Проект

З А К О Н
ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ НА ЗАКОНА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

(обн. ДВ. бр.1 от 2002 г., изм. ДВ. бр.70 от 2004 г., изм. ДВ. бр.93 от 2004 г., изм. ДВ. бр.43 от 2005 г., изм. ДВ. бр.103 от 2005 г., изм. ДВ. бр.30 от 2006 г., изм. ДВ. бр.91 от 2006 г., изм. ДВ. бр.57 от 2007 г., изм. ДВ. бр.42 от 2009 г., изм. ДВ. бр.94 от 2010 г., изм. ДВ. бр.97 от 2010 г., изм. ДВ. бр.39 от 2011 г., изм. ДВ. бр.81 от 2011 г., изм. ДВ. бр.105 от 2011 г., изм. и доп. ДВ. бр.15 от 2013 г., доп. ДВ. бр.81 от 2016 г., изм. ДВ. бр.7 от 19 януари 2018 г.)

§ 1. Член 1 се изменя така:

„Чл. 1. (1) Този закон въвежда мерките за изпълнение и прилагане на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), (ОВ, L119/1 от 4 май 2016 г.), наричан по-нататък „Регламент (ЕС) 2016/679“.

(2) С този закон се определят и особените правила във връзка със защитата на физическите лица по отношение на обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване.

(3) Целта на закона е да осигури защита на физическите лица във връзка с обработването на лични данни в съответствие с Регламент (ЕС) 2016/679, както и във връзка с обработването на лични данни от компетентните органи за целите на предотвратяване, разследване, разкриване или наказателно преследване на престъпления или изпълнение на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване.

(4) Този закон урежда и:

1. създаването на Комисията за защита на личните данни като единствен надзорен орган, отговорен за защита основните права и свободи на физическите лица във връзка с обработването и улесняване свободното движение на личните данни в рамките на Европейския съюз;

2. средствата за правна защита;

3. акредитирането и сертифицирането в областта на защитата на личните данни;

4. особени ситуации за обработване на лични данни;

5. административно-наказателната отговорност и принудителните административни мерки при нарушения на този закон.

(5) Доколкото в специален закон не е предвидено друго, този закон не се прилага за обработването на лични данни за целите на отбраната на страната и националната сигурност.

(6) При прилагането на този закон следва да се отчитат специалните потребности на микропредприятията, малките и средни предприятия при условията на Регламент (ЕС) 2016/679.

(7) Този закон не се прилага за обработването на лични данни на починали лица, с изключение на чл. 25к.

(8) При обработване на лични данни по чл. 2 от Регламент 2016/679 държавите, които са страни по Споразумението за Европейско икономическо пространство и Швейцария са равнопоставени на държавите членки на Европейския съюз. Всички други държави са трети държави.

(9) При обработване на лични данни по чл. 42 държавите, участващи в изпълнението, прилагането и развитието на достиженията на правото от Шенген, са равнопоставени на държавите членки на Европейския съюз. Всички други държави са трети държави.“

§ 2. Членове 2-5 се отменят.

§ 3. В чл. 6 се правят следните изменения и допълнения:

1. Алинея 1 се изменя така:

„(1) Комисията за защита на личните данни, наричана по-нататък „комисията“, е постоянно действащ независим надзорен орган, който осъществява защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент (ЕС) 2016/679 и този закон.“

2. Добавя се нова ал. 4 със следното съдържание:

„(4) При осъществяване на своята дейност, комисията се подпомага от администрация.“

§4. В чл. 7 се правят следните изменения:

1. Алинея 4 се изменя както следва:

„(4) Председателят на комисията получава основно месечно възнаграждение в размер 90 на сто от основното месечно възнаграждение на председателя на Народното събрание, а членовете на комисията – 80 на сто от основното месечно възнаграждение на председателя на комисията.“

2. Алинея 5 се отменя.

3. В ал. 6 датата „31 януари“ се заменя с „31 март“.

§5. В чл. 9 се правят следните изменения и допълнения:

1. Алинея 1 се отменя.

2. Алинея 2 се изменя както следва:

„(2) Комисията урежда в правилник своята дейност, дейността на администрацията си и производствата, които се развиват пред нея, и го обнародва в „Държавен вестник“.“

§6. В чл. 10 се правят следните изменения и допълнения:

1. Създава се нова ал. 1:

„(1) Комисията изпълнява на територията на Република България задачите по чл. 57 от Регламент (ЕС) 2016/679.“

2. Досегашната ал. 1 става ал. 2 и се изменя така:

„(2) Комисията изпълнява и следните задачи:

1. анализира и осъществява цялостен надзор, и осигурява спазването на Регламент (ЕС) 2016/679, на този закон и на нормативните актове в областта на защитата на лични данни;

9. издава подзаконови нормативни актове в областта на защита на личните данни;

10. осигурява прилагането на решенията на Европейската комисия в областта на защитата на личните данни и изпълнението на задължителните решения на Европейския комитет по защита на данните

11. участва в международното сътрудничество между органите по защита на личните данни и международните организации по въпросите в областта на защита на личните данни;

12. участва в преговорите и сключването на двустранни или многостранни споразумения по въпроси от своята компетентност;

13. организира, координира и провежда обучение в областта на защитата на личните данни;

14. издава общи и нормативни административни актове, свързани с правомощията ѝ, в случаите, предвидени в закон;

15. приема критерии за акредитация на сертифициращи органи;

16. издава насоки, препоръки и най-добри практики в случаите, когато такива не са издадени от Европейския комитет по защита на данните.“

3. Досегашната ал. 2 се отменя.

4. Създава се нова ал. 3:

„(3) Комисията изпълнява и останалите задачи, възложени ѝ с Регламент (ЕС) 2016/679 в качеството ѝ на надзорен орган.“

5. Досегашната ал. 3 става ал. 4.

6. Досегашната ал. 4 става ал. 5 и се изменя така:

„(5) Комисията одобрява проекти на кодекси за поведение по сектори и области на дейност и при установяване на несъответствие с нормативната уредба дава задължителни предписания.“

§7. Създават се чл. 10а, чл. 10б, чл. 10в и чл. 10 г:

„Чл. 10а (1) Комисията упражнява на територията на Република България правомощията по чл. 58 от Регламент (ЕС) 2016/679.

(2) Комисията има и следните правомощия:

1. сезира съда за нарушаване на Регламент (ЕС) 2016/679;

2. издава задължителни предписания, дава указания и препоръки във връзка със защитата на личните данни;

3. прилага принудителни административни мерки.

Чл. 10б. На комисията могат да бъдат възлагани други задачи и правомощия само със закон.

Чл. 10в. Член 10, ал.2, т. 1 не се прилага при обработване на лични данни от органите на съдебната власт, когато действат при изпълнение на правораздавателните си функции.

Чл. 10г. (1) Комисията участва в механизма на съгласуваност и осъществява сътрудничество с водещия и/или засегнатите надзорни органи, в т.ч. като обменя информация, предоставя или иска взаимопомощ и/или участва в съвместни операции.

(2) Формите на участие в механизма за съгласуваност, предоставянето и искането на взаимопомощ и участието в съвместни операции, както и процедурите, по които те се реализират, се уреждат с правилника за дейността на комисията и нейната администрация.“

§8. В чл. 11, т. 4 думите „чл. 43, ал. 2“ се заменят с „чл. 87, ал. 2“.

§9. В чл. 12 се правят следните изменения и допълнения

1. В ал. 1 думите „предварителни, текущи и последващи проверки за спазване на този закон“ се заменят с „предварителни консултации, проверки (одити) и съвместни операции за спазване на Регламент 2016/679 и на този закон.“

2. Алинея 2 се изменя така:

„(2) Предварителни консултации се извършват когато:

1. оценката на въздействието върху защитата на данните покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска.

2. се обработват данни в случаи, когато, съгласно решение на комисията, се застрашават правата и законните интереси на физическите лица.

3. се обработват данни в изпълнение на задача в обществен интерес, включително обработване във връзка със социалната закрила и общественото здраве. В този случай комисията може да разреши обработването, като даде предварително разрешение за това и преди изтичане на срока по ал. 3.“

3. Алинея 3 се изменя така:

„(3) При предварителните консултации по ал. 2, комисията дава становище на администратора или обработващия лични данни в срок до осем седмици след

получаване на искането. Предвид сложността на планираното обработване, този срок може да бъде удължен с още шест седмици, за което администраторът или обработващият следва да бъдат уведомени.“

4. Алинея 4 се изменя така:

„(4) Проверки (одити) се извършват по инициатива на комисията, по молба на заинтересовани лица и след подаден сигнал.“

5. В ал. 8 се създава изречение второ: „В този случай алтернативно може да се наложи принудителна административна мярка по реда на Административнопроцесуалния кодекс.“

6. Създава се ал. 10:

„(10) Съвместни операции с надзорни органи на държави членки се извършват по целесъобразност за съвместни разследвания и съвместни мерки за изпълнение и в тях участват освен лицата по ал. 1, и членове или упълномощени представители от администрацията на надзорен орган на държавата членка.“

§10. Създава се чл. 12а:

„Чл. 12а. (1) Наличието на търговска, производствена или друга защитена от закона тайна не може да бъде основание за отказ от съдействие от страна на администратора при осъществяване задачите и правомощията на комисията.

(2) Когато информацията съдържа данни, представляващи класифицирана информация, се прилага редът за достъп по Закона за защита на класифицираната информация.“

§11. Член 14 се изменя така:

„Чл. 14. (1) Комисията извършва акредитацията на сертифициращи органи в съответствие с Регламент (ЕС) 2016/679 въз основа на критерии, определени от нея или от Европейския комитет по защита на данните, или от водещия надзорен орган на друга държава членка – при трансгранично обработване на лични данни.

(2) Акредитацията се издава за срок от пет години и може да бъде подновена от комисията при същите условия.

(3) Комисията анулира акредитацията на сертифициращ орган, ако не са били спазени или вече не се спазват условията за акредитация, или ако предприетите от сертифициращия орган действия нарушават настоящия закон или Регламент (ЕС) 2016/679.

(4) Критериите, механизмите и процедурите за сертифициране, печати и маркировки се уреждат в наредба, издадена от комисията. Наредбата се обнародва в „Държавен вестник““.

§12. Създава се нов чл. 15:

„Чл. 15. (1) Комисията може да организира и провежда обучение на лицата, определени за заемане на длъжността „длъжностно лице по защита на данните“ или на лица, желаещи да бъдат обучени за заемане на тази длъжност.

