния глава на държавата членка или от независим орган, комуто съгласно правото на държавата членка е възложено да прави назначенията посредством прозрачна процедура. За да се гарантира независимостта на надзорния орган, членът или членовете следва 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. (...)

- 95a) 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-конкретно 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 местоживее на негова територия. Това следва да включва разглеждане на жалби, внесени от субекти на данни, водене на разследвания за прилагането на регламента, повишаване на обществената осведоменост за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни.
- 96) Надзорните органи следва да наблюдават прилагането на разпоредбите съгласно настоящия регламент и да допринасят за неговото съгласувано прилагане навсякъде в Съюза с цел защита на физическите лица по отношение на обработването на личните им данни и улесняване на свободното движение на личните данни в рамките на вътрешния пазар. За тази цел настоящият регламент следва да задължава и оправомощава надзорните органи да си сътрудничат помежду си и с Комисията, без да е необходимо споразумение между държавите членки относно предоставянето на взаимопомощ или относно това сътрудничество.

- 97) 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 органи, които са засегнати, тъй като администраторът или обработващият лични данни има място на установяване на територията на тяхната държава членка, тъй като субекти на данни с местоживееие на тяхната територия са съществено засегнати или тъй като до тях е била подадена жалба. Също когато субект на данни, който не е с местоживееие в тази държава членка, е подал жалба, надзорният орган, до който е била подадена такава жалба, следва също да бъде засегнат надзорен орган. В рамките на задачите му да дава насоки по всякакви въпроси, отнасящи се до прилагането на настоящия регламент, Европейският комитет по защита на данните 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 адекватно и обосновано възражение.
- 97a) 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 разпоредбите 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. В случаите, когато решението е за пълно или частично отхвърляне на жалба от субект на данни, това решение се приема от надзорен орган, до който е била подадена жалбата.

97б) Това решение следва да е съгласувано 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 изпълнение на настоящия регламент и 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.

97в) 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 данни на наети лица в контекста на специфично трудово правоотношение в държава членка. В такива случаи надзорният орган следва незабавно да информира за това водещия надзорен орган. След като бъде информиран, водещият надзорен орган следва да реши дали ще се занимае със случая в рамките на механизма „обслужване на едно гише“ или информираният го надзорен орган следва да се занимае със случая на местно равнище. Когато взема това решение, водещият надзорен орган следва да отчита 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 решение спрямо администратора или обработващия лични данни. Когато водещият надзорен орган реши да се занимае със случая, информираният 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 проекторешението си в рамките на механизма „обслужване на едно гише“.

98) Правилата за водещия надзорен орган и механизма за обслужване на едно гише следва да не се прилагат, когато обработването се извършва от публични органи или от частни структури, които действат 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.

99) (...)

100) За да се гарантира съгласуваното 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 налагане на санкции, правомощия за даване на разрешения и становища и, особено в случаи на жалби от физически лица, и без да се засягат правомощията на прокуратурата съгласно националното право, правомощието да довеждат нарушения на настоящия регламент до знанието на съдебните органи и/или да встъпват в съдебни производства. Подобни правомощия следва да включват също правомощието да забрани обработването, за което е била направена консултация с надзорния орган. 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 със съответните процедурни гаранции, определени в правото на Съюза и националното право, независимо, справедливо и в разумен срок. По-специално всяка мярка следва да бъде подходяща, необходима и пропорционална с оглед 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 националното процесуално право, като например изискването за получаване на предварително съдебно разрешение.

Всяка правно обвързваща мярка на надзорен орган следва да бъде в писмен вид, 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 споменава правото на ефективна правна защита. Това следва да не пречи съгласно националното процесуално право да бъдат поставени допълнителни изисквания. Приемането на такова правно обвързващо решение предполага, че то може да породи съдебен контрол в държавата членка на надзорния орган, приел решението.

101) (...)

101a) Когато надзорният орган, до който е подадена жалбата, не е водещият надзорен орган, водещият надзорен орган следва да работи в тясно сътрудничество с надзорния орган, до който е подадена жалбата, в съответствие с разпоредбите за сътрудничество и съгласуваност, установени в настоящия регламент. В такива случаи, когато взема мерки, целящи да породят правни последици, включително налагане на административни глоби, водещият надзорен орган следва да отчита във възможно най-голяма степен становището на надзорния орган, до който 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.

101б) Надзорният орган, който е получил жалба, разкрил е или е бил информиран по друг начин за ситуации, които предполагат възможни нарушения на регламента, следва да се стреми към уреждане на спора по взаимно съгласие, а ако този опит се окаже неуспешен, да упражни целия си набор от правомощия в случаи, когато друг надзорен орган следва да функционира като водещ надзорен орган за дейностите по обработването на администратор или обработващ лични данни, но конкретният предмет на жалбата или възможното нарушение засяга единствено дейностите по обработването на администратора или обработващия лични данни в държавата членка, където е била подадена жалбата, или разкритото възможно нарушение и предметът не засягат съществено или няма вероятност да засегнат съществено субекти на данни в други държави членки. 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, или по отношение на обработване, което се извършва в контекста предлагането на стоки или услуги, специално предназначени за субекти на данни на територията на държавата членка на надзорния орган; или това трябва да се прецени, като се вземат предвид съответните правни задължения съгласно националното право.

102) 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, малките и средните предприятия, както и физическите лица, особено в образователен контекст.

- 103) 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. Когато надзорен орган, който е поискал взаимопомощ и не е получил отговор от замоления надзорен орган в рамките на един месец от получаването на искането, приеме временна мярка, тази временна мярка следва да бъде надлежно обоснована и да е само с временен характер.
- 104) Всеки надзорен орган следва да има правото да участва в съвместни операции на надзорните органи. Надзорният орган, до който е отправено искането, следва да бъде длъжен да отговори в определен срок на искането.
- 105) За да се гарантира съгласуваното 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 *засегнат* надзорен орган или Комисията поиска този въпрос да бъде разгледан чрез механизма за съгласуваност. Механизмът следва да действа, без да се засягат мерките, които Комисията може да предприеме в изпълнение на своите правомощия съгласно Договорите.
- 106) При прилагането на механизма за съгласуваност Европейският комитет по защита на данните следва да излезе със становище в рамките на определен срок, ако такова решение бъде взето с (...) мнозинство на неговите членове или ако това бъде поискано от *засегнат* надзорен орган или от Комисията. Европейският комитет по защита на данните следва също да бъде оправомощен да приема правно обвързващи решения в случай на спорове между надзорни органи. За целта той следва по принцип да взема с мнозинство от две трети от своите членове правно обвързващи решения в точно определени случаи, когато има противоречиви становища сред надзорните органи, по-конкретно в механизма за сътрудничество между водещия надзорен орган и *засегнатите* надзорни органи по съществото на спора, а именно дали е налице нарушение на настоящия регламент или не.
- 107) (...)

- 108) 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 надзорният орган следва да има възможност да приема временни мерки с определен срок на действие, когато прилага механизма за съгласуваност.
- 109) Прилагането на този 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.
- 110) За да се насърчи последователното прилагане на настоящия регламент, Европейският комитет за защита на данните следва да бъде създаден като независим орган на Съюза. За да се изпълнява целите си, Европейският комитет за защита на данните следва да притежава правосубектност. Европейският комитет по защита на данните следва да се представлява от своя председател. Той следва да замени Работната група за защита на лицата при обработването на лични данни, създадена с Директива 95/46/ЕО. Той следва да е съставен от по един ръководител на надзорен орган от всяка държава членка или неговия представител (...). Комисията *и Европейският комитет по защита на данните* следва да участват в дейностите на Европейския комитет по защита на данните без право на глас. Европейският комитет по защита на данните 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 насърчава сътрудничеството на надзорните органи навсякъде в Съюза. Европейският комитет по защита на данните следва да действа независимо при изпълнението на задачите си.

- 110a) Европейският комитет по защита на данните следва да бъде подпомаган от секретариат, осигурен от секретариата на Европейския надзорен орган по защита на данните. Служителите на секретариата на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачите, възложени на Европейския комитет по защита на данните с настоящия регламент, следва да ги изпълняват изключително под ръководството на председателя на Европейския комитет по защита на данните, като му се отчитат. Организационното отделяне на персонала следва да се отнася за всички услуги, необходими за независимото функциониране на Европейския комитет по защита на данните.
- 111) Всеки субект на данни следва да има право да подаде жалба до надзорен орган, по-конкретно в държавата членка на обичайно местопребиваване, както и право на средства за ефективна съдебна защита в съответствие с член 47 от Хартата за основните права, 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 отклонява 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 може да бъде попълнен също и по електронен път, без да се изключват други средства за комуникация.
- 112) 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, което е учредено съгласно правото на държава членка и чиято цел е да защитава правата и интересите на субектите на данни по отношение на защитата на техните данни, да подава жалби от негово име до надзорен орган или да упражнява правото на средства за съдебна защита от името на субектите на данни. Държавите членки могат да предвидят тази структура, организация или сдружение да има право, независимо от възложения от субекта на данни мандат, да подаде в тази държава членка жалба и/или да има право на ефективни средства за правна защита, когато има основания да смята, че (...) правата на субект на данни са били нарушени в резултат на обработване на лични данни, което не е в съответствие с настоящия регламент. Тази структура, организация или сдружение не може да има право да претендира за обезщетение от името на субекта на данни.

113) Всяко физическо или юридическо лице има правото да внася иск за отмяна на решения на Европейския комитет по защита на данните пред Съда на Европейския съюз („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 Европейския комитет по защита на данните засягат пряко и лично администратора, обработващия личните данни или жалбоподателя, те могат да внесат иск за отмяна на тези решения и следва да го направят в срок от два месеца от публикуването им на уебсайта на Европейския комитет по защита на данните, 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 ефективна правна 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 отклоняването или отхвърлянето на жалби. Същевременно това право не обхваща други мерки на 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 националното процесуално 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 отклонена 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, вкл. на настоящия регламент.

Допълнително, в случай на оспорване пред национален съд на решение на надзорен орган, изпълняващ решение на Европейския комитет по защита на данните, и ако валидността на това решение е под въпрос, този национален съд няма правомощието да обявява решението на Европейския комитет по защита на данните за невалидно, но трябва да отнесе въпроса за валидността до Съда в съответствие с член 267 от ДФЕС, съгласно тълкуването на Съда по дело *Foto-frost*¹, тогава когато счете решението за невалидно. Национален съд обаче не може да отнесе въпрос за валидността на решението на Европейския комитет по защита 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.

113а) 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 въпросния 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 последният 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.

114) (...)

115) (...)

¹ Дело C-314/85

116) 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 където пребивава субектът на данни, освен ако администраторът не е публичен орган, който действа в изпълнение на своите публични правомощия.

117) (...)

118) Всички вреди, които дадено лице може да претърпи в резултат на обработване на данни, което не е в съответствие с настоящия регламент, следва да бъдат обезщетени от администратора или обработващия лични данни, който 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 на Европейския съюз по начин, който отразява напълно целите на настоящия регламент. Посоченото по-горе не засяга евентуални иски за вреди, произтичащи от нарушаване на други правила на правото на Съюза или на държавата членка. (...)

Когато се споменава обработване на данни, което не е в съответствие с настоящия регламент, в това се включва и обработване, което не е в съответствие с делегираните актове и актовете за изпълнение, приети в съответствие с настоящия регламент, и националното право, 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 носи отговорност за цялата вреда. Когато обаче те са обединени в едно съдебно производство, в съответствие с националното право, обезщетението може да се разпредели съобразно отговорността на всеки администратор или обработващ лични данни за причинената от обработването вреда, при условие че на претърпелия вреда субект бъде осигурено пълно и действително обезщетение. Всеки администратор или обработващ лични данни, който е (...) изплатил пълно обезщетение, може впоследствие да предяви регресивен иск срещу другите администратори или обработващи лични данни, участвали в същото обработване.

118a) 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 компенсация, срещу администратор или обработващ лични данни, общите правила относно компетентността като правилата, предвидени в Регламент (ЕС) № 1215/2012, не следва да засягат прилагането на тези специфични правила.

- 118б) За да се укрепи прилагането на разпоредбите на настоящия регламент, освен или вместо подходящи мерки, наложени от надзорния орган съгласно настоящия регламент, при нарушение на регламента могат да се налагат санкции и административни глоби. 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 *предими* нарушения, имащи отношение, 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 и административни глоби следва да подлежи на адекватни процедурни мерки за защита в съответствие с общите принципи на правото на Съюза и Хартата на основните права, включително ефективна съдебна защита и справедлив съдебен процес. Когато националното право на дадена държава членка не предвижда административни глоби, тази държава членка може да се въздържа от предвиждането на административни глоби за нарушения на настоящия регламент, когато тези нарушения са предмет на наказателни санкции в националното право, като гарантира, че наказателните санкции са ефективни, съразмерни и възпиращи и при отчитане на размера на административните глоби, предвидени в настоящия регламент.
- 119) Държавите членки могат да установят разпоредби относно наказателни санкции за нарушения на настоящия регламент, включително за нарушения на националните разпоредби, приети по силата и в рамките на настоящия регламент. Тези наказателни санкции могат да предвиждат отнемане на облагите, получени в резултат на нарушаване на настоящия регламент. Налагането на наказателни санкции за нарушения на тези национални правила и на административни санкции обаче не следва да води до нарушаване на принципа *ne bis in idem* съгласно тълкуването на Съда на Европейския съюз.

120) С цел да се засилят и хармонизират административните санкции за нарушения на настоящия регламент, всеки надзорен орган следва да има правомощието да налага административни глоби. В настоящия регламент следва да се посочат нарушенията, максималният размер и критериите за определяне на съответните административни глоби, 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 регламента и за да се предотвратят или смекчат последиците от нарушението. При налагането на глоби на лица, които не са търговски предприятия, за да определи подходящия размер на глобата, надзорният орган следва да има предвид общото равнище на доход в съответната държава членка. Механизмът за съгласуваност може да се използва също за утвърждаването на съгласувано прилагане на административните глоби. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни глоби. Налагането на административна глоба или отправянето на предупреждение не засяга упражняването на други правомощия на надзорните органи или прилагането на други санкции по регламента.

120a) Когато административните санкции не са хармонизирани в настоящия регламент или при необходимост в други случаи, като например при сериозни нарушения на регламента, 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 националното право.

121) Правото на държавите членки следва да съвместява разпоредбите, уреждащи свободата на изразяване и информация, включително за журналистически, академични, художествени или литературни цели, и правото на защита на личните данни по настоящия регламент. Обработването на лични данни за журналистически цели или за художествено, академично 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 и информация, гарантирано в член 11 от Хартата на основните права на Европейския съюз. 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 изключенията и дерогациите, необходими за постигането на баланс между тези основни права. Държавите членки следва да приемат такива изключения и дерогации относно общите принципи, относно правата на субекта на данните, относно администратора на лични данни и обработващото лице, относно предаването на данни на трети държави или международни организации, относно независимите надзорни органи и относно сътрудничеството и съгласуваността. В случай че тези изключения или дерогации се различават в отделните държави членки, следва да се прилага националното право на държавата членка, на което се подчинява администраторът на лични данни. За да се вземе предвид важността на правото на свобода на изразяване във всяко демократично общество, е необходимо свързаните с тази свобода понятия, като журналистиката например, да се тълкуват широко. (...)

121a) Настоящият регламент дава възможност при прилагане на неговите разпоредби да се взема предвид принципът на публичен достъп до официални документи. Публичният достъп до официални документи може да се разглежда като 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 законодателството на Съюза или 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 общественния сектор с правото на защита на личните данни и следователно може да осигурява необходимите дерогации от правилата на настоящия регламент. Във връзка с това позоваването на публични органи и структури включва всички органи или други структури, обхванати от законодателството на държавата членка относно публичния достъп до документи. Директива 2003/98/ЕО на Европейския парламент и на Съвета от 17 ноември 2003 г. относно повторната употреба на информацията в общественния сектор 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-конкретно, тази директива следва да не 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 със закона за защита на физическите лица по отношение на обработката на лични данни.

122) (...)

123) (...)

124) В националното право или в колективните споразумения (включително „трудови споразумения“) могат да се предвиждат специални разпоредби относно обработването на личните данни на наетите лица по трудово правоотношение, по-специално 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 упражняване и ползване на индивидуална или колективна основа на правата и облагите от заетостта, а също и за целите на прекратяване на трудовото правоотношение.

125) Обработването на лични данни за исторически, статистически или научни (...) цели и за целите на архивирането в интерес на обществото (...) освен на общите принципи и конкретните правила на настоящия регламент, по-специално по отношение на условията за законосъобразно обработване, следва да съответства и на друго, имащо отношение към този въпрос законодателство, например относно клиничните изпитвания. Допълнителното обработване на лични данни за исторически, статистически и научни цели, както и за целите на архивирането в интерес на обществото (...) следва да не се счита за несъвместимо с целите, за които първоначално са събрани данните, и може да се обработват за тези цели по-дълго, отколкото е необходимо за първоначалната цел (...). На държавите членки следва да бъде разрешено да осигуряват, при конкретни условия и подходящи гаранции за субектите на данните, спецификации и дерогации по отношение на изискванията за информация и правата на достъп, коригиране, заличаване, правото „да бъдеш забравен“, правото на ограничение на обработването и на преносимост на данните и правото на възражение при обработването на лични данни за исторически, статистически или научни цели и за целите на архивирането (...) 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.

125a) (...).

- 125aa) Чрез съчетаване на информацията от регистрите научните изследователи могат да придобият нови познания с голяма стойност, например когато става дума за широко разпространени заболявания като сърдечносъдовите заболявания, рака, депресията и т.н. 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 въздействие на редица социални условия, напр. безработица, образование и съчетаването на тази информация с останалите условия на живот. Резултатите от научните изследвания, получени въз основа на 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 и т.н.
- С цел улесняване на научните изследвания, личните данни могат да бъдат обработвани за научни цели при подходящи условия и гаранции, определени от правото на държавите членки или правото на Съюза. Това означава, че по отношение на обработването за научни цели следва да не е необходимо съгласието на субекта на данните за всяко следващо обработване.
- 125б) Значението на архивите, за да се разбере историята и културата на Европа и фактът, че „добре съхранените и достъпни архиви допринасят за демократичното функциониране на нашите общества“, бяха изтъкнати в Резолюцията на Съвета от 6 май 2003 г. относно архивите на държавите членки². 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 на държавата членка, имат законово задължение да получават, съхраняват, оценяват, организират, описват, разпространяват и предоставят достъп до регистри с непреходна стойност в интерес на обществото, както и да предоставят информация за тях и да насърчават тяхното поддържане. Освен това на държавите членки следва да се разреши да предвидят допълнителното 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.

