

## III

(Актове, приети по силата на Договора за ЕС)

## АКТОВЕ, ПРИЕТИ ПО СИЛАТА НА ДЯЛ VI ОТ ДОГОВОРА ЗА ЕС

## РАМКОВО РЕШЕНИЕ 2008/977/ПВР НА СЪВЕТА

от 27 ноември 2008 година

относно защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за Европейския съюз, и по-специално членове 30 и 31 и член 34, параграф 2, буква б) от него,

като взе предвид предложението на Комисията,

като взе предвид становището на Европейския парламент <sup>(1)</sup>,

като има предвид, че:

- (1) Европейският съюз си е поставил за цел поддържането и развиването на Съюза като пространство на свобода, сигурност и правосъдие, в което да се предостави висока степен на сигурност чрез общи действия на държавите-членки в областите на полицейското и съдебното сътрудничество по наказателноправни въпроси.
- (2) Общите действия в областта на полицейското сътрудничество по член 30, параграф 1, буква б) от Договора за Европейския съюз и общите действия в областта на съдебното сътрудничество по наказателноправни въпроси по член 31, параграф 1, буква а) от Договора за Европейския съюз предполагат необходимост от обработване на съответната информация, която следва да е предмет на подходящи разпоредби за защитата на личните данни.
- (3) Законодателството, попадащо в обхвата на дял VI от Договора за Европейския съюз, следва да подпомага полицейското и съдебното сътрудничество по наказателноправни въпроси с оглед на тяхната ефикасност, както и на тяхната законосъобразност и зачитането на основните права, по-специално правото на неприкосновеност на личния живот и на защита на личните данни. Общите стандарти по отношение на обработването и защитата на

лични данни, обработвани с цел предотвратяване и борба с престъпността, допринасят за постигането и на двете цели.

- (4) Хагската програма за укрепване на свободата, сигурността и правосъдието в Европейския съюз, приета от Европейския съвет на 4 ноември 2004 г., подчерта необходимостта от новаторски подход към трансграничния обмен на информация за правоприлагането при строгото спазване на основните изисквания в областта на защитата на данните и прикани Комисията да представи предложения в тази връзка най-късно до края на 2005 г. Това беше отразено в Плана за действие на Съвета и Комисията за прилагане на Хагската програма за укрепване на свободата, сигурността и правосъдието в Европейския съюз <sup>(2)</sup>.
- (5) Обменът на лични данни в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, особено в съответствие с принципа за наличност на информацията, заложен в Хагската програма, следва да бъде подкрепен с ясни правила, които засилват взаимното доверие между компетентните органи и осигуряват защитата на съответната информация по начин, който изключва всяка дискриминация по отношение на такова сътрудничество между държавите-членки, като същевременно напълно защита основните права на физическите лица. Съществуващите на европейско равнище инструменти не са достатъчни; Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни <sup>(3)</sup> не се прилага за обработването на лични данни в хода на дейност, попадаща извън обхвата на общностното право, като например дейностите, предвидени в дял VI от Договора за Европейския съюз, нито във всеки случай, за операции по обработване, отнасящи се до обществената сигурност, отбраната, държавната сигурност или дейности на държавата в областите на наказателното право.

<sup>(1)</sup> ОВ С 125 Е, 22.5.2008 г., стр. 154.

<sup>(2)</sup> ОВ С 198, 12.8.2005 г., стр. 1.

<sup>(3)</sup> ОВ L 281, 23.11.1995 г., стр. 31.