(2) Обучението по ал.1, когато е по искане на администраторите, обработващите или обучаващите се, е за тяхна сметка и се заплаща по тарифа, определена от министъра на финансите.“

§13. Създава се нов чл. 16:

„Чл. 16. (1) Комисията води следните публични регистри:

1. Регистър на длъжностните лица по защита на данните;

2. Регистър на акредитираните по чл. 14 сертифициращи органи;

3. Регистър на кодекси за поведение.

(2) Комисията води вътрешен регистър на нарушения на Регламент (ЕС) 2016/679 и този закон, както и на предприетите мерки в съответствие с упражняването на корективните правомощия по чл. 58, пар. 2 от Регламент (ЕС) 2016/679, който не е публичен.

(3) Редът за водене на регистрите по ал. 1 и 2, съдържанието и достъпа до тях се уреждат в правилника за дейността на комисията и на нейната администрация.“

§14. Глава трета и глава четвърта се отменят.

§15. Създава се глава четвърта „а“ с чл. 25а-25к със следното съдържание:

„Глава четвърта „а“

Допълнителни правила и особени ситуации на обработване на лични данни

Чл. 25а. Когато лични данни са предоставени от субекта на данни на администратор или обработващ, без правно основание по чл. 6, пар. 1 или в противоречие с принципите по чл. 5 от Регламент (ЕС) 2016/679, администраторът/обработващият ги връща незабавно или ги изтрива, или унищожава в срок от един месец от узнаването.

Чл. 25б. (1) Извън случаите по чл. 37, пар. 1 от Регламент (ЕС) 2016/679 администраторът или обработващият лични данни задължително определя длъжностно лице по защита на данните, когато обработва лични данни на над 10 000 физически лица.

(2) Администраторът съобщава имената и данните за контакт на длъжностното лице по защита на данните на комисията, както и последващи промени в тях и публикува координатите за връзка с него. Формата и съдържанието на уведомлението и реда за подаването му до комисията се определят с правилника за дейността на комисията и нейната администрация.

(3) Длъжностното лице по защита на данните може да изпълнява задачите си по трудово или служебно правоотношение, вкл. по вътрешно съвместителство, или въз основа на договор за услуги. Администраторът и обработващият не могат да съвместяват и функциите на длъжностно лице по защита на данните.

Чл. 25в. В случаите на пряко предлагане на услуги на информационното общество, ако субектът на данните е лице под 14 години, обработването е

законосъобразно, само ако съгласието е дадено от упражняващия родителски права родител или от настойника на субекта на данните.

Чл. 25г. (1) Публичен достъп до ЕГН/ЛНЧ се предоставя, само ако закон изисква това. В тези случаи законът определя реда и условията за достъп с цел недопускане неговата общодостъпност.

(2) Администраторите, предоставящи услуги по електронен път, предприемат подходящи технически и организационни мерки, които не позволяват единният граждански номер да е единственият идентификатор за предоставяне на съответната услуга.

Чл. 25д. (1) Когато при упражняването на правото на свобода на изразяване и информация, включително за журналистически цели и за целите на академичното, художественото или литературното изразяване, се обработват лични данни на физически лица, администраторът на лични данни прави преценка за законосъобразността на обработването във всеки конкретен случай. Решението на администратора не може непропорционално да ограничава свободата на изразяване и информация.

(2) При преценката по ал. 1 администраторът взема предвид съвкупността от следните критерии:

1. естеството на личните данни;

2. влиянието, което разкриването на личните данни или тяхното обществено оповестяване би оказало върху неприкосновеността на личния живот на субекта на данни и неговото добро име;

3. обстоятелствата, при които личните данни са станали известни на администратора;

4. характера и естеството на изявлението, чрез което се упражняват правата по ал.1;

5. значението на разкриването на лични данни или общественото им оповестяване за изясняването на въпрос от обществен интерес;

6. отчитане дали субектът на данни е лице, което заема длъжност по чл. 2, ал. 1 от Закона за публичност на имуществото на лицата, заемащи висши държавни и други длъжности или е лице, което поради естеството на своята дейност или ролята му в обществения живот е с по-занижена защита на личната си неприкосновеност или чиито действия имат влияние върху обществото;

7. отчитане дали субектът на данни с действията си е допринесъл за разкриване на свои лични данни и/или информация за личния си и семеен живот;

8. целта, съдържанието, формата и последиците от изявлението, чрез което се упражняват правата по ал. 1;

9. съответствието на изявлението, чрез което се упражняват правата по ал. 1 с основните права на гражданите;

10. други обстоятелства, относими към конкретния случай.

Чл. 25е. Работодателят по смисъла на §1, т.1 от Допълнителните разпоредби на Кодекса на труда (работодателят)/органът по назначаването (органът по назначаването) по смисъла на Закона за държавния служител може да копира документ за самоличност, свидетелство за управление на моторно превозно средство, документ за пребиваване на работник/държавен служител, само ако закон предвижда това.

Чл. 25ж. (1) Работодателят/органът по назначаването приема правила и процедури при:

1. използване на система за докладване на нарушения;

2. ограничения при използване на вътрешнофирмени ресурси;

3. въвеждане на системи за контрол на достъпа, работното време и трудовата дисциплина.

(2) Правилата и процедурите съдържат информация относно обхвата, задълженията и методите за прилагането им на практика. Те отчитат предмета на дейност на работодателя/органа по назначаването и свързаното с него естество на работата и не могат да ограничават правата на физическите лица по Регламент (ЕС) 2016/679 и този закон.

(3) Правилата и процедурите по ал. 1 се довеждат до знанието на работниците и служителите.

Чл. 25з. (1) Работодателят/органът по назначаването определя срок за съхранение на лични данни на участници в процедури по подбор на персонала, който не може да бъде по-дълъг от три години.

(2) Когато в процедура по подбор работодателят/органът по назначаването е изискал да се представят оригинали или нотариално заверени копия на документи, удостоверяващи физическа и психическа годност на кандидата, необходимата квалификационна степен и стаж за заеманата длъжност, субектът на данните, който не е одобрен за назначаване, може да поиска в 30-дневен срок от окончателното приключване на процедурата по подбор да получи обратно представените документи. Работодателят/органът по назначаването връща документите, по начина, по който са подадени.

Чл. 25и. Работодател/орган по назначаване може да обработва лични данни на работник/служител, които не е поискал или които не се изискват от нормативен акт, ако субектът на данни е дал своето изрично съгласие и няма забрана за това в нормативен акт.

Чл. 25й. (1) Администраторът/обработващият приема специални правила при обработване на лични данни чрез систематично мащабно наблюдение на публично достъпни зони, вкл. чрез видеонаблюдение. В правилата се уреждат правните основания и целите за изграждане на система за наблюдение, местоположение, обхват на наблюдение и средства за наблюдение, срок на съхранение на записите с информация и изтриването им, правото на преглед от страна на наблюдаваните лица,

информиране на обществеността за осъществяваното наблюдение, както и ограничения при предоставяне на достъп до информацията на трети лица.

(2) Комисията определя минималните изисквания към администраторите при изпълнение на задължението им по ал. 1, които публикува на интернет страницата си.

Чл. 25к. (1) При обработване на лични данни на починали лица, администраторът предприема подходящи мерки за недопускане неблагоприятно засягане на правата и свободите на други лица и/или на обществен интерес. В тези случаи администраторът може да съхранява данните, само при наличие на правно основание за това.

(2) Администраторът осигурява, при поискване, достъп до лични данни на починало лице, вкл. предоставя копие от тях, на наследниците му или на други лица с правен интерес.“

§16. Глава пета и глава шеста се отменят.

§17. Наименованието на глава седма се изменя така:

„Упражняване на правата на субектите на данни. средства за правна защита, отговорност за причинени вреди“

§18. Създават се чл. 37а и 37б:

„Чл. 37а. (1) Правата по чл. 15 – 22 от Регламент (ЕС) 2016/679 се осъществяват с писмено заявление до администратора на лични данни.

(2) Заявление може да бъде отправено и по електронен път по реда на Закона за електронния документ и електронния подпис.

(3) Заявлението по ал. 1 се отправя лично от субекта на данни или от изрично упълномощено от него лице, освен ако специален закон не предвижда друго.

Чл. 37б. (1) Заявлението по чл. 37а съдържа:

1. име, адрес и други данни за идентифициране на съответното физическо лице;

2. описание на искането;

3. предпочитана форма за комуникация и действия по чл. 15-22 от Регламент (ЕС) 2016/679;

4. подпис, дата на подаване на заявлението и адрес за кореспонденция.

(2) При подаване на заявление от упълномощено лице към заявлението се прилага и съответното пълномощно.“

§19. В чл. 38 се правят следните изменения и допълнения:

1. Алинея 1 се изменя така:

„(1) При нарушаване на правата му по Регламент (ЕС) 2016/679 и този закон всеки субект на лични данни има право да сезира комисията в едногодишен срок от узнаване на нарушението, но не по-късно от пет години от извършването му.“

2. Създава се нова ал. 2:

„(2) Комисията информира жалбоподателя за напредъка в разглеждането на жалбата или за резултата от нея в тримесечен срок от сезирането й.“

3. Досегашната ал. 2 става ал. 3 и се изменя така:

„(3) Комисията се произнася с решение, като може да даде задължителни предписания, да определи срок за отстраняване на нарушението или да наложи административно наказание.“

4. Алинея 4 се изменя така:

„(4) Комисията изпраща копие от решението си и на субекта на данните.“

5. Алинея 5 се изменя така:

„(5) В случаите по ал. 1, когато се обработват лични данни за целите, посочени в чл. 42, решението на комисията съдържа само констатация относно законосъобразността на обработването."

6. В ал. 6 цифрата „2“ се заменя с „3“.

§20. Член 39 се изменя и допълва така:

1. Алинея 1 се изменя така:

„(1) При нарушаване на правата му по Регламент (ЕС) 2016/679 и този закон всеки субект на данни може да обжалва действия и актове на администратора и обработващия по съдебен ред пред съответния административен съд или пред Върховния административен съд по общите правила за подсъдност.“

2. В ал. 2 думите „физическото лице“ се заменят със „субектът на данни“.

3. Алинея 3 се отменя.

4. Алинея 4 се изменя така:

„(4) Субектът на данни не може да сезира съда, ако има висящо производство пред комисията за същото нарушение или нейно решение относно същото нарушение е обжалвано и няма влязло в сила решение на съда. По искане на субекта на данни комисията удостоверява липсата на висящо производство пред нея по същия спор.“

§21. Създава се чл. 39а:

„В случаите, когато Европейският комитет по защита на данните е приел решение със задължителен характер и валидността на същото е оспорена, се прилагат чл. 263, съответно член 267 от Договора за функционирането на Европейския съюз.“

§22. Създава се нова глава осма с чл. 42-83 със следното съдържание:

„Глава осма

Особени правила за защита на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване

Раздел I
ОБЩИ РАЗПОРЕДБИ

Чл. 42. (1) Правилата на настоящата глава се прилагат при обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване.