² ОБ С 113, 13.5.2003 г., стр. 2.

Кодексите за поведение могат да допринесат за правилното прилагане на настоящия регламент, включително когато личните данни се обработват за целите на архивирането в интерес на обществото, като се определят допълнително подходящи гаранции за правата и свободите на субекта на данните. Такива кодекси следва да се изготвят от официалните служби по архивите на държавите членки или от Европейската група по архивите. Що се отнася до международното предаване на лични данни, съхранявани в архивите, то трябва да се осъществява, без да се засягат действащите европейски и национални правила за движението на продукти на културата и национални богатства.

126) Когато се обработват лични данни за научни цели, настоящият регламент следва да се прилага и за този вид обработване. За целите на настоящия регламент обработването на лични данни за научни цели следва да включва фундаменталните научни изследвания, приложните научни изследвания и частно финансираните научни изследвания, а освен това следва да се отчита и заложената в член 179, параграф 1 от Договора за функционирането на Европейския съюз цел за изграждането на европейско научноизследователско пространство. Научните цели следва да включват и проучвания, провеждани в интерес на обществото в областта на общественото здраве. С оглед на особеностите на обработването на лични данни за научни цели следва да се прилагат специални условия, по-конкретно по отношение на публикуването или оповестяването по друг начин на лични данни в контекста на научните 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.

126a) Когато се обработват лични данни за исторически цели, настоящият регламент следва да се прилага и за този вид обработване. Това следва да включва също исторически научни изследвания и научни изследвания за генеалогични цели, като се има предвид че настоящият регламент следва да не се прилага за починали лица.

126б) 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.

126в) 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 държавите членки следва да определи 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.

126г) 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 Договора за функционирането на Европейския съюз, докато националната статистика следва да съответства и на националното право.

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 на Европейския парламент и на Съвета за предоставянето на поверителна статистическа информация на Статистическата служба на Европейските общности, Регламент (ЕО) № 322/97 на Съвета относно статистиката на Общността и Решение 89/382/ЕИО, Евратом на Съвета за създаване на Статистически програмен комитет на Европейските общности конкретизират допълнително изискванията относно поверителността на данните на европейската статистика.

127) По отношение на правомощията на надзорните органи да получават от администратора на лични данни или обработващото лице достъп до лични данни и достъп до помещенията му, 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 прилагат професионална тайна, когато това се изисква от правото на Съюза.

128) 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 Договора за функционирането на Европейския съюз. (...).

- 129) За 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 Договора за функционирането на Европейския съюз. По-специално делегирани актове следва да бъдат приети по отношение на (...); критериите и изискванията за механизмите за сертифициране; (...); (...) 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 Съвета.
- 130) За да се гарантират еднакви условия за изпълнение на настоящия регламент, на Комисията следва да бъдат предоставени изпълнителни правомощия за: (...); 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 или територия, или обработващ данни сектор в тази трета държава, или международна организация; приемане на стандартни клаузи за защита на данните; формати и процедури за обмен на информация между администраторите, обработващите лични данни и надзорните органи за задължителните фирмени правила; (...) взаимопомощ; (...); договорености за обмен на информация чрез електронни средства между надзорните органи, както и между надзорните органи и Европейския комитет по защита на данните. Тези правомощия следва да бъдат упражнявани в съответствие с 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. В този контекст Комисията следва да обмисли специалните мерки за микропредприятията, малките и средните предприятия.

- 131) 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 или територия, или обработващ данни сектор в тази трета държава, или международна организация; приемане на стандартни клаузи за защита на данните; формати и процедури за обмена на информация чрез електронни средства между администраторите, обработващите лични данни и надзорните органи за задължителните фирмени правила; взаимопомощ; (...); договорености за обмена на информация чрез електронни средства между надзорните органи, както и между надзорните органи и Европейския комитет по защита на данните, при условие че тези актове са от общ характер.
- 132) Комисията следва да приеме актове за изпълнение с незабавно приложение, когато в надлежно обосновани случаи, свързани с трета държава или територия или обработващ данни сектор в тази трета държава, или международна организация, които не осигуряват адекватно ниво на защита (...), наложителни причини за спешност изискват това.
- 133) Тъй като целите на настоящия регламент, а именно осигуряване на еквивалентно ниво на защита на физическите лица и свободното движение на данни навсякъде в Съюза, не могат да бъдат постигнати в достатъчна степен от държавите членки и следователно могат, поради обхвата или последиците от предвиденото действие, да бъдат по-добре постигнати на равнището на Съюза, Съюзът може да приема мерки в съответствие с принципа на субсидиарност, установен в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, установен в посочения член, настоящият регламент не надхвърля необходимото за постигането на тези цели.

- 134) Директива 95/46/ЕО следва да бъде отменена с настоящия регламент. Обработването на данни, което вече е в ход към датата на влизане в сила на настоящия регламент, следва да се приведе в съответствие с него в срок от две години, след което регламентът влиза в сила. Когато обаче това обработване на данни е в съответствие с Директива 95/46/ЕО, изискванията на настоящия регламент относно извършването на оценки на въздействието върху защитата на личните данни и предварителната консултация с надзорния орган следва да не се прилагат за дейностите по обработване, които са в ход преди влизането в сила на настоящия регламент, предвид това, че тези изисквания, поради тяхното естество, би трябвало да са изпълнени преди да започне обработването на данни. Когато обработването на данни е в съответствие с Директива 95/46/ЕО, субектът на данни не е необходимо също да дава отново съгласието си, за да може администраторът да продължи обработването на данни след датата на прилагането 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.
- 135) 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, 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 (...).
- 136) (...)
- 137) (...)
- 138) (...).
- 139) (...)

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ГЛАВА I

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и цели

1. С настоящия регламент се определят правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни, 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.
- 2а. Държавите членки могат да запазят или да въведат по-конкретни разпоредби, за да адаптират прилагането на правилата на настоящия регламент по отношение на обработването на лични данни, необходимо за спазването на законово задължение или за изпълнението на задачи от обществен интерес, или при упражняването на официални правомощия, предоставени на администратора на лични данни, или в други особени случаи на обработване, предвидени в член 6, 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. 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 на лични данни или които са предназначени да съставляват част от регистър на 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 институциите, органите, службите и агенциите на Съюза;
- в) от държавите членки, когато извършват дейности, които попадат в приложното поле на дъл V, глава 2 от Договора за Европейския съюз;
- г) когато се извършва от физическо лице в хода на (...) лични или домашни дейности;
- д) от компетентните (...) органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления, изпълнението на наказателни санкции или предпазването от заплахи за обществената сигурност и предотвратяването им.

3. (...)

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.
2. Настоящият регламент се прилага за обработването на лични данни на субекти на данни с местоживее в Съюза от администратор, 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 Европейския съюз.
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 националното право 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 или идентифицируемо физическо лице („субект на данни“); идентифицируемо лице 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 неговата физическа, физиологична, генетична, психическа, икономическа, културна или социална идентичност.
- 2а) (...)
- 3) „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на предоставяне на данните, поддръждане или комбиниране (...) ограничаване, заличаване или унищожаване;
- 3а) „ограничаване на обработването“ означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;
- 3б) „псевдонимизация“ означава обработването на лични данни по такъв начин, че данните не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, доколкото тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира невъзможността да се направи връзка с идентифицирано лице или с лице, което може да бъде идентифицирано (...).
- 4) „регистър на 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;

- 5) „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 обработването се определят от правото на Съюза или на държава членка, администраторът или специалните критерии за неговото назначаване могат да бъдат определени в правото на Съюза или в правото на държава членка;
- 6) „обработващ лични данни“ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;
- 7) „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 органите, които могат да получават данни в рамките на конкретно разследване, не се считат за получатели;
- 8) „съгласие на субекта на данните“ означава всяко свободно изразено, конкретно и информирано (...) 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;
- (9) „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;
- (10) „генетични данни“ означава всички лични данни, свързани с генетичните белези на дадено физическо лице, наследени или придобити (...), които дават уникална информация за отличителните черти или здравето на това физическо лице и са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;
- 11) „биометрични данни“ означава всички 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 лице, като лицеви изображения или дактилоскопични данни;

- 12) „данни за здравословното състояние“ означава данни, свързани с физическото или психическото здраве на физическо лице, които дават информация за здравословното му състояние;
- 12а) „профилиране“ означава всяка форма на автоматизирано обработване на лични данни, изразяващо се в използване на тези данни за оценяване на лични аспекти, свързани с физическо лице, и по-конкретно за анализиране и прогнозиране на аспекти, отнасящи се до изпълнението на професионалните задължения, икономическото състояние, здравето, личните предпочитания или интереси, надеждността или поведението, местоположението или движението;
- 12б) (...)
- 13) „основно място на установяване“ означава
- по отношение на администратор, установен в повече от една държава членка — мястото, където се намира главното 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 този случай мястото на установяване, където са взети тези решения, се счита за основно място на установяване.
 - по отношение на обработващ лични данни, установен в повече от една държава членка — мястото, където се намира главното му управление в Съюза, а ако обработващият лични данни няма главно 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;
- 14) „представител“ означава всяко физическо или юридическо лице, установено в Съюза, което, (...) назначено от администратора в писмена форма съгласно член 25, представлява администратора във връзка със задълженията на администратора по настоящия регламент (...);
- 15) „предприятие“ означава всяко физическо или юридическо лице, което осъществява икономическа дейност, независимо от правната му форма, (...) включително (...) партньорствата или сдруженията, които редовно осъществяват икономическа дейност;

- 16) „група предприятия“ означава контролиращо предприятие и контролираните от него предприятия;
- 17) „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 на Съюза, 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 предприятия, развиващи съвместна икономическа дейност;
- 18) (...)
- 19) „надзорен орган“ означава независим публичен орган, създаден от държава членка съгласно член 46;
- 19а) „засегнат надзорен орган“ означава
— надзорен орган, който е засегнат от обработването, тъй като:
а) администраторът или обработващият лични данни е установен на територията на държавата членка на този надзорен орган;
б) субектите на данни с местоживееене в тази държава членка са засегнати съществено или е вероятно да бъдат засегнати съществено от обработването;
или
в) жалбата, поради която се извършва обработването, е подадена до този надзорен орган.
- 19б) „транснационално обработване на лични данни“ означава или:
а) обработване, 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, 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.

19в) „адекватно и обосновано възражение“ означава:

възражение за това дали е налице нарушение на настоящия регламент или не,
или — в зависимост от случая — дали предвижданото действие по отношение
на администратора или обработващия лични данни е в съответствие с
регламента. Възражението трябва ясно да доказва, че проектът за решение
води до значителни рискове за основните права и свободи на субектите на
данни и за свободното движение на лични данни, където е приложимо.

20) „услуга на информационното общество“ означава всяка услуга по смисъла на
член 1, параграф 2 от Директива 98/34/ЕО на Европейския парламент и на
Съвета от 22 юни 1998 г. за определяне на процедура за предоставяне на
информация в областта на техническите стандарти и регламенти, както и на
правила относно услугите на информационното общество.

21) „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 II

ПРИНЦИПИ

Член 5

Принципи, свързани с обработването на лични данни

1. Личните данни трябва да бъдат:

- а) обработвани законно, добросъвестно и по прозрачен начин по отношение на субекта на данните;
- б) събирани за конкретни, изрично указани и законни цели и да не се обработват допълнително по начин, несъвместим с тези цели; допълнителното обработване на лични данни за целите на архивирането в интерес на обществото, или за научни, статистически или исторически цели не се счита, съгласно член 83, за несъвместимо с първоначалните цели;
- в) подходящи, релевантни и да не надвишават необходимото за целите, за които (...) се обработват;
- г) точни и при необходимост актуализирани; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното заличаване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;
- 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 за целите на архивирането в интерес на обществото, или за научни, статистически или исторически цели съгласно член 83, при условие че бъдат приложени съответните технически и организационни мерки, предвидени в регламента с цел да бъдат гарантирани правата и свободите на субекта на данните;
- дд) обработвани по начин, който гарантира подходящо ниво на сигурност на личните данни.
- е) (...)

2. Администраторът носи отговорност за спазването на параграф 1.

Член 6

Законосъобразност на обработването

1. Обработването на лични данни е законосъобразно само ако и доколкото е приложимо поне едно от следните условия:
 - а) субектът на данните е дал недвусмислено 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 мерки по искане на субекта на данните преди сключването на договор;
 - в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора на лични данни;
 - г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго лице;
 - д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора на лични данни;
 - е) обработването е необходимо за целите на законните интереси на администратора на лични данни 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. (...).
2. Обработването на лични данни, което е необходимо за целите на архивирането в интерес на обществото или за исторически, статистически или научни цели, е законосъобразно, при условие че са спазени също условията и гаранциите, посочени в член 83.

3. Основанието за обработването, посочено в параграф 1, букви в) и д), трябва да бъде установено в съответствие със:

- а) правото на Съюза или
- б) националното право на държавата членка, което се прилага спрямо администратора на лични данни.

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 свързана с упражняването на официални правомощия, които са предоставени на администратора на лични данни. Това правно основание може да включва конкретни разпоредби за адаптиране на прилагането на разпоредбите на настоящия регламент, наред с останалото, общите условия, които определят законосъобразността на обработването на данните от администратора на лични данни, вида данни, които подлежат на обработване, съответните субекти на данни; образуванията, пред които могат да бъдат разкривани 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, в това число за други конкретни случаи на обработване съгласно предвиденото в глава IX.

За. За да се увери дали целта на допълнителното обработване (...) е съвместима с първоначалната, за която са събрани данните, освен ако субектът на данните е дал съгласие, администраторът на лични данни наред с другото взема под внимание:

- а) всяка връзка между целите, за които са били събрани данните, и целите на предвиденото допълнително обработване;
- б) контекста, в който са били събрани данните;
- в) естеството на личните данни, по-специално дали се обработват специални категории лични данни съгласно член 9;
- г) възможните последствия на предвиденото допълнително обработване за субектите на данните;
- д) наличието на подходящи гаранции.

4. Когато целта на допълнителното обработване не е съвместима с тази, за която личните данни са били събрани от същия администратор, допълнителното обработване трябва да има за правно основание поне едно от основанията, посочени в параграф 1, букви а)–д). Допълнително обработване от същия администратор за несъвместими цели, въз основа на законните интереси на този администратор или на трета страна, е законосъобразно, ако тези интереси имат преимущество пред интересите на субекта на данните.
5. (...)

Член 7

Условия за даване на съгласие

1. Когато се прилага член 6, параграф 1, буква а), администраторът е в състояние да докаже, че субектът на данни е дал недвусмислено съгласие.
- 1а. Когато се прилага член 9, параграф 2, буква а), администраторът е в състояние да докаже, че субектът на данни е дал изричното си съгласие.
2. Ако съгласието на субекта на данните трябва да бъде дадено в рамките на писмена декларация, която се отнася и до други въпроси, искането за съгласие трябва да бъде представено по начин, който ясно да го отличава (...) от другите въпроси, да бъде в разбираема и лесно достъпна форма, с използването на ясен и прост език.
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.
4. (...)

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 деца на услуги на информационното общество, обработването на личните данни на дете (...) е законосъобразно, само ако и доколкото такова съгласие е дадено или разрешено от носещия родителска отговорност за детето или е дадено от детето при обстоятелства, които се считат за валидни съгласно правото на Съюза или на държавата членка.
- 1а. 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.
2. Параграф 1 не засяга общото договорно право на държавите членки като разпоредбите относно действителността, сключването или последиците от даден договор по отношение на дете.
3. (...)
4. (...)

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, членство в синдикални организации, както и обработването на генетични данни или на данни, свързани със здравето или сексуалния живот (...).
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 (...), освен когато в правото на Съюза или на държава членка се предвижда, че посочената в параграф 1 забрана не може да бъде отменена от субекта на данни; или

- 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 на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции; или
- в) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие; или
- 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 данните не се разкриват без съгласието на субектите на данните; или
- д) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните (...); или
- е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи; или
- ж) обработването е необходимо по (...) съображения от обществен интерес и се основава на правото на Съюза или на държава членка, в което се предвиждат подходящи и конкретни мерки за гарантиране на законните интереси на субекта на данните; или
- 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 на държава членка или съгласно договор с медицинско лице и при условията и гаранциите, посочени в параграф 4; или
- за) (...);

зб) обработването е необходимо по 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 на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните; или

и) обработването е необходимо за целите на архивирането в интерес на обществото или за исторически, статистически, или научни (...) цели и при спазване на условията и гаранциите, установени в правото на Съюза или на държавата членка, включително посочените в член 83.

й) (...)

3. (...)

4. Личните данни, посочени в параграф 1, могат да бъдат обработвани въз основа на правото на Съюза или на държавата членка 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 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 на държавата членка или правилата, установени от националните компетентни органи.

4а. (...).

5. Държавите членки могат да запазят или да въведат по-специфични разпоредби по отношение на генетичните или здравните данни. Това включва възможността държавите членки да (...) въведат допълнителни условия за обработването на тези данни.

Член 9а

Обработване на данни, свързани с присъди и престъпления

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

Член 10

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 или да се сдобие с (...) допълнителна информация, нито да предприеме допълнително обработване, за да идентифицира субекта на данни с единствената цел да бъде спазен (...) настоящият регламент.(...)
2. Когато в такива случаи администраторът не е в състояние да идентифицира субекта на данните, членове 15, 16, 17, 17а, 17б и 18 не се прилагат, освен когато субектът на данните, с цел да упражни правата си по тези членове, предостави допълнителна информация, позволяваща неговото идентифициране.

ГЛАВА III
ПРАВА НА СУБЕКТА НА ДАННИ

РАЗДЕЛ 1
ПРОЗРАЧНОСТ И УСЛОВИЯ

Член 11

Прозрачна информация и комуникация

1. (...)
2. (...)