- (6) Настоящото рамково решение се прилага само за данни, събрани или обработвани от компетентни органи за целите на предотвратяването, разследването, откриването или наказателното преследване на престъпления или изпълнението на наказания. Настоящото рамково решение следва да оставя на държавите-членки да определят с по-голяма точност на национално равнище какви други цели следва да се смятат за несъвместими с целта, за която личните данни са били събрани първоначално. По принцип по-нататъшното обработване за исторически, статистически или научни цели не следва да се счита за несъвместимо с първоначалната цел на обработването.
- (7) Обхватът на настоящото рамково решение е ограничен до обработването на лични данни, които се изпращат или предоставят между държавите-членки. От това ограничение не следва да произтичат никакви заключения относно компетентността на Съюза да приема актове, свързани със събирането и обработването на лични данни на национално равнище или целесъобразността Съюзът да предприеме това в бъдеще.
- (8) За да улеснят обмена на данни в рамките на Съюза, държавите-членки възнамеряват да гарантират, че стандартът за защита на данни, постигнат при обработването на данни на национално равнище, съответства на предвидения в настоящото рамково решение. По отношение на обработването на данни на национално равнище настоящото рамково решение не възпрепятства държавите-членки да предоставят по-високи гаранции за защита на личните данни от установените в настоящото рамково решение.
- (9) Настоящото рамково решение не следва да се прилага за лични данни, които държава-членка е получила в рамките на настоящото рамково решение и които са с произход от същата държава-членка.
- (10) Сближаването на законодателствата на държавите-членки не би следвало да води до понижаване на равнището на предоставяната от тях защита на данните, а напротив, следва да цели осигуряване на високо ниво на защита в рамките на Съюза.
- (11) Необходимо е да се уточнят целите на защитата на данни в рамките на полицейските и съдебните дейности и да се установят правни норми относно законосъобразността на обработването на лични данни, за да се гарантира, че всяка информация, която би могла да се обменя, е обработена законосъобразно и в съответствие с основните принципи, свързани с качеството на данните. Същевременно законните дейности на полицейските, митническите, съдебните и други компетентни органи не следва да бъдат застрашени по никакъв начин.
- (12) Принципът за точност на данните следва да се прилага, като се отчитат естеството и целта на съответното обработване. Например, по-специално при съдебно производство данните се основават на субективното възприятие на физическите лица и в някои случаи не могат да бъдат проверени по никакъв начин. Следователно изискването за точност не може да бъде отнесено до точността на едно твърдение, а само до факта, че конкретно твърдение е било направено.
- (13) Архивирането в отделен набор от данни следва да е разрешено само ако данните вече не са необходими и не се използват за предотвратяването, разследването, откриването или наказателното преследване на престъпления или за изпълнението на наказания. Архивирането в отделен набор от данни следва да е разрешено също и ако архивираните данни се съхраняват в база данни с други данни по начин, който не дава възможност да бъдат използвани за предотвратяването, разследването, откриването или наказателното преследване на престъпления или за изпълнението на наказания. Целесъобразността на периода на архивиране следва да зависи от целите на архивирането и от законните интереси на субектите на данните. В случай на архивиране за исторически цели може да се предвиди много дълъг период.
- (14) Данните могат също така да бъдат изтрети чрез унищожаване на информационния носител.
- (15) По отношение на неточните, непълните или вече неактуалните данни, изпращани или предоставяни на друга държава-членка, и обработвани по-нататък от квазисъдебни органи, т.е. органи с правомощия да вземат правообвързващи решения, тяхното коригиране, заличаване или блокиране следва да се извършва в съответствие с националното законодателство.
- (16) Осигуряването на високо ниво на защита на личните данни на физическите лица изисква общи разпоредби за определяне на законосъобразността и качеството на данните, обработвани от компетентни органи в други държави-членки.
- (17) Подходящо е на европейско равнище да се определят условията, при които следва да бъде разрешено на компетентните органи на държавите-членки да предават и предоставят на органи и частни страни в държави-членки лични данни, получени от други държави-членки. В много случаи предаването на лични данни от съдебната власт, полицията или митниците на частни страни е необходимо с оглед наказателното преследване на престъпления или предотвратяването на непосредствена и сериозна заплаха за обществената сигурност или предотвратяването на сериозно нарушение на правата на физическите лица, например чрез отправяне на предупредителни сигнали до банките и кредитните институции относно подправянето на ценни книжа или при престъпления, свързани с превозни средства, чрез съобщаване на застрахователните компании на лични данни с оглед предотвратяването на незаконния трафик на откраднати моторни превозни средства или с оглед подобряването на условията за връщане от чужбина на откраднати моторни превозни средства. Това не е равносилно на прехвърлянето на полицейски или съдебни задачи на частни страни.