(2) В случаите, в които компетентните органи обработват лични данни за цели, различни от посочените в ал. 1, се прилагат Регламент (ЕС) 2016/679 и съответните разпоредби от този закон, които въвеждат мерки за неговото прилагане, освен ако обработването на лични данни е за целите на отбраната на страната и защита на националната сигурност, когато се прилага чл. 1, ал. 5.

Чл. 43. Правилата на настоящата глава се прилагат за обработването на лични данни изцяло или частично с автоматични средства, както и за обработването с други средства на лични данни, които са част от регистър с лични данни или са предназначени да съставляват част от такъв регистър.

Чл. 44. Обменът на лични данни между компетентните органи на държавите членки на Европейския съюз, когато той е в съответствие с правото на Съюза или законодателството на Република България, не се ограничава, нито забранява по причини, свързани със защитата на физическите лица във връзка обработването на лични данни.

Чл. 45. (1) При обработване на лични данни за целите по чл. 42 личните данни трябва да:

1. се обработват законосъобразно и добросъвестно;

2. се събират за конкретни, изрично указани и легитимни цели и да не се обработват по начин, който е несъвместим с тези цели;

3. са подходящи, относими и да не надхвърлят необходимото във връзка с целите, за които данните се обработват;

4. са точни и, при необходимост, поддържани в актуален вид; трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват;

5. се съхраняват във вид, който позволява идентифицирането на субектите на данните за период не по-дълъг от необходимия за целите, за които те се обработват;

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

(2) Обработването от същия или друг администратор за която и да е от целите, посочени в чл. 42, различна от целта, за която личните данни са събрани, се разрешава, при условие че:

а) администраторът е оправомощен да обработва такива лични данни за такава цел в съответствие с правото на Европейския съюз или законодателството на Република България; и

б) обработването е необходимо и пропорционално на тази различна цел в съответствие с правото на Европейския съюз или законодателството на Република България.

(3) Обработването от същия или друг администратор може да включва архивиране в обществен интерес, научно, статистическо или историческо използване на данните за целите по чл. 42, при прилагането на подходящи гаранции за правата и свободите на субектите на данните.

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

Чл. 46 (1) Сроковете за изтриването на лични данни или за периодична проверка на необходимостта от съхранението им се определят от администратора.

(2) Извършването на периодична проверка по ал. 1 се документира, а решението за продължаване на съхранението на данните се мотивира.

Чл. 47. Администраторът, когато е приложимо и доколкото е възможно, прави ясно разграничение между личните данни на различни категории субекти на данни, например:

1. лица, за които има сериозни основания да се счита, че са извършили или ще извършат престъпление;

2. лица, осъдени за престъпление;

3. лица, пострадали от престъпление или лица, по отношение на които определени факти дават основание да се счита, че може да са пострадали от престъпление; и

4. други трети лица по отношение на престъпление, например лица, които биха могли да бъдат призовани да свидетелстват при разследване на престъпления или при последващи наказателни производства, лица, които могат да предоставят информация за престъпления или свързани лица, или съучастници на някое от лицата, посочени в т. 1 и т. 2.

Чл. 48 (1) Администраторът, доколкото е възможно, прави разграничение между лични данни, основани на факти, и лични данни, основани на лични оценки.

(2) Администраторът предприема всички разумни стъпки, за да гарантира, че лични данни, които са неточни, непълни или вече не са актуални, не се предават или не се предоставят. За тази цел всеки компетентен орган, доколкото това е практически възможно, проверява качеството на личните данни преди тяхното предаване или предоставяне. Доколкото е възможно, при всяко предаване на лични данни се добавя необходимата информация, позволяваща на получаващия компетентен орган да оцени степента на точност, пълнота и надеждност на личните данни и до каква степен те са актуални.

(3) Ако се окаже, че са предадени неверни лични данни или че личните данни са предадени незаконосъобразно, получателят се уведомява незабавно. В такъв случай личните данни се коригират или заличават или обработването им се ограничава в съответствие с чл. 56.

Чл. 49 (1) Обработването на лични данни е законосъобразно, когато е необходимо за изпълнението на задача, осъществявана от компетентен орган за целите, определени в чл. 42, и се основава на правото на Европейския съюз или законодателството на Република България.

(2) Когато обработването на лични данни за целите по чл. 42 е в изпълнение на нормативен акт, в него се определят общите и конкретните цели на обработването, както и личните данни, които се обработват.

Чл. 50. (1) Личните данни, събирани от компетентните органи за целите, посочени в чл. 42, не се обработват за други цели, различни от посочените в чл. 42, освен когато това обработване е разрешено от правото на Европейския съюз или законодателството на Република България. Когато личните данни се обработват за такива други цели се прилагат Регламент (ЕС) 2016/679 и съответните разпоредби от този закон, които въвеждат мерки за неговото прилагане, освен ако обработването на лични данни е за целите на отбраната на страната и защита на националната сигурност, когато се прилага чл. 1, ал. 5.

(2) Когато съгласно законодателството на Република България компетентните органи са натоварени с изпълнението на задачи, различни от тези за изпълнението на целите, посочени в чл. 42, за обработването за такива цели се прилагат Регламент (ЕС) 2016/679 и съответните разпоредби от този закон, които въвеждат мерки за неговото прилагане, включително за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, освен ако обработването на лични данни е за целите на отбраната на страната и защита на националната сигурност, когато се прилага чл. 1, ал. 5.

(3) Когато правото на Европейския съюз или законодателството на Република България, приложимо за предаващия компетентен орган, предвижда специфични условия за обработването, предаващият компетентен орган уведомява получателя на тези лични данни, за тези условия и за изискването за съобразяване с тях.

(4) Предаването на лични данни на получатели в други държави членки или към агенции, служби и органи на Европейския съюз, създадени съгласно дял V, глави 4 и 5 от Договора за функционирането на Европейския съюз, се извършва при същите условия, които се прилагат при подобно предаване в рамките на Република България.

Чл. 51 (1) Обработването на лични данни от компетентни органи, разкриващо расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравето или сексуалния живот и сексуалната ориентация на лицето, е разрешено, когато това е абсолютно необходимо, съществуват подходящи гаранции за правата и свободите на субекта на данни и е разрешено съгласно правото на Европейския съюз или законодателството на Република България.

(2) По изключение, ако обработването не е разрешено съгласно правото на Европейския съюз или законодателството на Република България, данните по ал. 1 могат да бъдат обработвани за защита на жизненоважни интереси на субекта на

данните или на друго физическо лице или ако обработването касае данни, които очевидно са направени обществено достояние от субекта на данните.

(3) Във всички случаи на обработване на данни по ал. 1 компетентните органи прилагат подходящи мерки и гаранции за недопускане на дискриминация на физическите лица.

Чл. 52. (1) Вземането на решение, основано единствено на автоматизирано обработване, включително профилиране, което поражда неблагоприятни правни последици за субекта на данните или съществено го засяга, е забранено освен ако това не е разрешено от правото на Европейския съюз или законодателството на Република България и са осигурени подходящи гаранции за правата и свободите на субекта на данните, най-малко правото да получи човешка намеса при вземането на съответното решение от страна на администратора.

(2) Решенията по алинея 1 не могат да се основават на специалните категории лични данни, посочени в чл. 51, освен ако не са въведени подходящи мерки за защита на правата и свободите и легитимните интереси на субекта на данните.

(3) В случаите по ал. 1 и ал. 2 администраторът задължително извършва оценка на въздействието по чл. 64.

(4) Забранява се профилирането, което води до дискриминация на физически лица въз основа на специалните категории лични данни, посочени в чл. 51.

Раздел II
ПРАВА НА СУБЕКТА НА ДАННИ

53 (1) Администраторът предприема разумни мерки за предоставяне на субекта на данни на информация по чл. 54 и за осигуряване на комуникацията във връзка с членове 52, 55—58 и 68 относно обработването в сбита, разбираема и леснодостъпна форма, като използва ясен и прост език. Информацията се предоставя по всякакъв подходящ начин, включително по електронен път. Като общо правило администраторът предоставя информацията в същата форма като тази на искането.

(2) Администраторът улеснява упражняването на правата на субекта на данни, посочени в членове 52 и 55—58.

(3) Администраторът информира писмено и без излишно забавяне субекта на данните за действията, предприети във връзка с неговото искане.

(4) Информацията, предоставена по чл. 54, и комуникацията или действията, предприети съгласно членове 52, 55—58 и 68, се предоставят безплатно. Когато исканията от даден субект на данни са очевидно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може:

1. да начисли такса в разумен размер, като взема предвид административните разходи за предоставяне на информация или на комуникация или за предприемане на действия по искането; или

2. да откаже да предприеме действия по искането.

Администраторът носи тежестта на доказване на очевидно неоснователния или прекомерен характер на искането.

(5) Когато администраторът има основателни опасения във връзка със самоличността на физическото лице, което подава искане по членове 55 или 56, той

може да поиска да се предостави допълнителна информация, необходима за потвърждаване на самоличността на субекта на данните.

Чл. 54. (1) Администраторът предоставя на субектите на данни най-малко следната информация:

1. данните, които идентифицират администратора и координатите за връзка с него;

2. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

3. целите на обработването, за които са предназначени личните данни;

4. правото да бъде подадена жалба до комисията и нейните координати за връзка;

5. съществуването на право да се изиска от администратора достъп до, коригиране или изтриване на лични данни и ограничаване на обработването на лични данни, свързано със субекта на данните.

(2) Освен информацията, посочена в ал. 1, администраторът предоставя на субекта на данните, в конкретни случаи и с цел да му се даде възможност да упражни правата си, следната допълнителна информация:

1. правното основание за обработването;

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

3. когато е приложимо, категориите получатели на личните данни, включително в трети държави или международни организации;

4. ако е необходимо, и друга допълнителна информация, по-специално в случаите, когато личните данни са събрани без знанието на субекта на данните.

(3) Администраторът може да забави, да ограничи или да не предостави информация на субекта на данните съгласно ал. 2, като се отчитат основните права и легитимните интереси на засегнатото физическо лице, за да:

1. не се допусне възпрепятстването на служебни или законово регламентирани проверки, разследвания или процедури;

2. не се допусне неблагоприятно засягане на предотвратяването, разкриването, разследването или наказателното преследване на престъпления или изпълнението на наказания;

3. се защити обществения ред и сигурност;

4. се защити националната сигурност;

5. се защитят правата и свободите на други лица.