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 14 и 14а и на всякаква комуникация по членове 15—19 и член 32 относно обработването на лични данни на субекта на данни в разбираема и лесно достъпна форма, като използвайки и недвусмислени формулировки. Информацията се предоставя писмено или по друг начин, и когато е целесъобразно — електронно. Когато субектът на данните подава искането в електронна форма, информацията по правило може да се предостави в електронна форма, освен ако субектът на данните не е поискал друго. Ако субектът на данните е поискал това, информацията може да бъде дадена устно, при положение, че е доказана идентичността на субекта на данните.
- 1а. Администраторът съдейства за упражняването на правата на субекта на данните по членове 15—19. (...) В случаите, посочени в член 10, параграф 2, администраторът не отказва да предприеме действия по искане на субекта на данните за упражняване на правата му по членове 15—19, освен ако докаже, че не е в състояние да идентифицира субекта на данните.
2. Администраторът предоставя на субекта на данни (...) информация относно действията, предприети във връзка с искане по член 15 и членове 16—19 без излишно забавяне и най-късно до един месец от получаването на искането (...). При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността на искането и броят на исканията. Когато се прилага удълженият срок, в срок от един месец от получаване на искането субектът на данни се уведомява за причините за забавянето.

3. Ако администраторът не предприеме действия по искането на субекта на данни, администраторът уведомява субекта на данни без излишно забавяне и най-късно в срок от един месец от получаването на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган (...).
4. Информацията по членове 14 и 14а (...) и всяка комуникация по членове 16—19 и член 32 се предоставя безплатно. Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторемост, администраторът (...) може да откаже да предприеме действия по дадено искане. В този случай администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.
- 4а. Без да се засягат разпоредбите на член 10, когато администраторът има основателни опасения във връзка със самоличността на лицето, което подава искане по членове 15—19, администраторът може да поиска предоставянето на допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.
5. (...)
6. (...)

Член 13

Права по отношение на получателите

(...)

РАЗДЕЛ 2

ИНФОРМАЦИЯ И ДОСТЪП ДО ДАННИ

Член 14

Информация, предоставяна при събиране на 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 (...) представя на субекта на данните следната информация:
 - а) идентификацията и координатите за връзка на администратора, на представителя на администратора, ако има такъв, администраторът включва и координатите за връзка на длъжностното лице по защита на данните, ако има такава;
 - б) целите на обработването, за което личните данни са предназначени (...), както и правното основание за обработването.
- 1а. Освен информацията, посочена в параграф 1, в момента на получаване на личните данни администраторът предоставя на субекта на данните допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване на данните (...), като се вземат предвид конкретните обстоятелства и контекст, в които се обработват личните данни:
 - а) (...);
 - б) когато обработването се извършва въз основа на член 6, параграф 1, буква е), законните интереси, преследвани от администратора или от трета страна;
 - в) получателите или категориите получатели на личните данни;
 - г) когато е приложимо, информация, че администраторът възнамерява да предаде лични данни на получател в трета държава или международна организация;

- д) съществуването на право да се изиска от администратора достъп до личните данни, свързани със субекта на данните, както и коригирането, заличаването или ограничаването на обработването на лични данни, или да се изрази възражение срещу обработването на такива лични данни (...), както и правото на преносимост на данните;
- да) 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;
- е) правото на жалба до надзорен орган (...);
- ж) 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 данните и евентуалните последиствия, ако тези данни не бъдат предоставени;
- з) *съществуването на автоматизирано вземане на решения, включващо профилирането, посочено в член 20, параграфи 1 и 3, и информацията относно (...) използваната логика, както и значението и предвидените последиствия от това обработване за субекта на данните.*

16. Когато администраторът на данни възнамерява допълнително да обработва данните (...) за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това допълнително обработване информация за въпросната друга цел и всякаква друга необходима информация, както е посочено в параграф 1а.

2. (...)

3. (...)

4. (...)

5. Параграфи 1, 1а и 1б не се прилагат, когато и доколкото субектът на данните вече разполага с информацията.
6. (...)
7. (...)
8. (...)

Член 14а

Информация, предоставяна, когато данните идват от субекта на данните

1. Когато личните данни не идват от субекта на данните, администраторът предоставя на субекта на данните следната информация:
- а) идентификацията и координатите за връзка на администратора, на представителя на администратора, ако има такъв; администраторът включва и координатите за връзка на длъжностното лице по защита на данните, ако има такава;
 - б) целите на обработването, за което личните данни са предназначени, както и правното основание за обработването.
2. Освен информацията, посочена в параграф 1, администраторът предоставя на субекта на данните допълнителна информация, която е необходима за осигуряване на добросъвестно и прозрачно обработване на данните по отношение на субекта на данните, като се вземат предвид конкретните обстоятелства и контекст, в които се обработват личните данни (...):
- а) съответните категории лични данни;
 - б) (...)

- в) когато обработването се извършва въз основа на член 6, параграф 1, буква е), законните интереси, преследвани от администратора или от трета страна;
- г) получателите или категориите получатели на личните данни;
- га) когато е приложимо, информация, че администраторът възнамерява да прехвърли лични данни на получател в трета държава или на международна организация;
- д) съществуването на право да се изиска от администратора достъп до личните данни, свързани със субекта на данните, както и коригирането, заличаването или ограничаването на обработването на лични данни, и да се направи възражение срещу обработването на такива лични данни, както и правото на преносимост на данните (...);
- да) 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;
- е) правото на жалба до надзорен орган (...);
- ж) източникът на личните данни, освен ако данните не са от публично достъпен източник;
- з) *съществуването на автоматизирано вземане на решения, включващо профилирането, посочено в член 20, параграфи 1 и 3, и 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 данните, но най-късно до един месец, като се отчитат конкретните обстоятелства, при които данните се обработват, или

- б) ако е предвидено разкриване пред друг получател, най-късно при разкриването на данните за първи път.

3а. Когато администраторът на данни възнамерява допълнително да обработва данните (...) за цел, различна от тази, за която са събрани, той предоставя на субекта на данните преди това допълнително обработване информация за въпросната друга цел и всякаква друга необходима информация, както е посочено в параграф 2.

4. Параграфи 1—3а не се прилагат, когато и доколкото:

- а) субектът на данните вече разполага с информацията; или
- б) предоставянето на такава информация (...) се оказва невъзможно или изисква непропорционално големи усилия ; в такива случаи администраторът взема подходящи мерки за защита на правата, свободите и законните интереси на субекта на данните; или
- в) получаването или разкриването е изрично разрешено от правото на Съюза или 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) (...);
- д) данните трябва да останат поверителни в съответствие с правото на Съюза или на държавата членка (...).

5. (...)

6. (...)

Член 15

Право на достъп за субекта на данните

1. Субектът на данните има право да получи от администраторана разумни интервали и безплатно (...) потвърждение дали се обработват лични данни, свързани с него, и ако такива лични данни се обработват, да получи достъп до данните и следната информация:
 - а) целите на обработването;
 - б) (...)
 - 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, предвиденият срок, за който ще се съхраняват личните данни;
 - д) съществуването на право да се изиска от администратора достъп до личните данни, свързани със субекта на данните, както и тяхното коригиране, заличаване или ограничаване на обработването на лични данни, или да се изрази възражение срещу обработването на такива лични данни;
 - 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) при решения въз основа наавтоматизиранообработване, включващо профилиране, посочено в член 20, параграфи 1 и 3, информация за използваната логика, както и за значението и предвидените последици от такова обработване.
- 1а. 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 42 във връзка с предаването.

- 1б. При поискване и без това да е свързано с прекомерни разходи, администраторът предоставя на субекта на данните копие от личните данни, които са в процес на обработване.
2. (...)
- 2а. Правото на получаване на копие, посочено в параграф 1б (...), не се прилага, когато такова копие не може да бъде предоставено, без да се разкрият лични данни на други субекти на данни или поверителни данни на администратора. Освен това, посоченото право не се прилага, когато разкриването на лични данни би нарушило правата върху интелектуалната собственост във връзка с обработването на тези лични данни.
3. (...)
4. (...)

РАЗДЕЛ 3

КОРИГИРАНЕ И ЗАЛИЧАВАНЕ

Член 16

Право на коригиране

1. (...) Субектът на данни има право да поиска от администратора да коригира, без излишно забавяне, неточните лични данни, свързани с него. Като се имат предвид целите, за които се обработват данните, субектът на данните има право непълните лични данни да бъдат попълнени, включително чрез добавяне на декларация (...).
2. (...)

Член 17

Право на заличаване и „да бъдеш забравен“

1. Администраторът (...) е задължен да заличи личните данни без излишно забавяне, особено що се отнася до личните данни, които са събрани, когато субектът на данните е бил дете, а субектът на данните има право да поиска от администратора да заличи негови лични данни, без излишно забавяне, на едно от следните основания:
 - а) данните 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 на данните;
 - в) субектът на данните възразява срещу обработването на личните данни съгласно член 19, параграф 1 и няма законни основания за обработването, които да имат преимущество, или субектът на данните възразява срещу обработването на личните данни съгласно член 19, параграф 2;

- г) данните са били обработвани незаконосъобразно;
- д) заличаването е необходимо за спазването на правно задължение, което се прилага спрямо администратора;
- 1а Субектът на данни има и правото да получи от администратора заличаване на неговите лични данни, без излишно забавяне, ако данните са били събрани във връзка с предлагането на услуги на информационното общество, посочено в член 8, параграф 1.
- (...)
2. (...)
- 2а. *Когато администраторът (...) е направил личните данни обществено достояние и е задължен съгласно параграф 1 да заличи данните, той, като отчита наличната технология и разходите по изпълнението, предприема (...) разумни стъпки, включително технически мерки, (...) за да уведоми администраторите, обработващи данните, че субектът на данните е поискал заличаване от тези администратори на всички връзки, копия, или реплики на тези лични данни.*
3. Параграфи 1, 1а и 2а не се прилагат доколкото (...) обработването на лични данни е необходимо:
- а. за упражняване на правото на свобода на изразяването и правото на информация;
- б. за спазване на правно задължение, което изисква обработване на лични данни, предвидено в правото на Съюза или 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 зб), както и член 9, параграф 4;
- г. за целите на архивирането в интерес на обществото или занаучни, статистически и исторически (...) цели в съответствие с член 83;

д. (...)

е. (...)

ж. за установяването, упражняването или защитата на правни претенции.

4. (...)

5. (...)

Член 17a

Право на ограничение за обработването

1. Субектът на данните има право да получи от администратора ограничение за обработването на личните данни, когато:
 - а) точността на данните се оспорва от субекта на данните, за срок, който позволява на администратора да провери точността на данните;
 - б) 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; или
 - в) субектът на данните и възразил срещу обработването съгласно член 19, параграф 1 в очакване на проверка дали законните основания на администратора имат преимущество пред интересите на субекта на данните.
2. (...)
3. Когато обработването на лични данни е ограничено съгласно параграф 1, такива данни могат, с изключение на тяхното съхранение, да бъдат обработвани 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.

4. Когато субект на данните е получил ограничение за обработването съгласно параграф 1, (...) администраторът го информира преди вдигането на ограничението за обработване.
5. (...)
- 5a. (...)

Член 17б

Задължение за уведомяване при коригиране, заличаване или ограничаване

Администраторът съобщава всяко извършено в съответствие с член 16, член 17, параграф 1 и член 17а коригиране, заличаване или ограничение за обработване на всеки получател, на когото данните са били разкрити (...), освен ако това е невъзможно или изисква непропорционално големи усилия.

Член 18

Право на преносимост на данните

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

2а. Упражняването на това право не засяга член 17. Правото по параграф 2 не се отнася до обработването, необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора.

2аа. Правото по параграф 2 не се прилага, ако разкриването на лични данни ще наруши правата върху интелектуалната собственост във връзка с обработването на въпросните лични данни.

3. (...)

4. (...)

РАЗДЕЛ 4

ПРАВО НА ВЪЗРАЖЕНИЕ И АВТОМАТИЗИРАНО ВЗЕМАНЕ НА ИНДИВИДУАЛНИ РЕШЕНИЯ (...)

Член 19

Право на възразжение

1. Субектът на данните има право, по всяко време и на базата на основания, свързани с неговата конкретна ситуация, на възразжение срещу обработването на отнасящи се до него лични данни, което е основано на член 6, параграф 1, букви д) или е), член 6, параграф 4, алинея първа във връзка с член 6, параграф 1, буква д) или член 6, параграф 4, алинея втора.

Администраторът прекратява обработването на личните данни, (...) освен ако не докаже, че има 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.

- 1а. (...)
2. Когато се обработват лични данни за целите на директния маркетинг, субектът на данни има право по всяко време да направи възразжение (...) срещу обработването на отнасящи се до него лични данни за този вид маркетинг. Най-късно в момента на първо осъществяване на контакт със субекта на данните, той изрично се уведомява за съществуването на това право, (...) което му се представя по ясен начин и отделно от всяка друга информация.
- 2а. Когато субектът на данни възрази срещу обработването на данните за целите на директния маркетинг, обработването на личните данни за тези цели се прекратява.
- 2аа. Когато лични данни се обработват с историческа, статистическа или научна цел, субектът на данните има право, въз основа на конкретното си положение, да възрази срещу обработването на лични данни, които го засягат, освен ако обработването е необходимо за изпълнението на задача, осъществявана по причини от публичен интерес.
3. (...)
4. (...)

Автоматизирано вземане на индивидуални решения

1. Субектът на данните има право да не бъде обект на решение, (...)основаващо се единствено на автоматизирано обработване, включително профилиране, което поражда правни последствия за субекта на данните или го засяга в значителна степен.
- 1а. Параграф 1 не се прилага, ако решението: (...)
 - а) е необходимо за сключването или изпълнението на договор между субект на данни и администратор(...); или
 - б) е (...) разрешено от правото на Съюза или 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 (...).
- 1б. В случаите, посочени в параграф 1а, букви а) и в), администраторът на лични данни 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:
2. (...)
3. Решенията по параграф 1а 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.
4. (...)
5. (...)

РАЗДЕЛ 5 ОГРАНИЧЕНИЯ

Член 21

Ограничения

1. В правото на Съюза или на държава членка, което се прилага спрямо администратора на лични данни или обработващото лице, чрез законодателна мярка може да се ограничи обхватът на задълженията и правата, предвидени в (...) членове 12—20 и в член 32, както и в член 5, доколкото неговите разпоредби съответстват на правата и задълженията, предвидени в членове 12—20, когато подобно ограничение представлява необходима и пропорционална мярка в едно демократично общество с цел да се гарантира:
 - аа) националната сигурност;
 - аб) отбраната;
 - а) обществената сигурност;
 - б) предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции или предпазването и предотвратяването на заплахи за обществената сигурност;
 - в) 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, защитата на стабилността и целостта на пазара;
 - ва) защитата на независимостта на съдебната власт и съдебните производства;
 - г) предотвратяването, разследването, разкриването и наказателното преследване на нарушения на етичните кодекси при регламентираните професии;

- д) функция по наблюдението, проверката или регламентирането, свързана, дори само понякога, с упражняването на официални правомощия в случаите, посочени в букви аа), аб), а), б), в) и г);
- е) защитата на субекта на данните или на правата и свободите на други лица;
- ж) изпълнението на гражданскоправни иски.

2. Всяка законодателна мярка, посочена в параграф 1, съдържа специални разпоредби най-малко, където е целесъобразно, по отношение на целите на обработването или категориите обработване, категориите лични данни, обхвата на въведените ограничения, спецификацията на администратора или категориите администратори, периодите на съхранение и приложимите гаранции, като се имат предвид естеството, обхватът и целите на обработването или категориите обработване и рисковете за правата и свободите на субектите на данни.

ГЛАВА IV

АДМИНИСТРАТОР И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

РАЗДЕЛ 1

ОБЩИ ЗАДЪЛЖЕНИЯ

Член 22

Задължения на администратора

1. Като се отчитат естеството, обхватът, контекстът, и целите на обработването, както и вероятността и тежестта на риска за правата и свободите на лицата, администраторът (...) прилага подходящи мерки и е в състояние да докаже, че обработването на лични данни се извършва в съответствие с настоящия регламент.
2. (...)
- 2а. 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.
- 2б. Придържането към одобрени кодекси за поведение съгласно член 38 или одобрен механизъм за сертифициране в съответствие с член 39 може да се използва като елемент за доказване на спазването на задълженията на администратора.
3. (...)
4. (...)

Защита на данните на етапа на проектирането и по подразбиране

1. (...) Като се имат предвид наличните технологии и разходите за прилагането, както и естеството, обхватът, контекстът и целите на обработването и вероятността и тежестта на риска, породен от обработването за правата и свободите на лицата, администраторът прилага (...) технически и организационни мерки, подходящи за извършваната дейност по обработването и за нейните цели, като минимизиране и псевдонимизиране, по такъв начин че обработването да отговаря на изискванията на настоящия регламент и да защитава правата на (...) субектите на данни.
2. Администраторът прилага подходящи мерки, за да се гарантира, че по подразбиране се обработват само (...) лични данни (...), които са необходими за всяка конкретна цел на обработването; това се отнася до обема на (...) събраните данни, степента на обработването, периода на съхраняването им и тяхната достъпност. Когато обработването не се извършва с цел предоставяне на информация на обществеността, тези механизми гарантират, че по подразбиране личните данни не са достъпни без човешка намеса за неопределен брой лица.
- 2а. Одобреният механизъм за сертифициране съгласно член 39 може да се използва като елемент, за да се докаже спазването на изискванията, предвидени в параграфи 1 и 2.
3. (...)
4. (...)

Член 24

Съвместни администратори

1. Когато двама или повече администратори съвместно определят целите и средствата на обработването на лични данни, 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 14 и 14а, посредством договореност помежду си, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на Съюза или на държава членка, което се прилага спрямо администраторите. В договореността следва да се посочва кой от съвместните администратори действа като единна точка за контакт, за да упражняват правата си субектите на данни.
2. Независимо от условията на договореността, посочена в параграф 1, субектът на данни може да упражнява своите права по настоящия регламент по отношение на всеки и срещу всеки от (...) администраторите.
3. Договореността надлежно отразява съответните действителни роли на съвместните администратори спрямо субектите на данни, а съществените характеристики на договореността са достъпни за субекта на данните. Параграф 2 не се прилага, когато субектът на данни е информиран по прозрачен и недвусмислен начин за това кой от съвместните администратори носи отговорност, освен когато такава договореност, с изключение на договореност, определена от Съюза или от държава членка, е несправедлива по отношение на неговите права (...).