- (18) Нормите в настоящото рамково решение относно предаването на лични данни от съдебната власт, полицията или митниците на частни страни не се прилагат по отношение на разкриването на данни пред частни страни (такива като адвокати на защитата и жертви) в рамките на наказателно производство.
- (19) По-нататъшното обработване на лични данни, получени или предоставени от компетентния орган на друга държава-членка, по-специално по-нататъшното изпращане или предоставяне на тези данни, следва да бъде предмет на общи правила на европейско равнище.
- (20) В случаите, когато личните данни могат да бъдат обработени по-нататък, след като държавата-членка, от която са получени, е дала съгласието си, всяка държава-членка следва да може да определи реда и условията за даване на такова съгласие, включително например посредством общо съгласие за категории информация или за категории по-нататъшно обработване.
- (21) Когато лични данни могат да бъдат обработени по-нататък за административни действия, тези действия следва да включват също дейности, извършвани от регулаторни и надзорни органи.
- (22) Законните дейности на полицейските, митническите, съдебните и други компетентни органи може да изискват данните да бъдат изпратени на властите на трети държави или на международни структури, които имат задължения за предотвратяването, разследването, откриването или наказателното преследване на престъпления или изпълнението на наказания.
- (23) Когато лични данни се предават от една държава-членка на трети държави или международни структури, тези данни по принцип следва да се ползват с подходящо ниво на защита.
- (24) Когато лични данни се предават от една държава-членка на трети държави или международни структури, предаването следва да се извърши по принцип само след като държавата-членка, от която са получени данните, даде съгласието си за това. Всяка държава-членка следва да може да определи реда и условията за даване на такова съгласие, включително например чрез общо съгласие за категории информация или за конкретни трети държави.
- (25) В интерес на ефикасното сътрудничество в областта на правоприлагането се изисква в случаите, когато заплахата за обществената сигурност на държава-членка или на трета държава е толкова непосредствена, че да направи своевременното получаване на предварително съгласие невъзможно, компетентният орган да може да предаде съответните лични данни на заинтересованата трета държава без такова предварително съгласие. Същото би могло да се прилага, когато са поставени под въпрос съществени интереси на държава-членка с равностойно значение, например когато критична инфраструктура на държава-членка би могла да стане обект на непосредствена и сериозна заплаха или когато финансовата система на държава-членка би могла сериозно да бъде нарушена.
- (26) Може да се наложи субектът на данни да бъде информиран за обработването на неговите данни — по-специално когато е налице особено сериозно посегателство върху правата му в резултат на секретни мерки за събиране на данни — за да се гарантира, че субектът на данни може да се ползва от ефективна правна защита.
- (27) Държавите-членки следва да гарантират, че субектът на данните е информиран, че личните данни биха могли или се събират, обработват или предават на друга държава-членка за целите на предотвратяването, разследването, откриването или наказателното преследване на престъпления или изпълнението на наказания. Редът и условията относно правото на субекта на данните да бъде информиран и изключенията от тях следва да се определят от националното законодателство. Това може да стане по общ ред, например чрез закон или чрез публикуване на списък на операциите по обработване.
- (28) С цел осигуряване на защита на личните данни, без да се излагат на риск интересите на наказателното разследване, е необходимо да се определят правата на субекта на данните.
- (29) Някои държави-членки предоставят право на достъп на субекта на данните в наказателноправната област посредством система, при която националният надзорен орган вместо субектът на данните има достъп до всички лични данни на субекта на данните без никакво ограничение и може също да коригира, заличава или актуализира неточни данни. В такъв случай на непряк достъп националното законодателство на въпросните държави-членки може да предвижда, че националният надзорен орган ще информира субекта на данните само че са били извършени всички необходими проверки. Въпросните държави-членки също предвиждат и възможности за пряк достъп на субекта на данните в специфични случаи, като например достъп до съдебни регистри, с цел получаване на копия от собствените свидетелства за съдимост или от документи, свързани със собствените показания пред полицейските служби.
- (30) Уместно е да се установят общи правила относно поверителността и сигурността на обработването, относно отговорността и санкциите при неправомерно използване от компетентни органи, както и относно средствата за правна защита, които са на разположение на субекта на данните. Всяка държава-членка обаче сама определя естеството на разпоредбите при неправомерно увреждане и на санкциите, приложими при нарушения на националните разпоредби за защита на данните.
- (31) Настоящото рамково решение позволява принципът за обществен достъп до официални документи да се вземе под внимание при прилагане на определените в настоящото рамково решение принципи.