(4) След отпадане на съответното обстоятелство по ал. 3 администраторът предоставя без забавяне исканата информация.

Чл. 55. (1) Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, които го засягат, и ако случаят е такъв, да получи достъп до тях, както и информация за:

1. целите и правното основание за обработването;

2. обработваните категории лични данни;

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

4. когато е възможно, предвидения срок, за който ще се съхраняват личните данни, или ако това не е възможно, критериите за определяне на този срок;

5. съществуването на право да се изиска от администратора коригиране или изтриване на лични данни, или ограничаване на обработването на лични данни, свързано със субекта на данните;

6. правото да се подаде жалба до комисията и нейните координати за връзка;

7. съобщаването на личните данни, които са в процес на обработване, и на всякаква налична информация за техния произход.

(2) Администраторът предоставя информацията по ал. 1 в срок до 60 дни от получаването на искането.

(3) Правото на достъп на субекта на данните по ал. 1 може да се ограничи изцяло или частично, като се отчитат основните права и легитимните интереси на засегнатото физическо лице, в случаите по чл. 54, ал. 3 В тези случаи съответно се прилага чл. 54, ал. 4.

(4) В случаите по ал. 3 администраторът информира писмено в срок до 60 дни от получаването на искането субекта на данните за всеки отказ за достъп или ограничаване на достъпа и за причините за отказа или ограничаването. Тази информация може да не бъде предоставена, когато нейното предоставяне би възпрепятствало постигането на някоя от целите, посочени в чл. 54, ал.3. Администраторът информира субекта на данните за възможността за подаване на жалба до комисията или за търсене на защита по съдебен ред.

(5) Администраторът документира фактическите или правните основания, на които се основава решението. Тази информация се предоставя на комисията.

Чл. 56. (1) Субектът на данните има право да поиска администраторът да коригира без излишно забавяне неточните лични данни, свързани с него. Като се има предвид целта на обработването, субектът на данните има право да поиска непълните лични данни да бъдат попълнени, включително чрез предоставяне на допълнително заявление (декларация).

(2) Администраторът е длъжен да изтрие личните данни без излишно забавяне и субектът на данните има право да поиска администраторът да изтрие без излишно забавяне личните данни, които го засягат, когато обработването нарушава разпоредбите на чл. 45, чл. 49 или чл. 51, или когато личните данни трябва да бъдат изтрити с цел спазване на правно задължение за администратора.

(3) Администраторът коригира или допълва данните по реда на ал. 1, съответно изтрива данните по реда на ал. 2 в срок до 60 дни от получаването на искането.

(4) Администраторът ограничава обработването на личните данни, без да ги изтрие, когато:

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

2. личните данни трябва да бъдат запазени за доказателствени цели.

(5) Администраторът информира субекта на данните преди да премахне ограничаването на обработването, когато то е наложено на основание ал. 4, т. 1 от този член.

(6) Администраторът информира писмено субекта на данните за всеки отказ за коригиране или изтриване на лични данни, или ограничаване на обработването и за причините за отказа в срок до 60 дни от получаването на искането. Задължението за

предоставяне на такава информация може да бъде ограничено изцяло или частично, като се отчитат основните права и легитимните интереси на засегнатото физическо лице, в случаите по чл. 54, ал. 3. В тези случаи съответно се прилага чл. 54, ал. 4.

(7) Администраторът информира субекта на данните за възможността за подаване на жалба до комисията и за търсене на защита по съдебен ред.

(8) Администраторът съобщава на компетентния орган, от който произхождат неточните лични данни, за тяхното коригиране.

(9) Когато лични данни са коригирани или изтрити, или обработването им е ограничено съгласно ал. 1, 2 и 4 на този член, администраторът уведомява получателите им, които носят отговорност за тяхното съответно коригиране, изтриване или ограничаване на обработването.

Чл. 57. (1) В случаите по чл. 54, ал. 3, чл. 55, ал. 4 и чл. 56, ал. 6 субектът на данните може да упражни правата си и чрез комисията (непряко упражняване на права).

(2) Администраторът информира субекта на данните за възможността да упражни правата си чрез комисията съгласно ал. 1.

(3) В случаите по ал. 1, комисията информира субекта на данните най-малко за това, че е извършила всички необходими проверки или справки, както и за неговото право да потърси защита по съдебен ред.

Чл. 58. Упражняването на правата по чл. 54, чл. 55 и чл. 56, когато личните данни се съдържат в съдебно решение, документ или материали по дело, изготвени в рамките на наказателно производство, не засяга и не може да противоречи на разпоредбите на Наказателно-процесуалния кодекс.

Раздел III
АДМИНИСТРАТОР НА ЛИЧНИ ДАННИ И ОБРАБОТВАЩ ЛИЧНИ ДАННИ

Чл. 59. (1) Администраторът на лични данни, като отчита естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, прилага подходящи технически и организационни мерки, за да гарантира и да е в състояние да докаже, че обработването се извършва в съответствие с този закон. Тези мерки се преразглеждат и актуализират при необходимост.

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

(3) С цел ефективното прилагане на принципите за защита на личните данни и интегрирането на необходимите гаранции в процеса на обработване, администраторът, като отчита достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и породените от обработването рискове за правата и свободите на физическите лица, прилага съответни мерки по смисъла на ал. 1, като например псевдонимизация, както към момента на определянето на средствата за обработването на данни, така и към момента на самото обработване („защита на личните данни на етапа на проектирането“).

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

Чл. 60. (1) Когато двама или повече администратори съвместно определят целите и средствата на обработването, те са съвместни администратори.

(2) Съвместните администратори определят по прозрачен начин съответните си отговорности за съобразяване с правилата на настоящата глава, по-специално що се отнася до упражняването на правата на субекта на данни, и съответните си задължения за предоставяне на информацията по реда на чл. 54, посредством договореност помежду си, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на Европейския съюз или законодателството на Република България. В договореността се определя точката за контакт за субектите на данни. Съвместните администратори могат да посочат кой от тях действа като единна точка за контакт, така че субектите на данните да упражняват правата си.

(3) Независимо от условията на договореността, посочена в ал. 1, субектът на данни може да упражнява своите права, уредени в настоящата глава, по отношение на всеки и срещу всеки от администраторите.

Чл. 61. (1) Администратор може да възложи обработване на лични данни от негово име само на обработващи лични данни, които предоставят достатъчни гаранции, че ще прилагат подходящи технически и организационни мерки, по такъв начин че обработването да отговаря на изискванията на настоящата глава и да се гарантира защитата на правата на субекта на данни.

(2) Обработващият лични данни не може да добавя друг обработващ лични данни без предварителното конкретно или общо писмено разрешение на администратора. В случай на общо писмено разрешение, обработващият лични данни информира администратора за всякакви планирани промени за добавяне или замяна на други обработващи лични данни, като по този начин дава възможност на администратора да възрази срещу тези промени.

(3) Обработването от страна на обработващия лични данни се урежда с договор или друг правен акт съгласно правото на Европейския съюз или законодателството на Република България, който обвързва обработващия лични данни с администратора и регламентира предмета и срока на обработването, естеството и целта на обработването, вида лични данни и категориите субекти на данни, задълженията и правата на администратора. Посоченият договор или друг правен акт предвижда по-специално, че обработващият лични данни:

1. действа единствено по указания на администратора;
2. гарантира, че лицата, оправомощени да обработват личните данни, са поели ангажимент за поверителност или са задължени по закон да спазват поверителност;
3. подпомага администратора с всички подходящи средства, за да се гарантира спазването на разпоредбите относно правата на субекта на данни;

4. по избор на администратора заличава или връща на администратора всички лични данни след приключване на предоставянето на услуги по обработване на данни и заличава съществуващите копия, освен ако правото на Европейския съюз или законодателството на Република България не изисква съхранение на личните данни;

5. предоставя на администратора цялата информация, необходима за доказване на спазването на настоящия член;

6. спазва условията по алинеи 2 и 3 за включване на друг обработващ лични данни.

(4) Договорът или другият правен акт, посочен в ал. 3, се изготвя в писмена или електронна форма.

(5) Ако обработващ лични данни определи в нарушение на правилата на настоящата глава целите и средствата на обработването, обработващият личните данни се счита за администратор по отношение на това обработване.

(6) Обработващият лични данни и всяко лице, действащо под ръководството на администратора или на обработващия лични данни, което има достъп до личните данни, обработва тези данни само по указание на администратора, освен ако обработването се изисква от правото на Европейския съюз или законодателството на Република България.

Чл. 62. (1) Администраторите поддържат регистър с всички категории дейности по обработване под тяхна отговорност. Този регистър съдържа следната информация:

1. наименованието и координатите за връзка на администратора, и когато е приложимо, на съвместните администратори и на длъжностното лице по защитата на данните;

2. целите на обработването;

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

4. описание на категориите субекти на данни и на категориите лични данни;

5. когато е приложимо, използването на профилиране;

6. когато е приложимо, категориите предаване на лични данни на трета държава или международна организация;

7. посочване на правното основание за операцията по обработване, включително предаването на данни, за която са предназначени личните данни;

8. когато е възможно, предвидените срокове за изтриване на различните категории лични данни;

9. когато е възможно, общо описание на техническите и организационните мерки за сигурност по чл. 66.

(2) Всеки обработващ лични данни поддържа регистър с всички категории дейности по обработване, извършени от името на администратор, в който се съдържат:

1. наименованието и координатите за връзка на обработващия или обработващите лични данни, на всеки администратор, от чието име действа обработващият лични данни и на длъжностното лице за защита на данните, когато е приложимо;

2. категориите обработване, извършени от името на всеки администратор;

3. когато е приложимо, предаването на лични данни на трета държава или на международна организация, когато има изрични указания от администратора за това, включително идентификацията на тази трета държава или международна организация;

4. когато е възможно, общо описание на техническите и организационните мерки за сигурност по чл. 66.

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

(4) При поискване администраторът и обработващият лични данни предоставят достъп до регистрите на комисията.

Чл. 63. (1) В системите за автоматизирано обработване се водят записи (логове) най-малко за следните операции по обработване: събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване.

(2) Записите за извършена справка или разкриване трябва да дават възможност за установяване на основанието, датата и часа на такива операции и доколкото е възможно — идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни.

(3) Записите се използват единствено за проверяване на законосъобразността на обработването, за самоконтрол, за гарантиране на цялостността и сигурността на личните данни и при наказателни производства.

(4) Администраторът определя подходящи срокове за съхранение, вкл. архивиране на записите.