Член 25

Представители на администратори, които не са установени в Съюза

1. В случаите когато се прилага член 3, параграф 2, администраторът определя писмено представител в Съюза.

2. Това задължение не се прилага за:
- а) (...); или
 - б) обработване, което е спорадично и няма вероятност да породи (...) риск за правата и свободите на лицата предвид естеството, контекста, обхвата и целите на обработването (...); или
 - в) публичен орган или структура;
 - г) (...)
3. Представителят е установен в една от тези държави членки, в която пребивават постоянно субектите на данни, чиито лични данни се обработват във връзка с предлагането на стоки или услуги или чието поведение се наблюдава.
- 3а. Администраторът предоставя на представителя мандат, съгласно който по-специално надзорните органи и субектите на данни могат освен или вместо към администратора да се обръщат към представителя по всички въпроси, свързани с обработването на лични данни, с цел да се гарантира спазване на настоящия регламент.
4. Определянето на представител от администратора не засяга правните производства, които биха могли да бъдат образувани срещу самия администратор.

Член 26

Обработващ личните данни

1. (...) 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, предвидени в настоящия регламент(...).
- 1а. Обработващият данни не добавя друг обработващ данни без предварителното конкретно или общо писмено съгласие на администратора. В последния случай, обработващият данни винаги следва да информира администратора за всякакви планирани промени за добавяне или замяна на други лица, обработващи данни, като по този начин даде възможност на администратора да оспори тези промени.

16. (...)

2. Извършването на обработването от страна на обработващия лични данни се урежда с договор или с правен акт съгласно правото на Съюза или на държава членка, който обвързва обработващия лични данни с администратора, регламентира предмета и срока на действие на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни, правата на администратора (...) и в който се предвижда по-специално, че обработващият лични данни:

- а) обработва личните данни само по нареждане на администратора (...), освен когато е длъжен да направи това по силата на правото на Съюза или 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 на личните данни, освен ако това право забранява такова информироване на важни основания от публичен интерес;
- б) (...)
- в) взема всички (...) необходими мерки съгласно член 30;
- г) зачита условията за включване на друг обработващ лични данни (...), като например изискване за специално предварително разрешение от страна на администратора;
- д) (...) като отчита естеството на обработването, подпомага администратора при изготвянето на отговор по искания за упражняване на предвидените в глава III права на субектите на данни;
- е) (...) подпомага администратора да гарантира изпълнението на задълженията съгласно членове 30—34;
- ж) по избор на администратора връща или изтрива личните данни след приключване на предоставянето на услуги по обработване на данни, предвидено в договора или в друг правен акт, освен ако в правото на Съюза или на държавата членка, което се прилага спрямо обработващия лични данни, съществува изискване за съхраняване на данните;
- з) предоставя на администратора (...) цялата информация, необходима за доказване на изпълнението на задълженията, определени в настоящия член, и позволява и допринася за извършването на одити от страна на администратора.

Обработващият лични данни незабавно уведомява администратора, ако според него дадено нареждане нарушава настоящия регламент или разпоредбите относно защитата на данни на Съюза или на държавите членки.

- 2а. 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 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 2, 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 другото лице, обработващо 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 това друго лице, обработващо данните.
- 2аа. Придържането на обработващия лични данни към одобрен кодекс за поведение съгласно член 38 или одобрен механизъм за сертифициране в съответствие с член 39 може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграфи 1 и 2а.
- 2аб. Без да се засягат разпоредбите на индивидуалния договор между администратора и обработващия лични данни, договорът или другият правен акт, посочени в параграфи 2 и 2а, може да се основават изцяло или отчасти на стандартни договорни клаузи, посочени в параграфи 2б и 2в, или на стандартни договорни клаузи, които са част от сертифициране, предоставено на администратора или обработващия лични данни съгласно членове 39 и 39а.
- 2б. Комисията може да установява стандартни договорни клаузи по въпроси, посочени в параграфи 2 и 2а, и в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2.
- 2в. Надзорният орган може да приема стандартни договорни клаузи по въпросите, посочени в параграфи 2 и 2а, и в съответствие с механизма за съгласуваност, посочен в член 57.

3. Договорът или другият правен акт, посочен в параграфи 2 и 2а се изготвя в писмена форма, включително в електронна форма.
4. (...)
5. (...)

Член 27

Обработване под ръководството на администратора и обработващия лични данни

(...)

Член 28

Регистри на категории дейности по обработване на лични данни

1. Всеки администратор (...) и представител на администратор, ако има такъв, поддържа регистър на всички категории дейности по обработване на лични данни, за които отговоря. Този регистър съдържа (...) следната информация:
 - а) името и координатите за връзка на администратора и на всички съвместни администратори (...), на представителя на администратора и на длъжностното лице по защитата на данните, ако има такива;
 - б) (...)
 - в) целта на обработването, включително законният интерес, когато обработването се основава на член 6, параграф 1, буква е);
 - г) описание на категориите субекти на данни и на свързаните с тях категории лични данни;
 - д) (...) категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави;

- е) когато е приложимо, категориите предаване на лични данни на трета държава или международна организация (...);
 - ж) когато е възможно, предвидените срокове за заличаване на различните категории данни.
 - з) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 30, параграф 1.
- 2а. Всеки обработващ лични данни поддържа регистър с всички категории дейности за обработване на лични данни, 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, както и на представителя на администратора, ако има такъв;
 - б) името и координатите за връзка на длъжностното лице по защита на данните, ако има такава;
 - в) категориите обработване, извършвано от името на всеки администратор;
 - г) когато е приложимо, категориите предаване на лични данни на трета държава или международна организация;
 - д) когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 30, параграф 1.
- 3а. Регистрите, посочени в параграфи 1 и 2а, са в писмена форма, включително в електронна или друга нечетима форма, която е възможно да бъде превърнати в четима форма.
3. При поискване, администраторът, обработващият лични данни и представителят на администратора, ако има такъв, предоставят регистъра (...) на надзорния орган.
4. Задълженията, посочени в параграфи 1 и 2а, не се прилагат по отношение на:
- а) (...);

- б) предприятие или орган с по-малко от 250 служители, освен ако извършването от него обработване има вероятност да породи висок риск за правата и свободите на субекта на данни, като (...) дискриминация, кражба на самоличност или измама с фалшива самоличност, неразрешено премахване на псевдонимизация, финансови загуби, накърняване на репутацията, нарушаване на поверителността на данни, защитени с професионална тайна, или всякакви други икономически или социални неблагоприятни последици за субектите на данни, като се отчитат естеството, обхватът, контекстът и целите на обработването;
5. (...)
6. (...)

Член 29

Сътрудничество с надзорния орган

(...)

РАЗДЕЛ 2

СИГУРНОСТ НА ДАННИТЕ

Член 30

Сигурност на обработването

1. Като се имат предвид наличните технологии и разходите за прилагане и като се отчитат естеството, обхватът, контекстът и целите на обработването, както и вероятността и тежестта на риска за правата и свободите на лицата, администраторът и обработващият лични данни прилагат подходящи технически и организационни мерки, като (...) псевдонимизиране на лични данни, за осигуряване на съобразено с този риск ниво на сигурност.
 - 1а. При оценката на подходящото ниво на сигурност се вземат предвид по-специално рисковете, които са свързани с обработването на данни, (...) по-специално от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.
2. (...)
 - 2а. Придържането към одобрени кодекси за поведение съгласно член 38 или одобрен механизъм за сертифициране в съответствие с член 39 може да се използва като доказателство за предоставянето на достатъчно гаранции съгласно параграф 1.
 - 2б. Администраторът и обработващият лични данни вземат мерки всяко 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 на държава членка.
3. (...)
4. (...)

Уведомяване на надзорния орган за нарушение на сигурността на личните данни

1. В случай на нарушение на сигурността на личните данни, което има вероятност да породи висок риск за правата и свободите на лицата, включващ например дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизация, накърняване на репутацията, нарушаване на поверителността на данни, защитени от професионална тайна, или други значителни икономически или социални неблагоприятни последствия, администраторът, без излишно 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, който е компетентен в съответствие с член 51. Уведомлението до надзорния орган се придружава от мотивирана обосновка в случаите, когато не е подадено в срок от 72 часа.
- 1а. Не се изисква посоченото в параграф 1 уведомление, ако не се изисква посочване на субекта на данни по силата на член 32, параграф 3, букви а) и б).
2. (...) Обработващият лични данни уведомява администратора незабавно след като узнае за нарушаване на сигурността на лични данни .
3. В уведомлението, посочено в параграф 1, трябва да се съдържа най-малко следното:
 - а) описание на естеството на нарушението на сигурността на личните данни, включително — ако е възможно и ако се налага — приблизителните категории и брой на засегнатите субекти на данни и категориите и приблизителното количество на засегнатите записи на данни;
 - б) посочване на самоличността и координатите за връзка на длъжностното лице по защита на данните или на друго звено за контакт, от което може да се получи повече информация;
 - в) (...)
 - г) описание на вероятните последствия от нарушението на сигурността на личните данни, установени от администратора;

- д) описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни; и
 - е) ако е необходимо, посочване на мерките за намаляване на евентуалните неблагоприятни последици от нарушението на сигурността на личните данни.
- 3а. Когато и доколкото не е възможно информацията по параграф 3, букви г), д) и е) да се подаде едновременно с информацията по параграф 3, букви а) и б), администраторът предоставя тази информация без излишно забавяне.
4. Администраторът документира нарушенията на сигурността на личните данни, посочени в параграфи 1 и 2, като включва фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него. Тази документация трябва да дава възможност на надзорния орган да провери дали е спазен настоящият член. (...)
5. (...)
6. (...)

Член 32

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 лицата, включващ например дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, неразрешено премахване на псевдонимизация, нарушаване на поверителността на данни, защитени от професионална тайна, или други значителни икономически или социални неблагоприятни последици, администраторът (...), без излишно забавяне, съобщава на субекта на данните за нарушението на сигурността на личните данни.
2. В съобщението до субекта на данните, посочено в параграф 1, се описва естеството на нарушението на сигурността на личните данни и се съдържат най-малко информацията и препоръките, предвидени в член 31, параграф 3, букви б), д) и е).

3. Посоченото в параграф 1 съобщение (...) до субекта на данните не се изисква, ако:
- а. администраторът (...) е предприел подходящи технологични и организационни мерки за защита и тези мерки са били приложени по отношение на данните, засегнати от нарушението на сигурността на личните данни, по-специално мерките, които правят данните неразбираеми за всяко лице, което няма разрешение за достъп до тях, като например криптиране; или
 - 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; или
 - в. то би довело до непропорционални усилия, по-специално поради големия брой такива случаи. 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; или
 - г. то би имало неблагоприятни последствия за значителен обществен интерес.
4. (...)
5. (...)
6. (...)

РАЗДЕЛ 3

ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО ВЪРХУ ЗАЩИТАТА НА ДАННИТЕ И ПРЕДВАРИТЕЛНИ КОНСУЛТАЦИИ

Член 33

Оценка на въздействието върху защитата на данните

1. Когато съществува вероятност определен вид обработка, по-специално при използването на нови технологии, и предвид естеството, обхвата, контекста и целите на обработката, да породи висок риск за правата и свободите на лицата, включващ например дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, неразрешено премахване на псевдонимизация, нарушаване на поверителността на данни, защитени от професионална тайна, или други значителни икономически или социални неблагоприятни последствия, преди да бъде извършено обработването, администраторът (...) извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. (...)
- 1a. При извършването на оценка на въздействието върху защитата на данните администраторът иска становището на длъжностното лице по защита на данните, когато такова е определено.
2. Оценката на въздействието върху защитата на данните, посочена в параграф 1, се изисква по-специално в следните случаи:
 - а) систематична и подробна оценка (...) на личните аспекти по отношение на (...) физически лица (...), като тази оценка се базира на профилиране и служи за основа на решения, които имат правни последствия за субектите на данни или сериозно засягат субектите на данни;
 - б) обработване на специални категории лични данни по силата на член 9, параграф 1 (...), биометрични данни или данни за наказателни присъди или свързани с тях мерки за сигурност, когато данните са обработвани в големи мащаби с цел вземане на (...) решения по отношение на конкретни лица;

- в) *широкомащабно* наблюдение на публично достъпни зони, особено когато се използват оптично-електронни устройства (...);
- г) (...);
- д) (...)

- 2а. 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 Европейския комитет по защита на данните.
- 2б. 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 Европейския комитет по защита на данните.
- 2в. Преди приемането на списъците, посочени в параграфи 2а и 2б, компетентният надзорен орган прилага посочения в член 57 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 може съществено да засегне свободното движение на лични данни в рамките на Съюза.
- 3. Оценката съдържа поне общо описание на предвидените операции по обработване, оценка на посочения в параграф 1 риск, мерките, предвидени за справяне с риска, вкл. 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.

- 3а. При оценката на законосъобразността и въздействието на операциите по обработване, извършвани от администраторите и обработващите лични данни, и особено за целите на оценката на въздействието върху защитата на данните, надлежно се отчита и спазването от тяхна страна на одобрените кодекси за поведение, посочени в член 38.
4. *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 (...).*
5. (...) Когато обработването съгласно член 6, параграф 1, буква в) или д) има правно основание в правото на Съюза или на държавата членка, под чиято юрисдикция е администраторът, и това право регулира конкретната операция по обработване или набор от такива операции, параграфи 1—3 не се прилагат, освен ако държавите членки не сметнат за необходимо да направят такава оценка преди започването на дейностите по обработването.
6. (...)
7. (...)

Член 34

Предварителна (...) консултация

1. (...)
2. Администраторът (...) се консултира с надзорния орган преди обработването на лични данни, когато оценката на въздействието върху защитата на данните съгласно член 33 покаже, че обработването ще породви висок (...) риск, ако администраторът не предприеме мерки за ограничаване на риска.

3. Когато надзорният орган е на мнение, че планираното обработване, посочено в параграф 2, няма да съответства на настоящия регламент, особено когато администраторът не е идентифицирал или ограничил *риска* в достатъчна степен, в рамките максимум на 6 седмици след искането за консултация този орган дава становище на администратора на данните писмено, като може да използва всяко от правомощията си, посочени в член 53 (...). Този срок може да бъде удължен с още шест седмици предвид сложността на планираното обработване. Когато се прилага удълженият срок, администраторът или обработващият лични данни се уведомяват в срок от един месец от получаване на искането за причините за забавянето.
4. (...)
5. (...)
6. Когато се консултира с надзорния орган съгласно параграф 2, 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 данните 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 съгласно член 33; както и
 - е) всякаква (...) друга информация, поискана от надзорния орган (...).

7. Държавите членки се консултират с надзорния орган по време на изготвянето на предложения за законодателни мерки, приемани от националните парламенти, или на регулаторни мерки, основани на такива законодателни мерки, които предвиждат обработване на лични данни (...).
- 7a. Без да се засяга параграф 2, 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 на лични данни от администратор за изпълнението на задача, осъществявана от администратора в полза на обществен интерес, включително обработването на такива данни във връзка със социалната защита и общественото здраве.
8. (...)
9. (...)

РАЗДЕЛ 4

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Член 35

Определяне на длъжностното лице по защита на данните

1. Администраторът или обработващият лични данни може да определи, а ако това се изисква от правото на Съюза или на държава членка — определя длъжностно лице по защита на данните (...).
2. Група предприятия може да назначи едно 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. (...)
5. (...) Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания на правото и практиките в областта на защитата на данните и способността му да изпълнява задачите, посочени в член 37, по-специално отсъствието на какъвто и да било конфликт на интереси. (...)
6. (...)
7. (...) По време на своя мандат длъжностното лице по защита на данните може да бъде освободено от длъжност, с изключение на случаите на сериозни основания според правото на съответната държава членка, позволяващи да бъде уволнен служител или държавен служител, само ако престане да отговаря на условията, необходими за изпълнение на задачите съгласно член 37.
8. 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.
9. Администраторът или обработващият лични данни публикува координатите за връзка на длъжностното лице по защита на данните и ги съобщава на надзорния орган (...).

10. Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните данни и упражняването на техните права съгласно настоящия регламент.
11. (...)

Член 36

Позиция на длъжностното лице по защита на данните

1. Администраторът или обработващият лични данни гарантира, че длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни.
2. Администраторът или обработващият лични данни подпомага длъжностното лице по защита на данните при изпълнението на посочените в член 37 задачи, като осигурява (...) ресурсите, необходими за изпълнение на тези задачи, както и достъп до личните данни и операциите по обработването.
3. Администраторът или обработващият лични данни правят необходимото длъжностното лице по защита на данните да може да действа независимо при изпълнение на задачите си и да не получава никакви указания във връзка с тези задачи. Той не подлежи на санкции 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. 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 37

Задачи на длъжностното лице по защита на данните

1. (...) Длъжностното лице по защита на данните (...) има следните задачи:
- а) да информира и съветва администратора или обработващия лични данни и служителите, които обработват лични данни, за техните задължения по силата на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държави членки (...);

- б) да наблюдава спазването на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държави членки и на стратегиите 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) (...)
- г) (...)
- д) (...)
- е) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно член 33;
- ж) да наблюдава отговорите на искания от надзорния орган и в рамките на компетентността на длъжностното лице по защита на данните да си сътрудничи с надзорния орган по негово искане или по своя собствена инициатива;
- з) да действа като звено за контакт за надзорния орган по въпроси, свързани с обработването на лични данни, включително преди консултацията, посочена в член 34, и ако е необходимо да се консултира по всякакви други въпроси.

2. (...)

2а. 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 38

Кодекси за поведение

1. Държавите членки, надзорните органи, Европейският комитет по защита на данните 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.
- 1а. 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 разпоредбите на настоящия регламент, а именно:
 - а) добросъвестното и прозрачно обработване на данни;
 - аа) законните интереси, преследвани от администраторите в конкретни аспекти;
 - б) събирането на данни;
 - бб) псевдонимизацията на лични данни;
 - в) информирането на обществеността и на субектите на данни;
 - г) упражняването на правата на субектите на данни;
 - д) информацията и закрилата на децата и начинът за получаване на съгласие от родителите и настойниците;
 - дд) мерките и процедурите, посочени в членове 22 и 23, и мерките за осигуряване на посочената в член 30 сигурност на обработването;

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

е) (...)