(5) При поискване администраторът и обработващият лични данни предоставят тези записи на комисията.

Чл. 64. (1) Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни.

(2) Оценката по ал. 1 съдържа най-малко общо описание на предвидените операции по обработване, оценка на рисковете за правата и свободите на субектите на данните, мерките, предвидени за справяне с тези рискове, гаранции, мерки за сигурност и механизми за гарантиране на защитата на личните данни и за доказване на съответствие с правилата на настоящата глава, като се вземат предвид правата и легитимните интереси на субектите на данните и другите засегнати лица.

Чл. 65. (1) Администраторът или обработващият лични данни се консултира с надзорния орган преди обработването на лични данни, което ще бъде част от нов регистър с лични данни, който предстои да бъде създаден, когато:

1. оценката на въздействието върху защитата на данните съгласно чл. 64 покаже, че обработването ще породи висок риск, ако администраторът не предприеме мерки за ограничаване на риска; или

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

(2) При изготвяне на проекти на закони и на подзаконови нормативни актове, съдържащи мерки, които се отнасят до обработването, се провеждат консултации с комисията.

(3) Комисията приема наредба, с която определя списък на операциите по обработване, за които е задължителна предварителна консултация съгласно ал. 1.

(4) Администраторът предоставя на комисията оценката на въздействието върху защитата на данните, предвидена в чл. 64, и при поискване — всякаква друга информация, която ще й позволи да извърши оценка на съответствието на обработването, и по-специално на рисковете за защитата на личните данни на субекта на данните и на съответните гаранции.

(5) Когато комисията е на мнение, че планираното обработване, посочено в ал. 1 от настоящия член, би нарушило разпоредбите на настоящата глава, по-специално когато администраторът не е идентифицирал или ограничил риска в достатъчна степен, тя предоставя в рамките на период до шест седмици след получаване на искането за консултация писмено становище на администратора и, когато това е приложимо, на обработващия лични данни. Този срок може да бъде удължен с още един месец, в зависимост от сложността на планираното обработване. В срок от един месец от получаване на искането за консултация комисията уведомява администратора и, когато е приложимо, обработващия лични данни за всяко такова удължаване, включително и за причините за забавянето.

(6) Предоставянето на писмено становище по ал. 5 не засяга възможността на комисията да приложи по отношение на администратора или обработващия лични данни и правомощията си по член 80.

Чл. 66. (1) Администраторът и обработващият лични данни, като отчитат достиженията на техническия прогрес, разходите за прилагане и естеството, обхвата, контекста и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, прилагат подходящи технически и организационни мерки за осигуряване на съобразено с този риск ниво на сигурност, по-специално по отношение на обработването на лични данни по чл. 51.

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

1. контрол върху достъпа до оборудване - да се откаже достъп на неоправомощени лица до оборудването, използвано за обработване;

2. контрол върху носителите на данни - да се предотврати четенето, копирането, изменянето или отстраняването на носители на данни от неоправомощени лица;

3. контрол върху съхраняването - да се предотврати въвеждането на лични данни от неоправомощени лица, както и извършването на проверки, изменянето или заличаването на съхранявани лични данни от неоправомощени лица;

4. контрол върху потребителите - да се предотврати използването на автоматизирани системи за обработване от неоправомощени лица чрез използване на оборудване за предаване на данни;

5. контрол върху достъпа до данни - да се гарантира, че лицата, на които е разрешено да използват автоматизирана система за обработване, имат достъп само до личните данни, които са обхванати от тяхното разрешение за достъп;

6. контрол върху комуникацията - да се гарантира възможността за проверка и установяване на кои органи са били или могат да бъдат предадени или имат достъп до лични данни чрез оборудване за предаване на данни;

7. контрол върху въвеждането на данни - да се гарантира възможността за последваща проверка и установяване на това какви лични данни са били въведени в автоматизираните системи за обработване, както и кога и от кого са били въведени тези лични данни;

8. контрол върху пренасянето - да се предотврати четенето, копирането, изменянето или заличаването на лични данни от неоправомощени лица при предаването на лични данни или при пренасянето на носители на данни;

9. възстановяване - да се гарантира възможността за възстановяване на инсталираните системи в случай на отказ на функциите на системите;

10. надеждност - да се гарантира изпълнението на функциите на системата и докладването за появили се във функциите дефекти;

11. цялостност - да се гарантира недопускане на увреждане на съхраняваните лични данни вследствие на неправилно функциониране на системата.

Чл. 67. (1) В случай на нарушение на сигурността на личните данни администраторът, без излишно забавяне, но — не по-късно от 72 часа след като е разбрал за него, уведомява комисията за нарушението на сигурността на личните данни, освен ако няма вероятност нарушението на сигурността на личните данни да доведе до риск за правата и свободите на физическите лица. Когато уведомлението до комисията не е подадено в срок от 72 часа, то се придружава от причините за забавянето.

(2) Обработващият лични данни уведомява администратора без излишно забавяне, след като е установил нарушение на сигурността на лични данни.

(3) В уведомлението, посочено в ал 1, се съдържа най-малко следното:

1. описание на естеството на нарушението на сигурността на личните данни, включително, когато това е възможно, категориите и приблизителния брой на засегнатите субекти на данни и категориите и приблизителния брой на засегнатите записи на лични данни;

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

3. описание на евентуалните последици от нарушението на сигурността на личните данни;

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

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

(5) Администраторът документира всяко нарушение на сигурността на личните данни, посочено в ал. 1, като включва фактите, свързани с нарушението на сигурността на личните данни, последиците от него и предприетите действия за справяне с него. Тази документация дава възможност на комисията да провери дали е спазен настоящият член.

(6) Когато нарушението на сигурността на личните данни засяга лични данни, които са били изпратени от или на администратор от друга държава членка, посочената

в ал. 3 информация се съобщава на администратора на въпросната държава членка без излишно забавяне.

Чл. 68. (1) Когато има вероятност нарушението на сигурността на личните данни да доведе до висок риск за правата и свободите на физическите лица, 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 ал. 1 от настоящия член, на ясен и прост език се описва естеството на нарушението на сигурността на личните данни и се съдържат най-малко информацията и мерките, посочени в чл. 67, ал. 3, точки 2, 3 и 4.

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

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

2. 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 ал. 1;

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

(4) Ако администраторът все още не е съобщил на субекта на данните за нарушението на сигурността на личните данни, комисията може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от администратора да направи съобщението или да реши, че е изпълнено някое от условията по ал. 3.

(5) Съобщението до субекта на данните, посочено в ал. 1 от настоящия член, може да бъде забавено, ограничено или пропуснато, при условията и на основанията, посочени в чл. 54, ал. 3.

Чл. 69. (1) Администраторът определя длъжностно лице по защита на данните въз основа на неговите професионални качества и по-специално въз основа на експертните му познания по законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите, посочени в член 70.

(2) Едно длъжностно лице по защита на данните може да бъде назначено съвместно за няколко компетентни органа, като се отчитат организационната им структура и мащаб.

(3) Администраторът публикува координатите за връзка на длъжностното лице по защита на данните и да ги съобщава на комисията по реда на чл.25б, ал.2.

(4) Алинея 1 не се прилага по отношение на органите на съдебната власт, когато действат в изпълнение на правораздавателните си функции.

Чл. 70. (1) Администраторът гарантира, че длъжностното лице по защита на данните участва по подходящ начин и своевременно по всички въпроси, свързани със защитата на личните данни.

(2) Администраторът възлага на длъжностното лице по защита на данните най-малко следните задачи:

1. да информира и съветва администратора и служителите, които извършват обработването, за техните задължения по силата на този закон и на други нормативни изисквания за защита на личните данни;

2. да наблюдава спазването на този закон и на други нормативни изисквания за защита на личните данни и на политиките на администратора 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;

3. при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването ѝ;

4. да си сътрудничи с Комисията за защита на личните данни;

5. да действа като точка за контакт с комисията за защита на личните данни по всички въпроси, свързани с обработването на лични данни.

(3) Администраторът подпомага длъжностното лице по защита на данните при изпълнението задачите му по ал. 2, като осигурява по-специално необходимите ресурси, достъп до личните данни и операциите по обработването и поддържането на неговите експертни знания.

Чл. 71. Компетентните органи определят подходящи процедури за пряко и поверително докладване от техните служители на съответното административно звено за контрол в структурата на администратора или на комисията на нарушения на тази глава.

Раздел IV.

ПРЕДАВАНЕ НА ЛИЧНИ ДАННИ НА ТРЕТИ ДЪРЖАВИ ИЛИ МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Чл. 72. (1) Компетентен орган може да предава лични данни, които са в процес на обработване или са предназначени за обработване след предаването им на трета държава или на международна организация, включително за последващо предаване на друга трета държава или международна организация, при условие че предаването е в съответствие с разпоредбите на този закон и е изпълнено всяко едно от следните условия:

1. предаването е необходимо за целите , посочени в чл. 42.

2. личните данни се предават на администратор в трета държава или на международна организация, която е орган, компетентен за целите, посочени в чл. 42;

3. когато се предават или се предоставят лични данни, получени от друга държава членка, тази държава членка е дала своето предварително разрешение за предаването в съответствие с националното си право;

4. Европейската комисия е приела решение, че съответната трета държава, територия, или един или повече конкретни сектори в тази трета държава, или съответната международна организация осигуряват адекватно ниво на защита или при отсъствието на такова решение са предвидени или съществуват подходящи гаранции съгласно член 74, а при отсъствието както на решение за адекватно ниво на защита, така и на подходящи гаранции, се прилага дерогация съгласно член 75, и

5. при последващо предаване на лични данни на друга трета държава или международна организация, компетентният орган, извършил първоначалното предаване, или друг компетентен орган разрешава последващото предаване на данни, след като надлежно е взел предвид всички значими фактори, включително тежестта на престъплението, целта на първоначалното предаване на личните данни, нивото на защита на личните данни в третата държава или международната организация, към която се извършва последващото предаване на лични данни.

(2) Предаването на данни без предварителното разрешение на друга държава членка в съответствие с ал.1, т. 3 се разрешава само ако предаването на личните данни е необходимо за предотвратяването на непосредствена и сериозна заплаха за обществения ред и сигурност на държава членка или на трета държава, или за основните интереси на държава членка и предварителното разрешение не може да бъде получено своевременно. В тези случаи, незабавно се уведомява органът на държавата членка, предоставила личните данни, в чиято компетентност е да даде предварителното разрешение по ал.1, т.3.

Чл. 73. (1) Лични данни може да се предават на трета държава или международна организация, ако е налице решение на Европейската комисия, че съответната държава, територия, или един или повече конкретни сектори в тази държава, или съответната международна организация осигуряват адекватно ниво на защита. За такова предаване не се изисква специално разрешение.