1аб. Освен регламента администраторът или обработващият лични данни може да спазва и кодекси за поведение, одобрени съгласно параграф 2, които не са предмет на настоящия регламент, в съответствие с член 3, за да се осигурят подходящи гаранции в рамките на предаването на лични данни на трети държави или международни организации съгласно условията, посочени в член 42, параграф 2, буква г). Тези администратори или обработващи лица поемат правно обвързващи и задължителни ангажменти, чрез договорни инструменти или по друг начин, да прилагат тези подходящи гаранции, включително по отношение на правата на субектите на данни.

1б. Такъв кодекс за поведение съдържа механизми, които позволяват на посочения в член 38а, 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 надзорния орган, който е компетентен по силата на член 51 или 51а.

2. Сдруженията и другите структури, посочени в параграф 1а, които възнамеряват да изготвят кодекс за поведение или да изменят или допълнят съществуващ кодекс, представят проекта за кодекс на надзорния орган, който е компетентен съгласно член 51. Надзорният орган дава становище дали проектът за кодекс или измененият или допълненият кодекс отговаря на изискванията на настоящия регламент и одобрява този проект за кодекс, изменен или допълнен кодекс, ако установи, че той осигурява достатъчно подходящи гаранции.

2а. Ако посоченото в параграф 2 становище потвърди, че проектът за кодекс или измененият или допълненият кодекс отговаря на изискванията на настоящия регламент и кодексът е одобрен, и ако кодексът за поведение няма отношение към дейности по обработване на данни в няколко държави членки, надзорният орган регистрира кодекса и публикува свързаната с това информация.

- 2б. Ако проектът на кодекс за поведение има отношение към дейности по обработване на данни в няколко държави членки, надзорният орган, компетентен съгласно член 51, го представя, преди да бъде одобрен, по посочената в член 57 процедура на Европейския комитет по защита на данните, който дава становище дали проектът на кодекса или измененият или допълненият кодекс отговаря на изискванията на настоящия регламент, или в случаите, посочени в параграф 1аб, осигурява подходящи гаранции.
3. Ако посоченото в параграф 2б становище потвърди, че кодексът за поведение или измененият или допълненият кодекс отговаря на изискванията на настоящия регламент или в случаите, посочени в параграф 1аб, осигурява подходящи гаранции, Европейският комитет по защита на данните представя становището си на Комисията .
4. Комисията може да приема актове за изпълнение, за да реши дали одобрените кодекси за поведение и измененията или допълненията към съществуващи одобрени кодекси за поведение, които са ѝ представени по силата на параграф 3, са общовалидни в рамките на Съюза. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2.
5. Комисията осигурява подходяща публичност на одобрените кодекси, за които е решено, че са общовалидни в съответствие с параграф 4.
- 5а. Европейският комитет по защита на данните събира всички одобрени кодекси за поведение и измененията към тях в регистър и ги прави обществено достъпни чрез всички подходящи средства, като например европейския портал за електронно правосъдие.

Член 38а

Наблюдение на одобрените кодекси за поведение

1. Без да се засягат задачите и правомощията на компетентния надзорен орган по членове 52 и 53, наблюдението на спазването на даден кодекс за поведение съгласно член 38, параграф 1б може да се осъществява от орган, който има съответното ниво на опит във връзка с предмета на кодекса и бива акредитиран за тази цел от компетентния надзорен орган.

2. Посоченият в параграф 1 орган може да бъде акредитиран за тази цел, 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;
 - 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 на Европейския комитет по защита на данните в съответствие с посочения в член 57 механизъм за съгласуваност.
4. Без да се засягат разпоредбите на глава VIII, орган по параграф 1 може, при наличие на адекватни предпазни мерки, да предприема съответните действия в случай на нарушение на кодекса от страна на администратор или обработващ лични данни, включително да суспендира членството в кодекса или да изключи 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 не са били спазени или вече не се спазват условията за акредитация, или ако предприетите от органа действия не са в съответствие с настоящия регламент.
6. Настоящият член не се прилага по отношение на обработването на лични данни, извършвано от публичните власти и органи.

Сертифициране

1. Държавите членки, Европейският комитет 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 извършваните операции по обработване от страна на администраторите и обработващите лични данни. Отчитат се конкретните нужди на микропредприятията, на малките и средните предприятия.
- 1а. Освен спазването на настоящия регламент от администратора или обработващия лични данни, може да се установяват и сертификационни механизми, печати или маркировки за защита на данните, одобрени съгласно параграф 2а, с цел да се демонстрира наличието на подходящи гаранции, осигурени от администраторите и обработващите лични данни, които не са обект на настоящия регламент по силата на член 3, в рамките на предаването на лични данни на трети държави или международни организации съгласно условията, посочени в член 42, параграф 2, буква д). Тези администратори или обработващи лични данни поемат правно обвързващи и задължителни ангажименти, чрез договорни инструменти или по друг начин, да прилагат тези подходящи гаранции, включително по отношение на правата на субектите на данни.
2. Сертифицирането по настоящия член не води до намаляване на отговорността на администратора или на обработващия лични данни за спазването на настоящия регламент и не засяга задачите и правомощията на надзорния орган, който е компетентен съгласно член 51 или член 51а.
- 2а. Сертификат по силата на настоящия член се издава от сертифициращите органи, посочени в член 39а, или ако е приложимо — от компетентния надзорен орган, въз основа на критериите, одобрени от компетентния надзорен орган, или, съгласно член 57, от Европейския комитет по защита на данните.
3. Администраторът или обработващият лични данни, който подлага своето обработване на механизма за сертифициране, осигурява на сертифициращия орган, посочен в член 39а, 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 сертифицирането.

4. Сертификатът се издава на администратора или обработващия лични данни, за максимален срок от 3 години и може да бъде подновен при същите условия, ако съответните изисквания продължават да са спазени. Той се оттегля от сертифициращите органи, посочени в член 39а, или ако е приложимо — от компетентния надзорен орган, ако изискванията за сертифицирането не са били спазени или вече не се спазват.
5. Европейският комитет по защита на данните обединява всички механизми за сертифициране и всички печати за защита на данните в регистър и ги прави обществено достъпни чрез всички подходящи средства, като например европейския портал за електронно правосъдие.

Член 39а

Сертифициращ орган и процедура по сертифициране

1. Без да се засягат задълженията и правомощията на компетентния надзорен орган по членове 52 и 53, сертификатът се издава и се подновява от сертифициращ орган, притежаващ подходящо ниво на опит в областта на защитата на данните. Всяка държава членка дава информация дали тези сертифициращи органи са акредитирани от:
- a) надзорния орган, компетентен съгласно член 51 или 51а; и/или
 - b) националния орган по акредитация, посочен в съответствие с 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 в съответствие с EN-ISO/IEC 17065/2012 и с допълнителните изисквания, определени от надзорния орган, който е компетентен съгласно член 51 или 51а.
2. Посоченият в параграф 1 сертифициращ орган може да бъде акредитиран за тази цел само ако:
- a) е доказал в задоволителна степен пред компетентния надзорен орган своята независимост и опит във връзка с предмета на сертифицирането;

- aa) е поел ангажимент да спазва критериите, посочени в член 39, параграф 2а, и одобрени от надзорния орган, който е компетентен съгласно член 51 или 51а или, съгласно член 57, от Европейския комитет по защита на данните;
- б) е установил процедури за издаването, периодичния преглед и отнемането на печати и маркери във връзка със защитата на данни;
- в) е установил процедури и структури за обработване на жалби за нарушения на сертификата или за начина, по който сертификатът 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;
- г) демонстрира в задоволителна степен пред компетентния надзорен орган, че задачите и задълженията му не водят до конфликт на интереси.
3. Акредитирането на сертифициращите органи по параграф 1 се извършва на базата на критериите, одобрени от надзорния орган, който е компетентен съгласно член 51 или 51а или, съгласно член 57, от Европейския комитет по защита на данните. В случай на акредитация в съответствие с параграф 1, буква б), тези изисквания допълват изискванията, предвидени в Регламент (ЕО) № 765/2008 и техническите правила, които описват методите и процедурите на сертифициращите органи.
4. Сертифициращият орган по параграф 1 отговаря за правилната оценка, която води до сертифициране или отнемане на издаден сертификат, без да се засяга отговорността на администратора или обработващия данни за спазването на настоящия регламент. Акредитацията се издава за максимален срок от пет години и може да бъде подновена при същите условия, ако органът отговаря на изискванията.
5. Сертифициращият орган по параграф 1 представя на компетентния надзорен орган мотивите за издаване или отнемане на съответния сертификат.

6. Изискванията, посочени в параграф 3, и критериите, посочени в параграф 2а от член 39, се оповестяват от надзорния орган в леснодостъпна форма. Надзорните органи предават тази информация и на Европейския комитет по защита на данните. Европейският комитет по защита на данните обединява всички механизми за сертифициране и всички печати за защита на данните в регистър и ги прави обществено достъпни чрез всички подходящи средства, като например европейския портал за електронно правосъдие.
- 6а. Без да се засягат разпоредбите на глава VIII, компетентният надзорен орган или националният орган по акредитация анулира акредитацията, дадена от него на сертифициращ орган по параграф 1, ако не са били спазени или вече не се спазват условията за акредитация, или ако предприетите от органа действия не са в съответствие с настоящия регламент.
7. Комисията се оправомощава да приема делегирани актове в съответствие с член 86 с цел (...) допълнително уточняване на критериите и изискванията, които да бъдат взети предвид по отношение на механизмите за сертифициране за защита на данните, посочени в параграф 1 (...).
- 7а. Европейският комитет по защита на данните представя становище на Комисията относно критериите и изискванията, посочени в параграф 7.
8. Комисията може 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 механизмите за сертифициране и на печатите и маркировките за защита на данните. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2.

ГЛАВА V

ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Член 40

Общ принцип на предаването на данни

(...)

Член 41

Предаване на данни въз основа на решение относно адекватността

1. Предаване на лични данни на (...) трета държава или международна организация може да има, ако Комисията реши, че въпросната трета държава или 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 по сектори, правилата и мерките за сигурност във връзка със защитата на данни, включително правилата за последващо предаване на лични данни на друга трета държава или международна организация, които са в сила във въпросната държава или международна организация, както и наличието на ефективни и приложими права на субектите на данни и ефективни административни и съдебни средства за защита за субектите на данни, чиито лични данни се прехвърлят (...);

- б) наличието и ефективното функциониране на един или повече независими надзорни органи във въпросната трета държава илина които се подчинява дадена международна организация, отговорни за осигуряване и прилагане на правилата за защита на данните, включително адекватни правомощия за налагане на санкции, за подпомагане и консултиране на субектите на данни при упражняването на техните права и за осъществяване на сътрудничество с надзорните органи на Съюза и на държавите членки;
- в) международните ангажменти, които съответната трета държава или международна организация е поела или други (...) задължения, произтичащи от нейното участие в многостранни или регионални системи, по-конкретно по отношение на защитата на личните данни.

2а. Европейският комитет по защита на данните 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 дадена трета държава или територия, или международна организация, или конкретен сектор са престанали да осигуряват адекватно ниво на защита.

3. След оценка на адекватността на нивото на защита Комисията може да реши, че дадена трета държава или територия, или един или повечеконкретни сектори в тази трета държава, или дадена международна организация осигуряват адекватно ниво на защита по смисъла на параграф 2. (...) В акта за изпълнение се уточнява неговото териториално и секторно приложение и когато е приложимо, се посочва (независимият) надзорен(надзорни) орган(и), споменати в параграф 2, буква б). Актовете за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2.

3а. *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 от решение на Комисията, прието в съответствие с параграф 3 или 5.*

4. (...)
- 4а. Комисията наблюдава изпълнението на решенията, приети съгласно параграф 3, и решенията, приети въз основа на член 25, параграф 6 и член 26, параграф 4 от Директива 95/46/ЕО.
5. Комисията може да реши, че дадена трета държава или територия, или конкретен сектор в тази трета държава, или дадена международна организация е престанала да осигурява адекватно ниво на защита по смисъла на параграф 2 и може, ако е необходимо, да отмени, измени или суспендира такова решение, което не поражда ефект със задна дата. Актовете за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2, или в особено спешни (...) случаи — съгласно процедурата, посочена в член 87, параграф 3. (...)
- 5а. Комисията започва консултации с третата държава или международната организация с цел да коригира положението, довело до решението, взето по силата на параграф 5.
6. Решението по параграф 5 не засяга предаването на лични данни на третата държава или територия, или конкретен сектор в тази трета държава, или на въпросната международна организация съгласно членове 42—44.(...)
7. Комисията публикува в *Официален вестник на Европейския съюз* списък на тези трети държави, територии и конкретни сектори в трети държави и международни организации, по отношение на които са взети решения съгласно параграфи 3, 3а и 5.
8. (...)

Предаване на данни с подходящи гаранции

1. При липса на решение съгласно член 41, параграф 3 даден администратор или обработващ лични данни може да предава лични данни на (...) трета държава или международна организация само ако администраторът или обработващият лични данни е предвидил подходящи гаранции, които обхващат и последващо предаване на данни (...).
2. Подходящите гаранции, посочени в параграф 1, могат да бъдат предвидени (...) без да се изисква специално разрешение от надзорния орган, посредством:
 - оа) правно обвързващ инструмент с изпълнителна сила между публичните органи или структури; или
 - а) задължителните фирмени правила, посочени в член 43; или
 - б) стандартни клаузи за защита на данните, приети от Комисията (...) в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2; или
 - в) стандартни клаузи за защита на данните, приети от надзорен орган (...) и приети от Комисията съгласно процедурата по разглеждане, посочена в член 87, параграф 2;
 - г) одобрен кодекс за поведение съгласно член 38, заедно със задължителни и изпълними ангажменти на администратора или обработващия лични данни (...) в трета държава да прилагат подходящите гаранции, включително и по отношение на правата на субектите на данни; или
 - д) одобрен механизъм за сертифициране съгласно член 39, заедно със задължителни и изпълними ангажменти на администратора или обработващия лични данни (...) в трета държава да прилагат подходящите гаранции, включително и по отношение на правата на субектите на данни.

- 2а. 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 данните (...) в третата държава или международната организация; или
 - б) (...)
 - в) (...)
 - г) разпоредби, които да се включват в административните договорености между публичните органи или структури(...).
3. (...)
4. (...)
5. (...)
- 5а. Надзорният орган прилага механизма за съгласуваност в случаите, посочени в член 57, параграф 2, букви ва), г), д) и е).
- 5б. *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 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 от решение на Комисията, прието в съответствие с параграф 2.*

Член 43

Задължителни фирмени правила

1. Компетентният надзорен орган одобрява задължителни фирмени правила в съответствие с механизма за съгласуваност, определен в член 57, ако те:
- а) са правно обвързващи, прилагат се спрямо и се привеждат в изпълнение от всеки съответен член на група предприятия или на група предприятия, развиващи съвместна стопанска дейност;

- б) изрично предоставят на субектите на данни приложими права по отношение на обработването на техните лични данни;
- 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 съответната група и на всеки неин член;
- б) предаването на данни или категориите предавания на данни, включително видовете 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, (...) качеството на данните, правното основание за обработването, обработването на специални категории лични данни, мерките за осигуряване сигурността на данните, както и изискванията по отношение на последващото предаване на данни на образувания, (...) които на се обвързани от задължителни фирмени правила;
- д) правата на субектите на данни по отношение на обработването на личните им данни и средствата за упражняване на тези права, включително правото на субекта на данни да не подлежи (...) на решения, основани единствено на автоматизирано обработване, включително профилиране, в съответствие с член 20, правото за подаване на жалба до компетентния надзорен орган и до компетентните съдилища на държавите членки в съответствие с член 75, 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 може да бъде изцяло или частично освободен от такава отговорност само ако се 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 информацията относно разпоредбите, посочени в букви г), д) и е) от настоящия параграф, се предоставя на субектите на данни в съответствие с членове 14 и 14а;

- з) задачите на всяко длъжностно лице по защита на данните, определено в съответствие с член 35, или всяко друго лице или образувание, натоварено да наблюдава (...) спазването на задължителните фирмени правила в рамките на групата, както и с наблюдението на обучението и разглеждането на жалбите;
- 33) процедурите по жалбите;
- и) механизмите в рамките на групата 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 образуванието, посочено в буква з), и на управителния съвет на контролиращото предприятие или на групата предприятия следва при поискване да се предоставят на компетентния надзорен орган;
- й) механизмите за докладване и записване на промени в правилата и докладването на надзорния орган за тези промени;
- к) механизмът за сътрудничество с надзорния орган с цел осигуряване на спазването на правилата от всеки член на групата (...), по-специално чрез предоставяне на надзорния орган на резултатите от (...) проверките на мерките, посочени в буква и) от настоящия параграф;
- л) механизмите за докладване на компетентния надзорен орган за всякакви правни изисквания, приложими към член на групата в трета държава, които е вероятно да доведат до съществени неблагоприятни последици за гаранциите, предоставяни от задължителните фирмени правила; както и
- м) подходящото обучение за защита на данните за персонала, който постоянно или редовно има достъп до лични данни(...).

2а. Европейският комитет по защита на данните дава насоки на Комисията относно формата и процедурите за обмена на информация между администраторите, обработващите лични данни и надзорните органи за задължителните фирмени правила.

3. (...)

4. Комисията може да определя формата 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 87, параграф 2.