(2) Ако Европейската комисия отмени, измени или спре действието на свое решение по ал. 1, това не засяга възможността предаването на лични данни на съответната трета държава, на територията или на един или повече конкретни сектори в тази трета държава, или на съответната международна организация да се осъществи при условията на членове 74 и 75.

Чл. 74. (1) При липса на решение на Европейската комисия относно адекватното ниво на защита на личните данни по чл. 73, ал. 1, предаване на лични данни на трета държава или международна организация може да се осъществи, когато:

1. в законодателството на тази държава или в устава на международната организация, или във влязъл в сила международен договор, по който Република България е страна, или в друг правно обвързващ акт са предвидени подходящи гаранции във връзка със защитата на личните данни; или

2. администраторът е извършил оценка на всички обстоятелства около предаването на лични данни и е стигнал до заключението, че по отношение на защитата на личните данни съществуват подходящи гаранции.

(2) Администраторът документира предаванията на основание на алинея 1, т. 2, включително датата и момента на предаване, информацията относно получаващия компетентен орган, обосновка на предаването и предадените лични данни.

(3) Администраторът информира комисията за категориите предавания по ал. 1, т. 2. и при поискване й предоставя достъп до документацията по ал. 2.

Чл. 75.(1) При липса на решение на Европейската комисия относно адекватното ниво на защита на личните данни съгласно член 73, ал. 1 или на подходящи гаранции съгласно член 74, предаване на лични данни на трета държава или международна организация може да се извърши само ако предаването е необходимо:

1. за да бъдат защитени жизненоважни интереси на субекта на данни или на друго лице;

2. за да бъдат защитени легитимни интереси на субекта на данни, когато законодателството на Република България предвижда това;

3. за предотвратяването на непосредствена и сериозна заплаха за обществения ред и сигурност на държава членка на Европейския съюз или на трета държава;

4. в отделни случаи за целите, посочени в чл. 42; или

5. в отделен случай за установяването, упражняването или защитата на правни претенции, свързани с целите, посочени в чл. 42.

(2) Лични данни не могат да бъдат предавани, ако предаващият компетентен орган реши, че основните права и свободи на въпросния субект на данните надделяват над обществения интерес от предаването, посочено в точки 4 и 5 на ал. 1.

(3) При предаването на данни на основание на алинея 1, то се документира и документацията се предоставя на комисията при поискване, включително датата и момента на предаване, информация относно получаващия компетентен орган, обосновка на предаването и предадените лични данни.

Чл. 76. (1) Чрез дерогация от член 72, ал.1, т. 2 и без да се засяга международен договор по ал. 2 от настоящия член, компетентен орган в отделни и специфични случаи може да предава лични данни пряко на получатели, установени в трети държави, само ако са спазени останалите разпоредби на тази глава и е изпълнено всяко едно от следните условия:

1. предаването е строго необходимо за изпълнението на задача на предаващия компетентен орган, произтичаща от правото на Европейския съюз или от законодателството на Република България, за целите, посочени в чл. 42;

2. предаващият компетентен орган реши, че никои основни права и свободи на въпросния субект на данни не надделяват над обществения интерес, който налага предаването в конкретния случай;

3. предаващият компетентен орган счита, че предаването на орган, който е компетентен в третата държава по отношение на целите, посочени в чл. 42, е неефективно или неподходящо, по-специално тъй като предаването не може да се осъществи навреме;

4. органът на третата държава, който е компетентен за целите, посочени в чл. 42, е уведомен без излишно забавяне, освен ако това е неефективно или неподходящо;

5. предаващият компетентен орган уведомява получателя за конкретната цел или цели, единствено за които последният обработва личните данни, при условие че такова обработване е необходимо.

(2) Международен договор по ал. 1 е всяко двустранно или многостранно международно споразумение, което е в сила между държави членки и трети държави в

областта на съдебното сътрудничество по наказателноправни въпроси и полицейското сътрудничество.

(3) Компетентният орган, предаващ данните, документира всяко предаване на основание ал. 1 и уведомява комисията.

Чл. 77. (1) По отношение на трети държави и международни организации комисията предприема подходящи мерки за:

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

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

3. включване на съответните заинтересовани страни в обсъждания и дейности, насочени към допълнително задълбочаване на международното сътрудничество за прилагането на законодателството за защита на личните данни;

4. насърчаване на обмена и документирането на законодателство и практики в областта на защитата на личните данни, включително във връзка със спорове за компетентност с трети държави.

Раздел V

НАДЗОР ЗА СПАЗВАНЕ НА ПРАВИЛАТА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ. СРЕДСТВА ЗА ПРАВНА ЗАЩИТА.

Чл. 78. (1) Надзорът за спазване на правилата за защита на личните данни по тази глава се упражнява от комисията.

(2) По отношение на независимостта, общите условия за председателя и членовете на надзорния орган и правилата за създаването му се прилагат съответно чл. 52 – 54 от Регламент 2016/679.

Чл. 79. (1) При упражняване на надзора по тази глава, освен задачите по чл. 10, ал.2, т. 1, 9-14 и т.16, комисията изпълнява и следните задачи:

1. наблюдава и гарантира прилагането на разпоредбите на тази глава и мерките за изпълнението им;

2. насърчава обществената информираност и разбиране на рисковете, правилата, гаранциите и правата, свързани с обработване;

3. дава становища относно проекти на закони и други нормативни актове, както и административни мерки, свързани със защитата на правата и свободите на физическите лица по отношение на обработването;

4. повишава осведомеността на администраторите и обработващите лични данни за техните задължения;

5. предоставя информация на всеки субект на данни във връзка с упражняването на правата му при поискване и, ако е уместно, си сътрудничи за тази цел с надзорните органи в други държави членки;

6. разглежда, разследва и се произнася по жалби, подадени от субект на данни по реда и условията на чл. 38 от този закон;

7. проверява законосъобразността на обработването в случаите по чл. 57 и информира субекта на данните за резултата от проверката в тримесечен срок от сезирането й или за причините, поради които проверката не е била извършена;

8. осъществява сътрудничество с други надзорни органи, включително чрез обмен на информация, и им предоставя взаимна помощ с оглед осигуряване на съгласуваното прилагане и привеждане в изпълнение на правилата за защита на личните данни;

9. извършва проучвания в областта на защитата на личните данни, включително въз основа на информация, получена от друг надзорен или публичен орган;

10. наблюдава съответното развитие, по-специално в областта на развитието на информационните и комуникационни технологии, дотолкова доколкото то има въздействие върху защитата на личните данни;

11. дава становища по операциите за обработване на данни, посочени в чл. 65.

12. участва в дейностите на Европейския комитет по защита на данните.

(2) Изпълнението на задачите по ал. 1 е безплатно за субекта на данни и за длъжностното лице по защита на данните.

(3) Администраторът и обработващият лични данни сътрудничат при поискване с комисията при изпълнението на задачите ѝ.

Чл. 80. (1) При упражняване на надзора по тази глава, освен правомощията по чл. 10а, ал.2, т. 2 и 3, комисията упражнява и следните правомощия:

1. правомощия за разследване:

а) да получава от администратора или обработващия лични данни достъп до всички лични данни, които се обработват;

а) да получава от администратора или обработващия цялата информация, необходима за изпълнението на задачите на комисията.

2. корективни правомощия:

а) да отправя предупреждения до администратора или обработващия лични данни, когато има вероятност планираните операции по обработване на данни да нарушат разпоредбите на тази глава;

б) да разпорежда на администратора или на обработващия лични данни да приведат операциите по обработване на данни в съответствие с разпоредбите на тази глава, вкл. да разпорежда коригирането, изтриването на лични данни или ограничаването на обработването съгласно чл. 56;

в) да налага временно или окончателно ограничаване, включително забрана, на обработването.

3. консултативни правомощия:

а) да дава становища на администратора в съответствие с процедурата по предварителна консултация по чл. 65;

б) да дава становища по собствена инициатива или при поискване по проекти на закони и други нормативни актове, както и на административни мерки, свързани със защитата на личните данни на физическите лица;

в) да дава становища по собствена инициатива или при поискване по всякакви други въпроси, свързани със защитата на личните данни.

(2) Комисията може да сезира съда за нарушения на разпоредбите от тази глава.

Чл. 81. (1) Комисията си сътрудничи с надзорните органи на другите държави членки, включително чрез обмен на информация и отправяне и изпълнение на искания за извършване на консултации, проверки и разследвания. Исканията за помощ следва да съдържат цялата необходима информация, включително целта и основанията на искането. Обменената информация се използва единствено за целите, за които е поискана.

(2) Комисията предприема всички необходими и подходящи мерки, за да се отговори на искането на друг надзорен орган без излишно забавяне и не по-късно от един месец след получаване на искането.

(3) Комисията може да откаже искане за помощ, ако:

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

б) удовлетворяването на искането би нарушило законодателството на Република България или правото на Европейския съюз.

(4) Комисията информира искащия надзорен орган за резултатите или, в зависимост от случая, за напредъка на предприетите мерки в отговор на искането. Комисията мотивира отказа си по ал. 3.

(5) Формите на сътрудничество и взаимопомощ между комисията и надзорните органи на други държави членки и процедурите, по които те се реализират, се уреждат с правилника за дейността на комисията и нейната администрация.

Чл. 82. (1) При нарушаване на правата му по тази глава, субектът на данните разполага със средствата за правна защита и може да търси отговорност за причинените му вреди по реда на глава седма от този закон.

(2) В случаите по чл. 38, ал. 1, комисията предоставя допълнителна помощ по искане на субекта на данните.

(3) Неизпълнението от комисията на задължението по чл. 38, ал. 2 може да се оспори по реда на чл. 257 от Административнопроцесуалния кодекс.“

Чл. 83. Субектът на данни има право да възложи на юридическо лице с нестопанска цел, осъществяващо дейност в обществена полза и развиващо дейност в областта на защитата 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 чл. 38, 39, 82, ал. 2 и ал. 3.

§23. Досегашната глава осма става глава девета с чл. 84-90 и се изменя и допълва така:

„Глава девета

ПРИНУДИТЕЛНИ АДМИНИСТРАТИВНИ МЕРКИ.
АДМИНИСТРАТИВНОНАКАЗАТЕЛНИ РАЗПОРЕДБИ

Чл. 84. (1) За предотвратяване и преустановяване на нарушенията, свързани с изпълнението на задълженията по Регламент (ЕС) 2016/679 и по този закон, както и за отстраняване на негативните последици от тях комисията може да налага временно или окончателно ограничаване, в т.ч. забрана, на обработването на данни, както и да разпорежда на администратора да съобщава на субекта на данните за нарушения на сигурността на личните данни.