Член 44

Дерогации в особени случаи

1. При липса на решение относно адекватността съгласно член 41, параграф 3 или на подходящи гаранции съгласно член 42, включително задължителни фирмени правила (...), предаване или категория предавания на лични данни на (...) трета държава или международна организация може да се извърши само при условие че:
- а) субектът на данните изрично е дал съгласието си за предлаганото предаване на данни, след като е бил информиран, че подобно предаване може да съдържа рискове за субекта на данните поради липсата на решение относно адекватността или на подходящи гаранции; или
 - 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; или
 - 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; или
 - г) предаването е необходимо поради важни причини от обществен интерес; или
 - д) предаването е необходимо за установяването, упражняването или защитата на правни претенции; или
 - е) предаването е необходимо, за да бъде защитен жизненоважен интерес на субекта на данните или на други лица, когато субектът на данните е физически или юридически неспособен да даде своето съгласие; или
 - ж) предаването се извършва от регистрационна система, която съгласно правото на Съюза или 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 на държавите членки, са изпълнени в конкретния случай; или

- 3) предаването, което не е широкомащабно, нито е често извършвано, е необходимо за целите на законните интереси, преследвани от администратора, над които не стоят интересите или правата и свободите на субекта на данните, като администраторът (...) е оценил всички обстоятелства, свързани с операцията или съвкупността от операции по предаването на данни и (...) въз основа на тази оценка е предоставил подходящи гаранции във връзка със защитата на личните данни.
2. Предаването съгласно параграф 1, буква ж) не трябва да включва всички лични данни или всички категории лични данни, съдържащи се в регистрационната система. Когато регистрационната система е предназначена за справка от лица, които имат законен интерес, предаването се извършва единствено по искане на тези лица или ако те са получателите.
3. (...)
4. Параграф 1, букви а), б), в) и з) не се прилагат за дейности, извършвани от публичните органи при упражняването на техните публични правомощия.
5. Общественият интерес, посочен в параграф 1, буква г), трябва да бъде признат в правото на Съюза или в националното право на държавата членка, прилагано към администратора. (...)
- 5а. При липсата на решение относно адекватността, правото на Съюза или 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 съобщават тези разпоредби на Комисията.
6. Администраторът или обработващият лични данни документира оценката, както и подходящите гаранции, (...) по параграф 1, буква з), в регистрите, посочени в член 28 (...).
- 6а. (...)
7. (...)

Член 45

Международно сътрудничество за защита на личните данни

1. По отношение на трети държави и международни организации Комисията и надзорните органи предприемат подходящи мерки за:
 - а) разработване на механизми за международно сътрудничество с цел подпомагане *ефективното* прилагане на законодателството за защита на личните данни;
 - б) осигуряване на международна взаимопомощ при прилагането на законодателството за защита на личните данни, включително чрез (...), 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.
2. (...)

ГЛАВА VI

НЕЗАВИСИМИ НАДЗОРНИ ОРГАНИ

РАЗДЕЛ 1

НЕЗАВИСИМ СТАТУТ

Член 46

Надзорен орган

1. Всяка държава членка предвижда един или повече независими публични органи да отговарят за наблюдението на прилагането на настоящия регламент.
- 1а. 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.
2. Когато в дадена държава членка е създаден повече от един надзорен орган, тази държава членка определя надзорния орган, който представя тези органи в Европейския комитет по защита на данните, и определя механизма за осигуряване на спазването от другите органи на правилата, отнасящи се до механизма за съгласуваност, посочен в член 57.
3. Всяка държава членка уведомява Комисията за тези разпоредби в своето законодателство, които приема по силата на настоящата глава, най-късно до датата, посочена в член 91, параграф 2, и я уведомява незабавно за всяко последващо изменение, което ги засяга.

Член 47

Независимост

1. Всеки надзорен орган действа напълно независимо при изпълнението на задълженията и упражняването на правомощията, които са му предоставени съгласно настоящия регламент.

2. При изпълнението на своите задължения и упражняването на своите правомощия 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. (...)
4. (...)
5. 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 задължения и упражняването на неговите правомощия, включително на тези, които ще бъдат изпълнявани в контекста на взаимопомощта, сътрудничеството и активното участие в Европейския комитет по защита на данните.
6. Всяка държава членка гарантира, че всеки надзорен орган има свой собствен персонал, който (...) е подчинен на члена или членовете на надзорния орган.
7. Държавите членки гарантират, че по отношение на всеки надзорен орган се извършва финансов контрол, който не засяга неговата независимост. Държавите членки гарантират, че всеки надзорен орган има отделен, публичен годишен бюджет, който може да бъде от общия държавен или национален бюджет.

Член 48

Общи условия за членовете на надзорния орган

1. Държавите членки предвиждат членът или членовете на всеки надзорен орган да бъдат назначавани (...) от парламента и/или от правителството или държавния глава на съответната държава членка или от независим орган, който според правото на държавата членка е натоварен да извършва назначенията чрез прозрачна процедура.

2. Членът или членовете трябва да имат квалификациите, опита и уменията, необходими, за да изпълняват своите задължения и да упражняват 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. (...)
5. (...)

Член 49

Правила за създаването на надзорния орган

1. Всяка държава членка урежда със закон:
 - а) създаването (...) на всеки надзорен орган;
 - б) квалификациите (...), необходими за изпълнение на задълженията на членовете на надзорния орган;
 - в) правилата и процедурите за назначаването на члена или членовете на всеки надзорен орган (...);
 - г) продължителността на мандата на члена или членовете на всеки надзорен орган, която не е (...) по-малко от четири години, с изключение на първите назначения след влизането в сила на настоящия регламент, 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 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 и функции, които са несъвместими с тези задължения по време на мандата и след неговото приключване, и правилата, от които се ръководи прекратяването на трудовите правоотношения;
 - ж) (...)

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 на държава членка, са обвързани от задължението за опазване на професионалната тайна по отношение на всяка поверителна информация, която е стигнала до тяхното знание в хода на изпълнението на техните (...) задължения или упражняването на техните правомощия.*

Член 50

Професионална тайна

(...)

РАЗДЕЛ 2
КОМПЕТЕНТНОСТ, ЗАДАЧИ И ПРАВОМОЩИЯ

Член 51

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, букви в) или д), компетентен е надзорният орган на съответната държава членка. В тези случаи член 51а 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 51а

Компетентност на водещия надзорен орган

1. Без да се засяга член 51, надзорният орган на основното място на установяване или на единственото място на установяване на администратора или обработващия лични данни е компетентен да функционира като водещ надзорен орган за транснационалното обработване, извършвано от този администратор или обработващ лични данни в съответствие с процедурата по член 54а.
2. (...)
- 2а. Чрез дерогация от параграф 1 всеки надзорен орган е компетентен да разглежда внесена при него жалба или да се занимава с евентуални нарушения на настоящия регламент, ако случаят се отнася единствено до място на установяване в държавата членка на надзорния орган или засяга съществено субекти на данни единствено в тази държава членка.

- 2б. В посочените в параграф 2а случаи надзорният орган незабавно уведомява за това водещия надзорен орган. В срок от три седмици след като е бил уведомен, водещият надзорен орган взема решение за това дали той самият ще се занимае или не със случая в съответствие с процедурата, предвидена в член 54а, като отчита дали администраторът или обработващият лични данни е установен в държавата членка на надзорния орган, който го е уведомил.
- 2в. Когато водещият надзорен орган реши да се занимае със случая, се прилага процедурата по член 54а. Надзорният орган, информирал водещия надзорен орган, може да предостави на този орган проект за решение. Водещият надзорен орган отчита в максимална степен този проект при изготвянето на проекта за решение, посочен в член 54а, параграф 2.
- 2г. В случай че водещият надзорен орган реши да не се занимае със случая, надзорният орган, уведомил водещия надзорен орган, разглежда случая в съответствие с членове 55 и 56.
3. За извършването от тях транснационално обработване администраторът или обработващият лични данни комуникират единствено с водещия надзорен орган.
4. (...)

Член 51б

Идентифициране на надзорния орган, компетентен за основното място на установяване

(...)

Член 51в

Регистър „обслужване на едно гише“

(...)

Задачи

1. Без да се засягат останалите задачи, определени с настоящия регламент, на своята територия всеки надзорен орган:
 - a) наблюдава и осигурява прилагането на настоящия регламент;
 - aa) насърчава обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни. Обръща се специално внимание на дейностите, специално насочени към децата;
 - аб) дава становища, в съответствие с националното право, 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 на лични данни;
 - ав) насърчава информираността на администраторите и обработващите лични данни за задълженията им по силата на настоящия регламент;
 - аг) 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;
 - б) разглежда жалбите, подадени от субект на данни или от орган, организация или сдружение, представляващо субект на данни, в съответствие с член 73, и проучва предмета на жалбата, доколкото това е целесъобразно, и информира субекта на данни или образуването, организацията или сдружението за напредъка и резултатите от проучването в разумен срок, особено ако е необходимо по-нататъшно проучване или координиране с друг надзорен орган;
 - в) сътрудничи си с други надзорни органи, включително чрез обмен на информация и взаимопомощ, с оглед осигуряване на съгласувано прилагане и изпълнение на настоящия регламент;
 - г) извършва проучвания по прилагането на настоящия регламент, включително въз основа на информация, получена от друг надзорен или публичен орган;
 - д) 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;

- е) приема стандартните договорни клаузи, посочени в член 26, параграф 2в;
- еа) съставя и изготвя списък във връзка с изискването за оценка на въздействието върху защитата на данните съгласно член 33, параграф 2а;
- ж) дава становища по операциите за обработване на данни, посочени в член 34, параграф 3;
- жа) насърчава съставянето на кодекси за поведение съгласно член 38 и предоставя становище и одобрява подобни кодекси за поведение, които осигуряват достатъчно гаранции съгласно член 38, параграф 2;
- жб) насърчава създаването на механизми за сертифициране за защита на данните и на печати и маркери за защита на данните, и одобрява критериите за сертифициране съгласно член 39, параграф 2а;
- жв) когато е приложимо, извършва периодичен преглед на сертификатите, издадени в съответствие с член 39, параграф 4;
- з) изготвя и публикува критериите за акредитация на органите за наблюдение на кодексите за поведение съгласно член 38а и на сертифициращите органи съгласно член 39а;
- за) извършва акредитацията на органите за наблюдение на кодексите за поведение съгласно член 38а и на сертифициращите органи съгласно член 39а;
- зб) дава разрешение за договорните клаузи, посочени в член 42, параграф 2а, буква а);
- и) одобрява задължителните фирмени правила съгласно член 43;
- й) допринася за дейностите на Европейския комитет по защита на данните;
- к) изпълнява други задачи, свързани със защитата на лични данни.

2. (...)

3. (...)

4. Всеки надзорен орган улеснява подаването на жалбите, посочени в параграф 1, буква б), чрез мерки като например осигуряване на формуляр за подаване на жалби, който може да бъде попълнен също и по електронен път, без да се изключват други средства за комуникация.

5. Изпълнението на задачите от страна на всеки надзорен орган е безплатно за субекта на данни и за длъжностното лице по защита на данните, ако има такова.

6. Когато исканията са очевидно неоснователни или прекомерни, по-специално поради своята повторяемост, надзорният орган може да откаже да предприеме действия по искането. Надзорният орган носи тежестта на доказване на очевидно неоснователния или прекомерния характер на искането.

Член 53
Правомоция

1. Всяка държава членка урежда със закон нейният надзорен орган да има поне следните правомоция за разследване:
- а) да разпорежда на администратора и на обработващия лични данни и когато е приложимо — на представителя на администратора да предоставят всяка информация, която той поиска за изпълнението на своите задачи;
 - аа) да провежда разследвания под формата на одити във връзка със защитата на данните;
 - аб) да извършва преглед на сертификатите, издадени в съответствие с член 39,
параграф 4;
 - б) (...)
 - в) (...)
 - г) да уведомява администратора или обработващия лични данни за предполагаемо нарушение на настоящия регламент;
 - га) да получава от администратора или обработващия лични данни достъп до всички лични данни и до цялата информация, необходима за изпълнението на своите задачи;
 - гб) да получава достъп до всички помещения на администратора и обработващия лични данни, включително до оборудване и средства за обработване на данни, в
съответствие с правото на Съюза или процесуалното право на държавата членка.
- 1а. (...)
- 1б. Всяка държава членка урежда със закон нейният надзорен орган да има следните
корективни правомоция:
- а) да отправя предупреждения до администраторите или обработващите 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 администраторите или обработващите лични данни, когато операции по обработване на данни са нарушили разпоредбите на настоящия регламент;
- в) (...);
- ва) да разпорежда на администратора или на обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно настоящия регламент;
- г) да разпорежда на администраторите или обработващите лични данни да съобразят операциите по обработване на данни с разпоредбите на настоящия регламент; ако се налага, това да стане по указан начин и в определен срок; по-специално, като разпорежда коригирането, ограничаването или заличаването на данни съгласно членове 16, 17 и 17а, както и уведомяването за тези действия на получатели, пред които данните са били разкрити съгласно член 17, параграф 2а и член 17б;
- д) да налага временно или окончателно ограничаване на обработването (...);
- е) да разпорежда преустановяването на притока на данни към получател в трета държава или към международна организация;
- ж) да налага административна глоба съгласно членове 79 и 79а, в допълнение към или вместо мерките, посочени в настоящия параграф, в зависимост от особеностите на всеки отделен случай.
- 1в. Всяка държава членка урежда със закон нейният надзорен орган да има следните правомощия да дава разрешения и становища:
 - а) да дава становища на администратора в съответствие с процедурата по предварителна консултация, посочена в член 34,
 - аа) да издава по собствена инициатива или при поискване становища до националния парламент, правителството на държавата членка или, в съответствие с националното право — до други институции и органи, както и до обществеността по всякакви въпроси, свързани със защитата на лични данни;
 - аб) да дава разрешение за обработването, посочено в член 34, параграф 7а, ако съгласно правото на държавата членка се изисква такова предварително разрешение;
 - ав) да дава становища и да одобрява проекти на кодекси за поведение съгласно член 38, параграф 2;
 - аг) да акредитира сертифициращи органи при условията на член 39а;
 - ад) да издава сертификати и да одобрява критериите за сертифициране в съответствие с член 39, параграф 2а;
 - а) да приема стандартните клаузи за защита на данните, посочени в член 42, параграф 2, буква в);
 - б) да дава разрешение за договорните клаузи, посочени в член 42, параграф 2а, буква а);

- ва) да дава разрешение за административните споразумения, посочени в член 42, параграф 2а, буква г);
- г) да одобрява задължителните фирмени правила съгласно член 43.
2. Упражняването на правомощията, предоставени на надзорния орган по силата на настоящия член, се осъществява при осигуряване на подходящи гаранции, в т.ч. ефективни средства за съдебна защита и справедлив съдебен процес, определени в правото на Съюза и държавите членки в съответствие с Хартата на основните права на Европейския съюз.
3. 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 илипо друг начин да участва в съдебни производства, с цел осигуряване на изпълнението на настоящия регламент.
4. (...)
5. (...)

Член 54

Доклад за дейността

Всеки надзорен орган изготвя годишен доклад за своята дейност. Докладът се предоставя на националния парламент, правителството и други органи, посочени в националното право. Докладът се предоставя на обществеността, Европейската комисия и Европейския комитет по защита на данните.

ГЛАВА VII
СЪТРУДНИЧЕСТВО И СЪГЛАСУВАНОСТ
РАЗДЕЛ 1
СЪТРУДНИЧЕСТВО

Член 54а

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 като се стреми към постигане на консенсус (...). Водещият надзорен орган и засегнатите надзорни органи обменят всякаква имаща отношение информация помежду си.

- 1а. Водещият надзорен орган може да поиска по всяко време от другите засегнати надзорни органи да предоставят взаимопомощ съгласно член 55 и може да провежда съвместни операции съгласно член 56, по-специално за да извършва разследвания или да наблюдава изпълнението на мярка, засягаща администратор или обработващ лични данни, установен в друга държава членка.

2. 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 предвид вижданията им.

3. Ако някой от другите засегнати надзорни органи изрази адекватно и обосновано възражение срещу проекта за решение в срок от четири седмици, след като е било поискано мнението му в съответствие с параграф^о2, водещият надзорен орган, в случай че не приеме възражението или счита, че то не е адекватно и обосновано, отнася въпроса до механизма за съгласуваност, посочен в член 57. (...)

3а. Ако водещият надзорен орган възнамерява да приеме направеното възражение, той изпраща на другите засегнати надзорни органи преработен проект за решението, за да получи тяхното мнение. За този преработен проект за решението се следва процедурата, посочена в параграф 3, за срок от две седмици.

4. Когато нито един от другите засегнати органи не е възразил срещу проекта за решение, представен от водещия надзорен орган в посочения в параграфи 3 и 3а срок, се счита, че водещият надзорен орган и засегнатите надзорни органи са съгласни с този проект за решение и са обвързани от него.

4а. 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 Европейския комитет по защита на данните за въпросното решение, като включва резюме на съответните факти и основания. Надзорният орган, до когото е била подадена жалбата, информира жалбоподателя за решението.

4б. Чрез дерогация от параграф 4а, когато дадена жалба е отклонена или отхвърлена, надзорният орган, до който е била подадена жалбата, приема решението и уведомява жалбоподателя за него и информира администратора за него.

4бб. Когато водещият надзорен орган и засегнатите надзорни органи са постигнали съгласие определени части от жалбата да бъдат отклонени 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 отклоняването или отхвърлянето на тази жалба, уведомява за него жалбоподателя и информира за това администратора или обработващия лични данни.

4в. След като е бил уведомен за решението на водещия надзорен орган съгласно параграфи 4а и 4бб, 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.

4г. 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 61.

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

Член 54б

Сътрудничество между водещия надзорен орган и другите засегнати надзорни органи в отделни случаи на евентуално несъответствие с настоящия регламент

(...)

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. Искането за помощ съдържа 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 изпратено искане за помощ, няма право да откаже да го изпълни, освен ако:
 - а) е некомпетентен относно предмета на искането или мерките, които се изисква да изпълни; или
 - б) удовлетворяването на искането би било в противоречие с разпоредбите на настоящия регламент или правото на Съюза или 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 или предприетите мерки в отговор на искането. В случай на отказ по силата на параграф 4 този орган излага мотивите си за отхвърляне на искането.

6. Надзорните органи по правило предоставят информацията, поискана от други надзорни органи, по електронен път, като използват стандартизиран формат.

7. За действията, предприети в отговор на искане за взаимопомощ, не се събират такси. Надзорните органи могат да приемат с други надзорни органи правила за предоставяне на обезщетение от страна на други надзорни органи 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, искащият надзорен орган може да приеме временна мярка на територията на своята държава членка в съответствие с член 51, параграф 1 и отнася въпроса до Европейския комитет по защита на данните (...), в съответствие с механизма за съгласуваност, предвиден в член 57.

9. Надзорният орган определя срок на действие на временната мярка, който не надвишава три месеца. Надзорният орган уведомява незабавно Европейския комитет по защита на данните (...) за прилагането на такава мярка, както и за основанията за приемането ѝ, в съответствие с механизма за съгласуваност, предвиден в член 57.

10. Комисията може да определи формата и процедурите за взаимопомощ по настоящия член, както и договореностите за обмена на информация чрез електронни средства между надзорните органи и между надзорните органи и Европейския комитет по защита на данните, и по-специално стандартизирания формат, посочен в параграф 6. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2.

Съвместни операции на надзорни органи

1. Надзорните органи могат, когато е подходящо, да провеждат съвместни операции, включително съвместни разследвания и съвместни мерки за изпълнение, в които участват членове или персонал от надзорни органи на други държави членки.

2. В случаите, 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 съвместните операции по целесъобразност. Компетентният надзорен орган 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 своята държава 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 на персонала от надзорния орган домакин. Спрямо членовете или персонала на командироващия надзорен орган се прилага националното право на надзорния орган домакин. (...)

3а. Когато в съответствие с параграф 1 персонал на командироващия надзорен орган участва в операция в друга държава членка, държавата членка на надзорния орган домакин носи отговорността за всякакви вреди, нанесени от този персонал по време на операциите, в съответствие с правото на държавата членка, на чиято територия се провежда операцията.

3б. Държавата членка, на чиято територия е нанесена вредата, компенсира 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 на лицата, които са имали правото да ги получат от тяхно име.

3в. Без да се засяга упражняването на правата ѝ по отношение на трети страни и с изключение на параграф 3б, всяка държава членка се въздържа в случая, предвиден в параграф 1, да иска обезщетение за вредите, които е претърпяла от друга държава членка.

4. (...)

5. Когато се планира съвместна операция и в срок от един месец даден надзорен орган не изпълни задължението, предвидено във второто изречение на параграф 2, другите надзорни органи могат да приемат временна мярка на територията на своята държава членка в съответствие с член 51, параграф 1.

6. Надзорният орган определя срока на действие на временната мярка, посочена в параграф 5, който не надвишава три месеца. Надзорният орган уведомява незабавно Европейския комитет по защита на данните (...) за прилагането на такава мярка, както и за основанията за приемането ѝ, в съответствие с механизма за съгласуваност, предвиден в член 57.

РАЗДЕЛ 2

СЪГЛАСУВАНОСТ

Член 57

Механизъм за съгласуваност

1. За целите, определени в член 46, параграф 1а, надзорните органи си сътрудничат помежду си и с Комисията чрез механизъм за съгласуваност, както е определено в настоящия раздел.
2. Европейския комитет по защита на данните дава становище всеки път, когато компетентен надзорен орган възнамерява да приеме някоя от мерките, изброени по-долу (...). За тази цел компетентният надзорен орган предава проекта за решението на Европейския комитет по защита на данните, когато то:
 - а) (...);
 - б) (...);
 - в) 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 33, параграф 2а; или
 - ва) се отнася до въпрос съгласно член 38, параграф 2б дали проект за кодекс на поведение или изменение или удължаване на действието на кодекс на поведение съответства на настоящия регламент; или
 - вб) има за цел одобряване на критериите за акредитиране на орган съгласно член 38а, параграф 3 или орган по сертифициране съгласно (...) член 39а, параграф 3;

- г) има за цел определяне на стандартните клаузи за защита на данните, посочени в член 42, параграф 2, буква в); или
- д) има за цел даване на разрешение за договорните клаузи, посочени в член 42, параграф 2, буква г); или
- е) има за цел одобряване на задължителни фирмени правила по смисъла на член 43.

3. Европейският комитет по защита на данните приема решение със задължителен характер в следните случаи:

- а) Когато, в случаи по член 54а, параграф 3, *засегнат* надзорен орган е изразил адекватно и обосновано възражение срещу проект за решение на водещия орган или водещият орган е отхвърлил възражението като неадекватно и/или необосновано. Решението със задължителен характер се отнася за всички въпроси, които са предмет на адекватното и обосновано възражение, особено когато има нарушение на регламента;
- б) Когато има противоречиви виждания за това кой от *засегнатите* надзорни органи е компетентен за основното място на установяване;
- в) (...)
- г) Когато компетентният надзорен орган не е поискал становището на Европейския комитет по защита на данните в случаите, посочени в параграф 2 от настоящия член, или не се е съобразил със становището на Европейския комитет по защита на данните, дадено по член 58. В този случай всеки засегнат надзорен орган или Комисията може да отнесе въпроса до Европейския комитет по защита на данните.

4. Всеки надзорен орган, председателят на Европейския комитет по защита на данните или Комисията може да поиска разглеждането на въпрос с общо приложение или с последици в повече от една държава членка от Европейския комитет по защита на данните с цел получаване на становище, по-специално когато даден компетентен надзорен орган не изпълнява задълженията за взаимопомощ съгласно член 55 или за съвместни операции съгласно член 56.

5. Надзорните органи и Комисията предоставят на Европейския комитет по защита на данните, по електронен път и посредством стандартизиран формат, всякаква 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.

6. Председателят на Европейския комитет по защита на данните без ненужно забавяне информира по електронен път членовете на Европейския комитет по защита на данните и Комисията за всяка значима информация, която му е била съобщена, като използва стандартизиран формат. При необходимост секретариатът на Европейския комитет по защита на данните предоставя писмен превод на съответната информация.

Член 58

Становище на Европейския комитет по защита на данните

1. (...)

2. (...)

3. (...)

4. (...)

5. (...)

6. (...)

7. В случаите, посочени в член 57, параграфи 2 и 4, Европейският комитет по защита на данните 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 един месец с обикновено мнозинство от членовете на Европейския комитет по защита на данните. Този срок може да бъде удължен с още един месец с оглед сложността на въпроса. По отношение на проекта за решение, разпространен до членовете на Комитета съгласно член 57, параграф 6, за член, който не е представил възражение в посочения от председателя срок, се счита, че е съгласен с проекта за решение.

7а. В рамките на посочения в параграф 7 срок компетентният надзорен орган не може да приема своя проект за решение в съответствие с член 57, параграф 2.

7б. Председателят на Европейския комитет по защита на данните информира без излишно забавяне надзорния орган, посочен — в зависимост от случая — в член 57, параграфи 2 и 4, и Комисията за становището и го оповестява публично.

8. Надзорният орган, посочен в член 57, параграф 2, взема предвид в най-голяма степен становището на Европейския комитет по защита на данните и в срок от две седмици след получаване на становището информира по електронен път председателя на Европейския комитет по защита на данните дали запазва или ще измени своя проект за решение и им представя изменения проект за решение, ако има такъв, като използва стандартизиран формат.

9. Когато засегнатият надзорен орган информира председателя на Европейския комитет по защита на данните в посочения в параграф 8 срок, че не възнамерява да се съобрази със становището на Комитета, изцяло или отчасти, като предостави съответните основания, се прилага член 57, параграф 3.

10. (...)

11. (...)

Член 58а

Решения на Европейския комитет по защита на данните

1. В случаите, посочени в член 57, параграф 3, Европейския комитет по защита на данните приема решение по въпроса, отнесен до него, с цел да осигури правилно и последователно прилагане на настоящия регламент в отделните случаи. Решението трябва да бъде обосновано, адресирано до водещия надзорен орган и всички засегнати надзорни органи и е със задължителен характер за тях.
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. Този срок може да бъде удължен с още един месец с оглед сложността на въпроса.
3. В случай че 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. В случай че членовете на Комитета са разделени поравно на две, решението се приема с решаващия глас на председателя.
4. Засегнатите надзорни органи не могат да приемат решение по отнесения до Комитета въпрос съгласно параграф 1 в рамките на сроковете, посочени в параграфи 2 и 3.
5. (...)

6. Председателят на Европейския комитет по защита на данните уведомява без излишно забавяне засегнатите надзорни органи за решението, посочено в параграф 1. Същата информация се изпраща и на Комисията. Решението се публикува на уебсайта на Европейския комитет по защита на данните без забавяне след като надзорният орган е уведомил за окончателното си решение, посочено в параграф 7.
7. 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, без излишно забавяне и най-късно един месец след като Европейският комитет по защита на данните е уведомил за решението си. Водещият надзорен орган или, според случая, надзорният орган, до който е била подадена жалбата, информира Европейския комитет по защита на данните за датата, на която администраторът или обработващият лични данни и съответно субектът на данни са били уведомени за неговото окончателно решение. Окончателното решение на засегнатите надзорни органи се приема по реда на член 54а, параграфи 4а, 4б и 4бб. Окончателното решение се позовава на решението, посочено в параграф 1, и уточнява, че посоченото в параграф 1 решение ще бъде публикувано на уебсайта на Европейския комитет по защита на данните в съответствие с параграф 6. Към окончателното решение се прилага решението, посочено в параграф 1.

Член 59

Становище на Комисията

(...)

Член 60

Суспендиране на проектомярка

(...)

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 член 57, или процедурата, предвидена в член 54а, да приеме незабавно временни мерки, които ще имат правни последици на територията на собствената му държава членка, с определен срок на валидност. Надзорният орган съобщава незабавно тези мерки и мотивите за приемането им на другите засегнати надзорни органи, Европейския комитет по защита на данните и 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 Европейския комитет по защита на данните 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 Европейския комитет по защита на данните, 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 58, параграф 7 и член 58а, параграф 2, спешното становище или спешното решение със задължителен характер, посочени в параграфи 2 и 3 от настоящия член, се приема в срок от две седмици с обикновено мнозинство на членовете на Европейския комитет по защита на данните.

Член 62

Актове за изпълнение

1. Комисията може да приема актове за изпълнение с общ обхват за:

а) (...);

б) (...);

в) (...);

г) да посочи договореностите за обмена на информация чрез електронни средства между надзорните органи, както и между надзорните органи и Европейския комитет по защита на данните, по-специално стандартизирания формат, посочен в член 57, параграфи 5 и 6 и член 58, параграф 8.

Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 87, параграф 2.

2. (...)

3. (...)

Член 63

Правоприлагане

(...)

Раздел 3
Европейски комитет по защита на данните

Член 64
Европейски комитет по защита на данните

1а. Създава се Европейски комитет по защита на данните, който е орган на Съюза и притежава правосубектност.

1б. Европейският комитет по защита на данните се представлява от своя председател.

2. Европейският комитет по защита на данните е съставен от по един ръководител на надзорен орган от всяка държава членка или неговия представител и на Европейския надзорен орган по защита на данните.

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

4. Комисията и Европейският надзорен орган по защита на данните или негов представител имат право да участват в дейностите и заседанията на Европейския комитет по защита на данните без право на глас. Комисията посочва свой представител. Председателят на Европейския комитет по защита на данните уведомява Комисията (...) за дейностите на Европейския комитет по защита на данните.

Член 65

Независимост

1. Европейският комитет по защита на данните действа независимо при изпълнението на задачите си или упражняването на правомощията си съгласно членове 66 (...) и 67.
2. Без да се засягат исканията на Комисията, посочени в член 66, параграф 1, буква б) и параграф 2, Европейският комитет по защита на данните не търси и не приема указания от никого при изпълнението на своите задачи или упражняването на своите правомощия.

Член 66

Задачи на Европейския комитет по защита на данните

1. Европейският комитет по защита на данните утвърждава съгласуваното прилагане на настоящия регламент. За тази цел по-специално Европейският комитет по защита на данните по своя собствена инициатива или по искане на Комисията:
 - аа) наблюдава и осигурява правилното прилагане на регламента в случаите, предвидени в член 57, параграф 3, без да се засягат задачите на националните надзорни органи;
 - а) консултира Комисията по всеки въпрос, свързан със защитата на личните данни в Съюза, включително относно всяко предложено изменение на настоящия регламент;

- б) разглежда по своя собствена инициатива, по инициатива 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;
- ба) изготвя насоки за надзорните органи относно прилагането на мерките, посочени в член 53, параграфи 1, 1б и 1в, и определянето на размера на административни глоби съгласно членове 79 и 79а;
- в) извършва преглед на практическото прилагане на насоките, препоръките и най-добрите практики, посочени в букви б) и ба);
- ва) 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 38 и 39;
- вб) извършва акредитацията на сертифициращи органи и периодичния ѝ преглед съгласно член 39а и поддържа публичен регистър на акредитираните органи съгласно член 39а, параграф 6 и на акредитираните администратори и обработващи лични данни, установени в трети държави, съгласно член 39, параграф 4;
- вг) уточнява изискванията, посочени в член 39а, параграф 3, с оглед на акредитацията на сертифициращи органи по член 39;
- вд) предоставя на Комисията становища относно нивото на защита на личните данни в трети държави или международни организации, по-специално в случаите, посочени в член 41;
- г) дава становища по проекти за решения на надзорните органи по силата на механизма за съгласуваност, посочен в член 57, параграф 2, и по въпроси, разглеждани съгласно параграф 4 от същия член;

- д) насърчава сътрудничеството и ефективния двустранен и многостранен обмен на информация и практики между надзорните органи;
- е) насърчава общите програми за обучение и улеснява обмена на персонал между надзорните органи, както и с надзорните органи на трети държави или на международни организации, когато е целесъобразно;
- ж) насърчава обмена на знания и документация относно законодателството и практиките в областта на защитата на данните с надзорните органи по защита на данните в цял свят;
- з) (...);
- и) 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 Европейския комитет по защита на данните, тя може да посочи срок, като се взема предвид спешността на въпроса.
3. Европейският комитет по защита на данните изпраща своите становища, насоки, препоръки и най-добри практики на Комисията и на комитета, посочен в член 87, и ги прави обществено достояние.

Член 67

Доклади

1. (...)
2. Европейският комитет по защита на данните изготвя годишен доклад относно защитата на физически лица по отношение на обработването на лични данни в Съюза когато е от значение — в трети държави и международни организации. Докладът се оповестява публично и се предава на Европейския парламент, Съвета и Комисията.
3. В годишния доклад се включва преглед на практическото прилагане на насоките, препоръките и най-добрите практики, посочени в член 66, параграф 1, буква в), както и на решенията със задължителен характер, посочени в член 57, параграф 3.

Член 68

Процедура

1. Европейският комитет по защита на данните приема решенията със задължителен характер, посочени в член 57, параграф 3, в съответствие с изискванията относно мнозинството, установени в член 58а, параграфи 2 и 3. Що се отнася до решенията, свързани с останалите задачи, изброени в член 66 от настоящия регламент, те се вземат с обикновено мнозинство от членовете.
2. Европейският комитет по защита на данните приема свой процедурен правилник с мнозинство от две трети от своите членове и определя своите методи на работа.

Член 69

Председател

1. Европейският комитет по защита на данните избира председател и двама заместник-председатели измежду своите членове с обикновено мнозинство(...).
2. Мандатът на председателя и на заместник-председателите е пет години и може да бъде подновяван еднократно.

Член 70

Задачи на председателя

1. Председателят има следните задачи:
 - а) да свиква заседанията на Европейския комитет по защита на данните и да изготвя дневния ред;
 - aa) да уведоми водещия надзорен орган и засегнатите надзорни органи за решенията, приети от Европейския комитет по защита на данните съгласно член 58a;
 - б) да осигурява своевременното изпълнение на задачите на Европейския комитет по защита на данните, по-специално във връзка с механизма за съгласуваност, посочен в член 57.
2. В своя процедурен правилник Европейският комитет по защита на данните определя разпределението на задачите между председателя и заместник-председателите.

Член 71
Секретариат

1. Европейският комитет по защита на данните разполага със секретариат, който се осигурява от секретариата на Европейския надзорен орган по защита на данните (...).

1а. Секретариатът извършва задачите си изключително под ръководството на председателя на Европейския комитет по защита на данните.

1б. Служителите на секретариата на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачите, възложени на Европейския комитет по защита на данните с настоящия регламент, следва да бъдат организационно отделени от служителите, участващи в изпълнението на задачи, възложени на Европейския надзорен орган по защита на данните, и да подлежат на отделни механизми за докладване.

1в. При необходимост Европейският комитет по защита на данните, след консултация с Европейския надзорен орган по защита на данните, изготвя и публикува кодекс за поведение за прилагане на настоящия член, който се прилага спрямо служителите на секретариата на Европейския надзорен орган по защита на данните, участващи в изпълнението на задачите, възложени на Европейския комитет по защита на данните с настоящия регламент.

2. Секретариатът предоставя аналитична, административна и логистична подкрепа на Европейския комитет по защита на данните.

3. Секретариатът отговаря по-специално за:

- а) ежедневната работа на Европейския комитет по защита на данните;
- б) комуникацията между членовете на Европейския комитет по защита на данните, неговия председател и Комисията, както и за комуникацията с други институции и с обществеността;

- в) използването на електронни средства за вътрешна и външна комуникация;
- г) превода на значима информация;
- д) подготовката на заседанията на Европейския комитет по защита на данните и последващите действия във връзка с тях;
- е) подготовката, изготвянето и публикуването на становища, решения относно уреждането на спорове между надзорни органи и други текстове, приети от Европейския комитет по защита на данните.

Член 72

Поверителност

1. Обсъжданията на Европейския комитет по защита на данните са поверителни.
2. Достъпът до документи, предоставени на членове на Европейския комитет по защита на данните, експерти и представители на трети страни се урежда от Регламент (ЕО) № 1049/2001.

ГЛАВА VIII

СРЕДСТВА ЗА ПРАВНА ЗАЩИТА, ОТГОВОРНОСТ ЗА ПРИЧИНЕНИ ВРЕДИ И САНКЦИИ

Член 73

Право на подаване на жалба до надзорен орган

1. Без да се засягат които и да било други административни или съдебни средства за защита, всеки субект на данни има право да подаде жалба до един 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 отнасящи се до него лични данни не се извършва в съответствие с настоящия регламент.
2. (...)
3. (...)
4. (...)
5. Надзорният орган, до когото е подадена жалбата, информира жалбоподателя за напредъка в процеса на разглеждане и за резултата от жалбата, включително за възможността за съдебна защита съгласно член 74 (...).

Член 74

Право на ефективна съдебна защита срещу надзорен орган

1. Без да се засяга което и да било друго административно или несъдебно средство за защита, всяко физическо или юридическо лице има право на ефективни средства за съдебна защита срещу правнообвързващо решение на надзорен орган, което го касае.

2. Без да се засяга което и да било друго административно или несъдебно средство за защита, всяко физическо или юридическо лице има право на ефективни средства за съдебна защита, когато компетентният надзорен орган съгласно член 51 и член 51a не е разгледал жалбата или не е информирал субекта на данните в срок от три месеца или по-кратък срок, предвиден в правото на Съюза или на държавата членка, за напредъка в процеса на разглеждане или за резултата от жалбата, подадена съгласно член 73.
3. (...) Производствата срещу (...) надзорен орган се образуват пред съдилищата на държавата членка, в която е установен съответният надзорен орган.
- 3a. Когато се образува производство срещу решението на надзорен орган, което е било предхождано от становище или решение на Европейския комитет по защита на данните в съответствие с механизма за съгласуваност, надзорният орган предава това становище или решение на съда.
4. (...)
5. (...)