(2) Мерките по ал. 1 се издават по ред и условия, определени в Правилника за дейността на комисията.

(3) Решението на комисията по ал. 2 подлежи на обжалване по реда на Административнопроцесуалния кодекс в 14-дневен срок от получаването му. Решението подлежи на незабавно изпълнение, освен ако съдът не постанови друго.

Чл. 85. (1) За нарушения, посочени в чл. 83, параграф 5 и параграф 6 от Регламент (ЕС) 2016/679 и за нарушения на чл. 45, ал. 1, чл. 49, ал. 1, чл. 52, чл. 54-56, чл. 80, ал. 1, т. 1, б. „а“, т. 2, б. „б“ и б. „в“ от глава осма администраторът или обработващият лични данни се наказва с глоба или имуществена санкция от 10 000 до левовата равностойност на 20 000 000 евро.

(2) За нарушения по чл. 83, параграф 4 от Регламент (ЕС) 2016/679, чл. 59, чл. 62, чл. 64-69 от глава осма административното наказание глоба или имуществена санкция е в размер от 5000 до левовата равностойност на 10 000 000 евро.

(3) За други нарушения по този закон администраторите и/или обработващите лични данни се наказват с глоба или с имуществена санкция от 1000 до 5000 лв.

Чл. 86. Когато нарушенията по Регламент (ЕС) 2016/679 и този закон са извършени повторно, се налага глоба или имуществена санкция в двоен размер на първоначално наложената, но не повече от максимално предвидените размери в чл. 83 от Регламент (ЕС) 2016/679.

Чл. 87. (1) Актовете за установяване на административните нарушения се съставят от член на комисията или от упълномощени от комисията длъжностни лица.

(2) Наказателните постановления се издават от председателя на комисията.

(3) Имуществените санкции и глобите по влезли в сила наказателни постановления се събират по реда на Данъчно-осигурителния процесуален кодекс.

(4) Установяването на нарушенията, издаването, обжалването и изпълнението на наказателните постановления се извършват по реда на Закона за административните нарушения и наказания.

(5) Събраните суми от наложени имуществени санкции и глоби постъпват по бюджета на комисията.

Чл. 88. За неизпълнение на задължително предписание на комисията се налага глоба или имуществена санкция в размер от 2 000 лв. до 200 000 лв.

Чл. 89. (1) В случаите на чл. 10а, при упражняване на корективните си правомощия по чл. 58, пар. 2, б. „а“-„з“ и б. „й“ от Регламент (ЕС) 2016/679, комисията

налага административни наказания и/или принудителни административни мерки по Регламент (ЕС) 2016/679.

(2) Административните наказания и/или принудителните административни мерки по Регламент (ЕС) 2016/679 по ал. 1 се налагат с решение на комисията по ред и условия, определени в Правилника за дейността на комисията.

Чл. 90. За други нарушения по Регламент (ЕС) 2016/679 се издава задължително предписание или се налага административно наказание глоба или имуществена санкция в размер от 2 000 лв. до 200 000 лв. по реда и условия, определени в чл. 84 и чл. 87.“

§24. В Допълнителните разпоредби §1 се изменя така:

„§1. Извън определенията по чл. 4 от Регламент (ЕС) 2016/679, по смисъла на този закон:

1. „Общодостъпност“ е разкриване на лични данни или по друг начин осигуряване на достъп до тях от неограничен кръг от лица, без да са предприети мерки за осигуряване на отчетност;
2. „Маркировка“ е механизъм за самооценка, чрез който се демонстрира съответствие с Регламент (ЕС) 2016/679, по критерии, определени от комисията;
3. „Мащабно“ е системното наблюдение и/или обработване на лични данни на неограничен кръг субекти на лични данни.
4. „Риск“ е функция от вероятността дадена заплаха да се превърне в потенциална уязвимост и резултатното въздействие от неблагоприятното събитие върху организацията.
5. „Уязвимост“ са слабости в процедурите за сигурност на системата, в процесите на разработване и изпълнение, във вътрешните контроли и т.н., които могат да бъдат инцидентно или умишлено експлоатирани и това да доведе до нарушение на политиката на сигурност на системата.
6. Микропредприятия, малки и средни предприятия са предприятията по чл. 3 от Закона за малките и средни предприятия.“

§25. В Допълнителните разпоредби се създава нов § 1а:

„§ 1а. По смисъла на глава осма от този закон:

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

2. „обработване“ означава всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други

средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друга форма на осигуряване на достъп до данните, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

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

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

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

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

7. „компетентен орган“ означава:

а) всеки публичен орган, който е компетентен за предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване; или

б) всякакъв друг орган или образувание, който по силата на закон разполага с публична власт и публични правомощия за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществената сигурност и тяхното предотвратяване;

8) „администратор“ означава компетентният орган, който сам или съвместно с други органи определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на Европейския съюз или правото на Република България, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Европейския съюз или в националното законодателство;

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

10) „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. Публичните органи, които могат да получават лични данни в

рамките на конкретно разследване в съответствие с правото на Република България, не се считат за получатели; обработването на тези данни от тези публични органи отговаря на приложимите правила за защита на данните съгласно целите на обработването;

11) „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;

12) „генетични данни“ означава лични данни, свързани с наследени или придобити генетични белези на дадено физическо лице, които дават уникална информация относно физиологията или здравето на това физическо лице и които са получени по-специално чрез анализ на биологична проба от въпросното физическо лице;

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

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

15) „надзорен орган“ означава независим публичен орган от държава членка на Европейския съюз, отговорен за наблюдението на прилагането на правилата за защита на личните данни, с които са въведени разпоредбите на Директива 2016/680 в съответното национално законодателство, с цел да се защитят основните права и свободи на физическите лица във връзка с обработването на лични данни и да се улесни свободното им движение в рамките на ЕС. За Република България надзорен орган е Комисията за защита на личните данни от този закон.

16) „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.“

§26. В Допълнителните разпоредби досегашният § 1а става § 1б и се изменя така:

„§1б. Този закон въвежда мерките за изпълнение на Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ, L119/1 от 4 май 2016 г.) и изискванията на Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и

относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ, L 119/89 от 4 май 2016 г.).“

§27 В Преходните и заключителнителните разпоредби се създава §6:

„§6. Системите за автоматизирано обработване, използвани от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания, включително предпазването от заплахи за обществения ред и сигурност и тяхното предотвратяване, създадени преди 6 май 2016 г., се привеждат в съответствие с член 63, ал. 1 и ал. 2 до 6 май 2023 г.“

Преходни и Заключителни разпоредби

§ 28. Образуваните преди 25 май 2018 г. производства за нарушения на този закон се приключват по досегашния ред.

§ 29. В Закона за Министерството на вътрешните работи (обн. ДВ. бр.53 от 2014г., изм. ДВ. бр.98 от 2014г., изм. ДВ. бр.107 от 2014г., изм. и доп. ДВ. бр.14 от 2015г., изм. и доп. ДВ. бр.24 от 2015г., доп. ДВ. бр.56 от 2015г., доп. ДВ. бр.61 от 2015г., изм. и доп. ДВ. бр.81 от 2016г., изм. и доп. ДВ. бр.97 от 2016г., изм. и доп. ДВ. бр.98 от 2016г., изм. и доп. ДВ. бр.103 от 2016г., доп. ДВ. бр.13 от 2017г., изм. ДВ. бр.26 от 2017г., доп. ДВ. бр.58 от 2017г., изм. и доп. ДВ. бр.97 от 2017г., изм. и доп. ДВ. бр.103 от 2017г., изм. ДВ. бр.7 от 19 януари 2018г., изм. ДВ. бр.10 от 30 януари 2018г.) се правят следните изменения и допълнения:

1. Член 22, ал. 1 се отменя.
2. В чл. 24 се създава ал. 4:
   „(4) Информационните фондове, изграждани за административно обслужване на гражданите, се използват и за целите на защита на националната сигурност, противодействие на престъпността, опазване на обществения ред и провеждане на наказателното производство.“
3. Създава се чл. 25а:
   „Чл. 25а (1) Обработването на лични данни, разкриващо расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионални съюзи, обработването на генетични данни, биометрични данни с цел уникално идентифициране на физическото лице, данни, свързани със здравето или сексуалния живот и сексуалната ориентация на лицето, е разрешено само когато това е абсолютно необходимо.
   (2) Личните данни по ал. 1 се събират само във връзка с други данни на засегнатото физическо лице.“
4. В чл. 26 се правят следните изменения и допълнения:
   а) В ал. 1 се правят следните изменения и допълнения:

аа) думата „свързани“ се заменя със „свързано“;

бб) точка 3 се отменя;

вв) точка 4 се изменя така:

„4. предоставят личните данни на органите за защита на националната сигурност, противодействие на престъпността и опазване на обществения ред, както и на органите на съдебната власт за нуждите на конкретно наказателно производство;“

гг) Създава се т. 5:

„5. Предоставят личните данни на други администратори, които са публични органи, или получатели, с оглед обработването им за цели, различни от целите за защита на националната сигурност, противодействие на престъпността, опазване на обществения ред и провеждане на наказателното производство, в съответствие със Закона за защита на личните данни и по ред, определен в инструкцията на министъра на вътрешните работи по чл. 29, ал. 2.“

дд) Създава се т. 6:

„6. обменят лични данни с компетентни органи и получатели от държави членки на Европейския съюз, органи и агенции на Европейския съюз, трети държави или международни организации в съответствие със Закона за защита на личните данни.“

б) Алинея 2 се изменя така:

„(2) Сроковете за заличаване на данните по ал. 1 или за периодична проверка на необходимостта от съхранението им се определят от министъра на вътрешните работи. Тези данни се заличават и в изпълнение на съдебен акт или решение на Комисията за защита на личните данни.“

5. В чл. 28, ал. 1, т. 3 след думите „Шенгенската информационна система (ШИС)“ се поставя запетая и се добавя „базите данни на Интерпол или базите данни на Европол“.
6. В чл. 29 се създава ал. 3:

„(3) Министърът на вътрешните работи определя длъжностно лице по защита на данните в съответствие със Закона за защита на личните данни.“

§ 30. В Закона за митниците (обн. ДВ. бр.15 от 1998г., изм. ДВ. бр.89 от 1998г., изм. ДВ. бр.153 от 1998г., изм. ДВ. бр.30 от 1999г., изм. ДВ. бр.83 от 1999г., изм. ДВ. бр.63 от 2000г., изм. ДВ. бр.110 от 2001г., доп. ДВ. бр.76 от 2002г., изм. ДВ. бр.37 от 2003г., изм. ДВ. бр.95 от 2003г., доп. ДВ. бр.38 от 2004г., изм. ДВ. бр.45 от 2005г., изм. ДВ. бр.86 от 2005г., изм. ДВ. бр.91 от 2005г., изм. ДВ. бр.105 от 2005г., изм. ДВ. бр.30 от 2006г., изм. ДВ. бр.105 от 2006г., изм. ДВ. бр.59 от 2007г., изм. ДВ. бр.109 от 2007г., изм. ДВ. бр.28 от 2008г., изм. ДВ. бр.43 от 2008г., изм. ДВ. бр.106 от 2008г., изм. ДВ. бр.12 от 2009г., изм. ДВ. бр.32 от 2009г., изм. ДВ. бр.42 от 2009г., изм. ДВ. бр.44 от 2009г., изм. ДВ. бр.95 от 2009г., изм. ДВ. бр.54 от 2010г., изм. ДВ. бр.55 от 2010г., изм. ДВ. бр.73 от 2010г., изм. ДВ. бр.94 от 2010г., изм. ДВ. бр.82 от 2011г., изм. ДВ. бр.38 от 2012г., изм. ДВ. бр.54 от 2012г., изм. и доп. ДВ. бр.15 от 2013г., изм. ДВ. бр.66 от 2013г., изм. ДВ. бр.98 от 2014г., изм. ДВ. бр.42 от 2015г., изм. и доп. ДВ. бр.60 от

2015г., изм. и доп. ДВ. бр.58 от 2016г., изм. и доп. ДВ. бр.75 от 2016г., изм. и доп. ДВ. бр.98 от 2016г., доп. ДВ. бр.99 от 2017г., изм. и доп. ДВ. бр.103 от 2017г.) чл. 17а се изменя и допълва така:

„Чл. 17а. (1) При изпълнение на служебните си задължения митническите служители могат да обработват лични данни.

(2) Митническите служители могат да обработват и лични данни, получени от други органи, за целите, за които са предоставени. Тези данни се препредават само с разрешение на органа, който ги е предоставил.

(3) При обработване на лични данни, свързано с дейностите по разузнаване, разкриване и разследване на нарушения или престъпления по чл. 234, 242, 242а и 251 от Наказателния кодекс и по чл. 255 от Наказателния кодекс по отношение на задължения за ДДС от внос и акцизи, митническите служители:

1. могат да не искат съгласието на физическото лице;

2. могат да не информират физическото лице преди и по време на обработването на личните му данни;

3. предоставят личните данни само на органите за защита на националната сигурност, противодействие на престъпността и опазване на обществения ред, както и на органите на съдебната власт за нуждите на конкретно наказателно производство.

4. обменят лични данни с компетентни органи и получатели от държави членки на Европейския съюз, трети държави или международни организации в съответствие със Закона за защита на личните данни.

(4) Сроковете за заличаване на данните по ал. 3 или за периодична проверка на необходимостта от съхранението им се определят от директора на Агенция „Митници“. Тези данни се заличават и в изпълнение на съдебен акт или решение на Комисията за защита на личните данни.

(5) Обработването на лични данни се осъществява при условията и по реда на този закон и на Закона за защита на личните данни.

(6) Администратор на лични данни е директорът на Агенция „Митници“, който възлага обработката на лични данни на оправомощени от него длъжностни лица, при условията и по реда на Закона за защита на личните данни.

(7) Директорът на Агенция „Митници“ определя длъжностно лице по защита на данните в съответствие със Закона за защита на личните данни.“

§ 31. В Закона за електронните съобщения (обн. ДВ. бр.41 от 2007г., изм. ДВ. бр.109 от 2007г., изм. ДВ. бр.36 от 2008г., изм. ДВ. бр.43 от 2008г., изм. ДВ. бр.69 от 2008г., изм. ДВ. бр.17 от 2009г., изм. ДВ. бр.35 от 2009г., изм. ДВ. бр.37 от 2009г., изм. ДВ. бр.42 от 2009г., изм. ДВ. бр.45 от 2009г., изм. ДВ. бр.82 от 2009г., изм. ДВ. бр.89 от 2009г., изм. ДВ. бр.93 от 2009г., изм. ДВ. бр.12 от 2010г., изм. ДВ. бр.17 от 2010г., изм. ДВ. бр.27 от 2010г., изм. ДВ. бр.97 от 2010г., изм. ДВ. бр.105 от 2011г., изм. и доп. ДВ. бр.38 от 2012г., изм. ДВ. бр.44 от 2012г., изм. ДВ. бр.82 от 2012г., изм. ДВ. бр.15 от 2013г., доп. ДВ. бр.27 от 2013г., доп. ДВ. бр.28 от 2013г., изм. ДВ. бр.52 от 2013г., изм. ДВ. бр.66 от 2013г., изм. ДВ. бр.70 от 2013г., доп. ДВ. бр.11 от 2014г., изм. ДВ. бр.53 от 2014г., изм. ДВ. бр.61 от 2014г., изм. ДВ. бр.98 от 2014г., изм. ДВ. бр.14 от 2015г., изм.

ДВ. бр.23 от 2015г., изм. и доп. ДВ. бр.24 от 2015г., изм. и доп. ДВ. бр.29 от 2015г., изм. ДВ. бр.61 от 2015г., изм. ДВ. бр.79 от 2015г., изм. ДВ. бр.50 от 2016г., изм. ДВ. бр.95 от 2016г., изм. и доп. ДВ. бр.97 от 2016г., изм. и доп. ДВ. бр.103 от 2016г., изм. ДВ. бр.58 от 2017г., изм. ДВ. бр.85 от 2017г., изм. и доп. ДВ. бр.101 от 2017г., изм. и доп. ДВ. бр.7 от 19 януари 2018г.) се правят следните изменения и допълнения:

1. Член 249, ал. 1 се изменя така:

„(1) Предприятията, предоставящи обществени електрони съобщителни услуги, обработват данните по чл. 248, ал. 2, т. 2, буква "а", както и всички други данни, законосъобразно получени от потребителите физически лица, в съответствие с Регламент (ЕС) 2016/679 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 и за отмяна на Директива 95/46/ЕО.“

2. Член 249, ал. 2 се изменя така:

„(2) Предприятията, предоставящи обществени електронни съобщителни услуги, не могат да поставят като условие за предоставяне на услугите си получаването на съгласието на потребител - физическо лице за обработване на личните му данни за цели, за които съгласно Регламент (ЕС) 2016/679 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 и за отмяна на Директива 95/46/ЕО е нужно изрично съгласие.“

§ 32. В Закона за обществените поръчки (обн. ДВ. бр.13 от 2016г., доп. ДВ. бр.34 от 2016г., изм. и доп. ДВ. бр.63 от 2017г., изм. ДВ. бр.85 от 2017г., доп. ДВ. бр.96 от 2017г., изм. и доп. ДВ. бр.102 от 2017г., изм. ДВ. бр.7 от 19 януари 2018г., изм. и доп. ДВ. бр.15 от 16 февруари 2018г., доп. ДВ. бр.17 от 23 февруари 2018г.) се правят следните изменения и допълнения:

1. Аления 5 на чл. 42 се изменя така:

„(5) При публикуване на документите по ал. 2 се заличава информацията, по отношение на която участниците правомерно са се позовали на конфиденциалност във връзка с наличието на търговска тайна, единните граждански номера и подписи на физическите лица, както и друга информация, която е защитена със закон. На мястото на заличената информация се посочва основанието за заличаване.“

2. В чл. 48 се създава алинея 7 със следното съдържание:

„(7) Когато предметът на поръчката е разработване, проектиране и използване на услуги и продукти, които се основават на обработване на лични данни или обработват лични данни, техническите спецификации, които определят характеристиките на предмета на поръчката трябва да бъдат съобразени с правилата за защита на лични данни съгласно чл. 25 от Регламент 2016/679, когато съответното обработване на лични данни попада в материалния обхват на Регламент 2016/679.“

§ 33. В Закона за съдебната власт (обн. ДВ. бр.64 от 2007г., изм. ДВ. бр.69 от 2008г., изм. ДВ. бр.109 от 2008г., изм. ДВ. бр.25 от 2009г., изм. ДВ. бр.33 от 2009г., изм. ДВ. бр.42 от 2009г., изм. ДВ. бр.102 от 2009г., изм. ДВ. бр.103 от 2009г., изм. ДВ. бр.59 от 2010г., изм. ДВ. бр.1 от 2011г., изм. ДВ. бр.23 от 2011г., изм. ДВ. бр.32 от 2011г.,

изм. ДВ. бр.45 от 2011г., изм. ДВ. бр.81 от 2011г., изм. ДВ. бр.82 от 2011г., изм. ДВ. бр.93 от 2011г., изм. ДВ. бр.20 от 2012г., изм. и доп. ДВ. бр.50 от 2012г., изм. ДВ. бр.81 от 2012г., изм. ДВ. бр.15 от 2013г., изм. ДВ. бр.17 от 2013г., изм. ДВ. бр.30 от 2013г., доп. ДВ. бр.52 от 2013г., изм. ДВ. бр.66 от 2013г., доп. ДВ. бр.70 от 2013г., изм. ДВ. бр.71 от 2013г., изм. ДВ. бр.19 от 2014г., изм. и доп. ДВ. бр.21 от 2014г., изм. ДВ. бр.53 от 2014г., изм. ДВ. бр.98 от 2014г., изм. ДВ. бр.107 от 2014г., изм. ДВ. бр.14 от 2015г., изм. и доп. ДВ. бр.28 от 2016г., изм. ДВ. бр.39 от 2016г., изм. ДВ. бр.50 от 2016г., изм. и доп. ДВ. бр.62 от 2016г., изм. ДВ. бр.76 от 2016г., изм. ДВ. бр.13 от 2017г., изм. ДВ. бр.14 от 2017г., изм. и доп. ДВ. бр.63 от 2017г., изм. и доп. ДВ. бр.65 от 2017г., изм. ДВ. бр.85 от 2017г., изм. и доп. ДВ. бр.90 от 2017г., изм. и доп. ДВ. бр.103 от 2017г., изм. и доп. ДВ. бр.7 от 19 януари 2018г., изм. ДВ. бр.15 от 16 февруари 2018г.) в чл. 54, ал.1 се създава т. 15:

„15. осъществява надзор за спазване на правилата за защита на личните данни от органите на съдебната власт, когато действат при изпълнение на правораздавателните си функции, включително разглежда жалби на физически лица във връзка с обработването на личните им данни.“