Член 75

Право на ефективна съдебна защита срещу администратор или обработващ лични данни

1. Без да се засяга което и да било налично административно или несъдебно средство за защита, включително правото на жалба до надзорен орган по член 73, субектите на данни имат право на ефективни средства за съдебна защита, ако считат, че са нарушени правата им по настоящия регламент вследствие на обработването на личните им данни при неспазване на разпоредбите на 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 алтернатива такива производства могат да се образуват пред съдилищата на държавата членка, в която субектът на данните пребивава обичайно, освен ако администраторът или обработващият личните данни не е публичен орган, който действа в изпълнение на своите публични правомощия.
3. (...)
4. (...)

Член 76

Представителство на субектите на данни

1. Субектът на данни има право да възложи на орган, организация или сдружение, което е учредено правомерно в съответствие с правото на държава членка и чиито уставни цели включват защита на правата и свободите на субектите на данни по отношение на защитата на техните лични данни, да подаде жалбата от негово име и да упражни от негово име правата, посочени в членове 73, 74 и 75.

1a. (...)

2. Държавите членки могат да предвидят, че всеки орган, организация или сдружение от посочените в параграф 1, независимо от възложения от субекта на данни мандат (...), има право да подаде в такава държава членка жалба до компетентния надзорен орган съгласно член 73 и да упражни правата, посочени в членове 73, 74 и 75, ако счита, че правата на субект на данни са били нарушени в резултат на обработване на лични данни, което не е в съответствие с настоящия регламент.

3. (...)

4. (...)

Член 76a

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 личните 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.

2а. 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.

3. (...)

Член 77

Право на обезщетение и отговорност за причинени вреди

1. Всяко лице, което е претърпяло материални или нематериални вреди в резултат на операция по обработване, която не съответства на настоящия регламент, има право да получи обезщетение от администратора или обработващия лични данни за нанесените вреди.
2. Администраторът (...), участващ в операцията по обработване, носи отговорност за вреди, произтичащи от извършеното обработване на лични данни, което не съответства на настоящия регламент. Обработващият лични данни носи отговорност за (...) вреди, произтичащи от извършеното обработване, само ако не е спазил задълженията по настоящия регламент, конкретно насочени към обработващите лични данни, или е действал извън законосъобразните указания на администратора или в противоречие с тях.
3. Администраторът или обработващият лични данни се освобождават от отговорност в съответствие с параграф 2, (...) ако (...) докажат, че по никакъв начин не са отговорни (...) за събитието, причинило вредата.
4. *Когато в една и съща операция по обработване на лични данни участва повече от един администратор или обработващ лични данни или участват и администратор, и обработващ лични данни, и когато те са отговорни за някаква вреда във връзка с обработването, в съответствие с параграфи 2 и 3, (...) всеки администратор или обработващ лични данни носи (...) отговорност за цялата вреда.*

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 на параграф 2.
6. Съдебните производства във връзка с упражняването на правото на обезщетение се образуват пред съдилища, компетентни съгласно националното право на държавата членка, посочена в член 75, параграф 2.

Член 78

Санкции

(...)

Член 79

Общи условия за налагане на административни глоби

1. Всеки надзорен орган (...) гарантира, че наложените от него административни глоби в съответствие с настоящия член за извършени нарушения на настоящия регламент, посочени в член 79а (...), са във всеки конкретен случай ефективни, съразмерни и възпиращи.
2. (...)
- 2а. В зависимост от обстоятелствата по всеки конкретен случай административните глоби се налагат в допълнение към или вместо мерките, посочени в член 53, параграф 1б, букви а) до е). Когато се взема решение дали да бъде наложена административна глоба (...) и за определяне на размера на административната глоба, във всеки конкретен случай надлежно се разглеждат (...) следните елементи:

- а) естеството, тежестта и продължителността на нарушението, като се взема предвид естеството, обхватът и целта на съответното обработване, както и броят на засегнатите субекти на данните и степента на причинената им вреда;
- б) дали нарушението е извършено умишлено или по небрежност;
- в) (...);
- г) действията, предприети от администратора или обработващия лични данни за смекчаване на последиците от вредите, претърпени от субектите на данни;
- д) степената на отговорност на администратора или обработващия лични данни във връзка с технически и организационни мерки, въведени от тях в съответствие с членове 23 и 30;
- е) евентуални свързани предишни нарушения, извършени от администратора или обработващия лични данни;
- ж) (...);
- з) начинът, 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) ако по отношение на засегнатия администратор или обработващ лични данни вече са били наложени някои мерки, посочени в (...) и член 53, параграф 1б, и букви а), г), д) и е) по същия въпрос, дали са спазени тези мерки;
- й) придържането към одобрени кодекси на поведение съгласно член 38 или одобрени механизми за сертифициране съгласно член 39;
- к) (...);
- л) (...);
- м) други утежняващи или смекчаващи фактори, приложими към обстоятелствата по случая.
- 3. (...)
- 3а. (...)

36. Всяка държава членка може да предвиди правила относно това дали и до каква степен могат да бъдат налагани административни глоби на публични органи и структури, установени в тази държава членка.
4. Упражняването от надзорния орган (...) на неговите правомощия по настоящия член зависи от съответните процедурни гаранции в съответствие с правото на Съюза и на държавите членки, в т.ч. ефективни средства за съдебна защита и справедлив съдебен процес.
5. Държавите членки могат да се въздържат от въвеждане на разпоредби за административните глоби, посочени в член 79а, параграфи 1, 2 и 3, когато техните правни системи не предвиждат административни глоби и към [датата, посочена в член 91, параграф 2] в тяхното национално право посочените нарушения вече подлежат на наказателни санкции, като същевременно гарантират, че тези наказателни санкции са ефективни, съразмерни и възпиращи, и вземат предвид размера на административните глоби, предвидени в настоящия регламент.

Когато вземат такова решение, държавите членки нотифицират пред Комисията съответните части от своето наказателно право.

Член 79а

Административни глоби

1. Надзорният орган (...) може да наложи глоба, която не надвишава 250 000 EUR, или за предприятия — 0,5 % от общия годишен оборот в световен мащаб за предходната финансова година, на администратор, който умишлено или по небрежност:
- а) не отговаря в рамките на срока, предвиден в член 12, параграф 2, на исканията на субекти на данни;
 - б) събира такса в нарушение на член 12, параграф 4, първото изречение.
2. Надзорният орган (...) може да наложи глоба, която не надвишава 500 000 EUR, или за предприятия — 1 % от общия годишен (...) оборот в световен мащаб за предходната финансова година, на администратор или обработващ лични данни, който умишлено или по небрежност:

- а) не предоставя информацията или (...) предоставя непълна информация, или не предоставя информацията [навреме или] по [достатъчно] прозрачен начин на субекта на данни съгласно член 12, параграф 3, член 14 и член 14а;
- б) не осигурява достъп на субекта на данни или не коригира личните данни съгласно членове 15 и 16 (...);
- в) не заличава лични данни в нарушение на правото на заличаване и правото „да бъдеш забравен“ съгласно член 17, параграф 1, буква а), б), г) или д);
- г) (...)
- га) обработва лични данни в нарушение на правото на ограничаване на обработването на лични данни съгласно член 17а или не информира субекта на данни преди да бъде отменено ограничението върху обработването на лични данни съгласно член 17а, параграф 4;
- гб) не съобщава за всяка корекция, заличаване или ограничаване на обработването на лични данни всеки получател, на когото администраторът е разкрил лични данни, в нарушение на член 17б;
- гв) не предоставя на субекта на данните свързаните с него лични данни (...) в нарушение на член 18;
- гг) обработва лични данни след възражение от субекта на данни съгласно член 19, параграф 1, без да докаже, че има 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;
- гд) не предоставя на субекта на данни информация за правото на възражение срещу обработването на лични данни за целите на директния маркетинг съгласно член 19, параграф 2 или продължава обработването на данни за целите на директния маркетинг, след като субектът на данни е възразил, в нарушение на член 19, параграф 2а;
- д) не определя или определя в недостатъчна степен съответните отговорности на съвместните администратори съгласно член 24;

е) не поддържа или поддържа в недостатъчна степен документацията съгласно член 28 и член 31, параграф 4.

ж) (...)

3. Надзорният орган (...) може да наложи глоба, която не надвишава 1 000 000 EUR, а за предприятия — 2 % от общия годишен оборот в световен мащаб за предходната финансова година, на администратор или обработващ лични данни, който умишлено или по небрежност:

а) обработва лични данни без (...) правно основание за обработването или не спазва условията за съгласие съгласно членове 6, 7, 8 и 9;

б) (...);

в) (...);

г) не спазва условията по отношение на (...) автоматизираното вземане на индивидуални решения, включително профилирането съгласно член 20;

га) не (...) прилага подходящи мерки или не е в състояние да докаже, че е спазил членове 22 (...) и 30;

гб) не определя представител в нарушение на член 25;

гв) обработва или възлага обработването на лични данни в нарушение на (...) член 26;

гг) не предупреждава или не уведомява за нарушение на сигурността на личните данни или не уведомява [своевременно или] изчерпателно за нарушението надзорния орган или субекта на данни в нарушение на членове 31 и 32;

гд) не извършва оценка на въздействието по отношение на защитата на данни в нарушение на член 33 или обработва лични данни без предварителна консултация с надзорния орган в нарушение на член 34, параграф 2;

д) (...);

е) злоупотребява с печат или маркировка за защита на данни по смисъла на член 39 или не изпълнява условията и процедурите, предвидени в членове 38а и 39а;

ж) извършва или възлага извършването на трансфер на данни до получател в трета държава или международна организация в нарушение на членове 41—44;

з) не спазва разпореждане, временно или окончателно ограничение върху обработването или наложено преустановяване на потоците от данни от надзорния орган съгласно член 53, параграф 1б, или не предоставя достъп в нарушение на член 53, параграф 1.

и) (...)

й) (...)

За. Ако администратор или обработващ лични данни умишлено или по небрежност нарушава няколко от разпоредбите на настоящия регламент, изброени в параграфи 1, 2 или 3, общият размер на глобата не може да надвишава размера, определен за най-тежкото нарушение.

4. (...)

Член 79б

Санкции

1. За нарушения (...) на настоящия регламент, по-специално за нарушения, които не подлежат на административни глоби съгласно (...) член 79а, държавите членки предвиждат правила относно санкциите, приложими при такива нарушения, и предприемат всички необходими мерки, за да се гарантира прилагането им (...). Тези санкции са ефективни, пропорционални и възпиращи.

2. (...)

3. *Всяка държава членка уведомява Комисията за тези разпоредби в своето право, които приема съгласно параграф 1, най-късно до датата, посочена в член 91, параграф 2, и я уведомява незабавно за всяко последващо, свързано с тях изменение.*

ГЛАВА IX

РАЗПОРЕДБИ, СВЪРЗАНИ С ОСОБЕНИ СИТУАЦИИ НА ОБРАБОТВАНЕ НА ДАННИ

Член 80

Обработване на лични данни и свобода на изразяване и информация

1. В правната уредба на държавите членки (...) се съгласува правото на защита на личните данни в съответствие с настоящия регламент с правото на свобода на изразяване и информация, включително обработването на лични данни за журналистически цели и за целите на академичното, художественото или литературното изразяване.
2. За обработването на лични данни, извършвано за журналистически цели и за целите на академичното, художественото или литературното изразяване, държавите членки предвиждат изключения или дерогации от разпоредбите в глава II (принципи), глава III (права на субекта на данни), глава IV (администратор на лични данни и обработващо лице), глава V (предаване на лични данни на трети държави и международни организации), глава VI (независими надзорни органи), глава VII (сътрудничество и съгласуваност), ако те са необходими за съгласуване на правото на защита на личните данни със свободата на изразяване и информация (...).

Член 80a

Обработване на лични данни 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 на държава 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 80aa

**Обработване на лични данни и повторна употреба на информацията в
обществения сектор**

Личните данни от информацията в обществения сектор, 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 на държава членка, на което се подчинява публичният орган или структура, за да се съгласува повторната употреба на такива официални документи и на информация в обществения сектор с правото на защита на личните данни в съответствие с настоящия регламент.

Член 80б

Обработване на национален идентификационен номер

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

Член 81

Обработване на лични данни за здравни цели

(...)

Член 81a

Обработване на генетични данни

(...)

Член 82

Обработване в контекста на трудово 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 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 правоотношение. (...)
2. Всяка държава членка уведомява Комисията за тези разпоредби в своето право, които приема съгласно параграф 1, най-късно до датата, посочена в член 91, параграф 2, и я уведомява незабавно за всяко последващо, свързано с тях изменение.
3. Държавите членки могат да определят със закон условията, при които личните данни в контекста на трудово правоотношение могат да бъдат обработвани въз основа на съгласието на наетото лице.

Член 82a

Обработване за целите на социалната закрила

(...)

Дерогации във връзка с обработването на лични данни за целите на архивирането от обществен интерес и за научни, статистически и исторически цели

1. Когато личните данни се обработват за научни, статистически или исторически цели, правото на Съюза или на държавите членки може, при осигуряване на подходящи гаранции за правата и свободите на субекта на данни, да предвиди дерогации от член 14а, параграфи 1 и 2, както и от членове 15, 16, 17, 17а, 17б, 18 и 19, доколкото тези дерогации са необходими за изпълнението на конкретните цели.
- 1а. Когато личните данни се обработват за целите на архивирането в интерес на обществото, правото на Съюза или на държавите членки може, при осигуряване на подходящи гаранции за правата и свободите на субекта на данни, да предвиди дерогации от член 14а, параграфи 1 и 2, както и от членове 15, 16, 17, 17а, 17б, 18, 19, 23, 32, 33 и 53, параграф 1б, букви г) и д), доколкото тези дерогации са необходими за изпълнението на посочените цели.
- 1б. Ако видът на обработването по параграфи 1 и 1а служи същевременно за друга цел, предвидените дерогации се прилагат единствено за обработване, извършвано за посочените в тези параграфи цели.
2. Подходящите гаранции, посочени в параграфи 1 и 1а, се определят от правото на Съюза или на държавата членка по начин, който гарантира, че технологичните и/или организационните мерки за защита в съответствие с настоящия регламент се прилагат за личните данни (...), за да се сведе до минимум обработването на лични данни съгласно принципите на пропорционалност и на необходимост, като например псевдонимизирането на данните, освен когато тези мерки възпрепятстват постигането на целта на обработването и тази цел не може да бъде изпълнена по друг начин с разумни средства.
3. (...)

Член 84

Задължения за опазване на тайна

1. (...) Държавите членки могат да приемат специални разпоредби, за да установят (...) правомощията на надзорните органи съгласно член 53, параграф 1, букви га) и гб) по отношение на администраторите на лични данни или обработващите лица, които по силата на правото на Съюза или на държавата членка или на разпоредби, установени от компетентните национални органи, са обвързани със задължение за опазване на професионална тайна, с други равностойни задължения за опазване на тайна или с кодекс за професионална етика, върху който упражняват надзор и чието спазване налагат професионалните организации, когато това е необходимо и пропорционално за съгласуване на правото на защита на личните данни със задължението за опазване на тайна. Тези разпоредби се прилагат само по отношение на лични данни, които администраторът на лични данни или обработващото лице е получило в хода на дейност, подлежаща на това задължение за опазване на тайна.
2. Всяка държава членка уведомява Комисията за разпоредбите, приети съгласно параграф 1, най-късно до датата, посочена в член 91, параграф 2, и я уведомява незабавно за всяко последващо, свързано с тях изменение.

Член 85

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 на лични данни, тези съществуващи правила могат да продължат да се прилагат, при условие че са приведени в съответствие с разпоредбите на настоящия регламент.
2. Църквите и религиозните сдружения, които прилагат цялостни правила в съответствие с параграф 1, 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 X

ДЕЛЕГИРАНИ АКТОВЕ И АКТОВЕ ЗА ИЗПЪЛНЕНИЕ

(1) Член 86

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 39а, параграф 7 (...), се предоставя на Комисията за неопределен срок, считано от датата на влизане в сила на настоящия регламент.
3. Делегирането на правомощия, посочено в (...) член 39а, параграф 7 (...), 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 на решението 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 Съвета.

5. Делегиран акт, приет съгласно (...) член 39а, параграф 7 (...), влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца от нотифицирането на акта на Европейския парламент и на 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 два месеца по инициатива на Европейския парламент или на Съвета.

Член 87

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 XI

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 88

Отмяна на Директива 95/46/ЕО

1. Директива 95/46/ЕО се отменя.
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 89

Връзка и изменение на Директива 2002/58/ЕО

1. Настоящият регламент не налага допълнителни задължения на физическите или юридическите лица по отношение на обработването на лични данни във връзка с доставката 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, установена в Директива 2002/58/ЕО.
- 2 (...)

Член 89а

Връзка с по-рано сключени споразумения

Международните споразумения за предаване на лични данни на трети държави или международни организации, които са сключени от държавите членки преди влизането в сила на настоящия регламент и са в съответствие с Директива 95/46/ЕО, остават в сила, докато не бъдат изменени, заменени или отменени.

Член 90

Оценка

1. Комисията редовно представя на Европейския парламент и на Съвета доклади относно оценката и прегледа на настоящия регламент.
2. В контекста на тези оценки Комисията разглежда по-специално прилагането и функционирането на разпоредбите на глава VII относно сътрудничеството и съгласуваността.
3. Първият доклад се представя не по-късно от четири години след влизането в сила на настоящия регламент. Следващите доклади се представят на всеки четири години след това. Докладите се оповестяват публично.
4. При необходимост Комисията представя подходящи предложения за изменение на настоящия регламент и за привеждане в съответствие на други правни инструменти, като отчита по-специално развитието на информационните технологии и с оглед на напредъка на информационното общество.

Член 91

Влизане в сила и прилагане

1. Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.
2. Прилага се от *[две години след датата, посочена в параграф 1]*.

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

Съставено в Брюксел

За Европейския парламент

За Съвета

Председател

Председател