- (32) Когато е необходимо да се защитят личните данни във връзка с обработването, което поради своя мащаб или вид излага на специфичен риск основните права и свободи, например обработване посредством нови технологии, механизми или процедури, е уместно преди създаването на системи за класиране, предназначени за обработването на тези данни, да се гарантира, че са консултирани компетентните национални надзорни органи.
- (33) Създаването в държавите-членки на надзорни органи, които напълно независимо упражняват функциите си, е основен елемент от защитата на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество между държавите-членки.
- (34) Надзорните органи, вече създадени в държавите-членки съгласно Директива 95/46/ЕО, следва да могат също така да поемат отговорност за задачите, които ще бъдат поставени пред националните надзорни органи, които предстои да бъдат създадени съгласно настоящото рамково решение.
- (35) Тези надзорни органи следва да разполагат с необходимите средства за изпълнение на своите задължения, включително правомощия за разследване и намеса, особено в случаи на жалби от физически лица, или правомощия за участие в съдебни производства. Тези надзорни органи следва да допринасят за осигуряването на прозрачност при обработването в държавите-членки, под чиято юрисдикция попадат. Техните правомощия обаче не следва да възпрепятстват специфичните норми, установени за наказателните производства или за независимостта на съдебната власт.
- (36) Член 47 от Договора за Европейския съюз предвижда, че никоя от разпоредбите в него не засяга договорите за създаване на Европейските общности или последващите договори и актове, които ги изменят или допълват. Съответно настоящото рамково решение не засяга защитата на лични данни съгласно общностното право, по-специално както е предвидено в Директивия 95/46/ЕО, в Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни<sup>(1)</sup> и в Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронните комуникации)<sup>(2)</sup>.
- (37) Настоящото рамково решение не засяга разпоредбите, отнасящи се до незаконния достъп до данни, установени в Рамково решение 2005/222/ПВР на Съвета от 24 февруари 2005 г. относно атаките срещу информационните системи<sup>(3)</sup>.
- (38) Настоящото рамково решение не засяга съществуващите задължения и ангажименти, поети от държавите-членки или от Съюза по силата на двустранни и/или многостранни споразумения с трети държави. Бъдещите споразумения следва да спазват разпоредбите относно обмена с трети държави.
- (39) Няколко акта, приети въз основа на дял VI от Договора за Европейския съюз, съдържат конкретни разпоредби относно защитата на лични данни, обменяни или по друг начин обработвани съгласно тези актове. В някои случаи тези разпоредби съставляват един пълен и последователен набор от норми, обхващащи всички съответни аспекти на защитата на данни (принципи за качеството на данните, правила за сигурност на данните, регламентиране на правата и гаранциите на субектите на данни, организиране на надзор и отговорност) и регламентират тези въпроси по-подробно, отколкото настоящото рамково решение. Съответният набор от разпоредби за защита на данните в тези актове, по-специално тези, които уреждат функционирането на Европол, Евроюст, Шенгенската информационна система (SIS) и Митническата информационна система (CIS), както и даващите пряк достъп на органите на държавите-членки до определени системи с данни на други държави-членки, не следва да бъдат засегнати от настоящото рамково решение. Същото се прилага и по отношение на разпоредбите за защита на данни, уреждащи автоматизираното прехвърляне между държавите-членки на ДНК профили, дактилоскопни данни и данни относно националната регистрация на превозни средства съгласно Решение 2008/615/ПВР на Съвета от 23 юни 2008 г. относно засилване на трансграничното сътрудничество, по-специално в борбата срещу тероризма и трансграничната престъпност<sup>(4)</sup>.
- (40) В други случаи разпоредбите относно защитата на данни в актове, приети въз основа на дял VI от Договора за Европейския съюз, са с по-ограничен обхват. Често те установяват за държавата-членка, която получава от други държави-членки информация, съдържаща лични данни, специфични условия по отношение на целите, за които може да използва тези данни, но относно други аспекти от защитата на данните се позовават на Конвенцията на Съвета на Европа от 28 януари 1981 г. за защита на физическите лица по отношение на автоматизираната обработка на лични данни или на националното законодателство. Когато разпоредбите на тези актове, налагащи на получаващата държава-членка условия по отношение на използването или по-нататъшното предаване на лични данни, са по-ограничаващи, отколкото съдържащите се в съответните разпоредби на настоящото рамково решение, първите разпоредби следва да останат непроменени. По отношение на всички останали аспекти обаче следва да се прилагат правилата, установени в настоящото рамково решение.
- (41) Настоящото рамково решение не засяга Конвенцията на Съвета на Европа за защита на физическите лица по отношение на автоматизираната обработка на лични данни, Допълнителния протокол към посочената конвенция от 8 ноември 2001 г. или конвенциите на Съвета на Европа относно съдебното сътрудничество по наказателноправни въпроси.

<sup>(1)</sup> ОВ L 8, 12.1.2001 г., стр. 1.

<sup>(2)</sup> ОВ L 201, 31.7.2002 г., стр. 37.

<sup>(3)</sup> ОВ L 69, 16.3.2005 г., стр. 67.

<sup>(4)</sup> ОВ L 210, 6.8.2008 г., стр. 1.

- (42) Тъй като целта на настоящото рамково решение, а именно определянето на общи норми за защита на личните данни, обработвани в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, не може да бъде постигната в достатъчна степен от държавите-членки, и следователно, поради мащаба и последиците на действието, може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за създаване на Европейската общност и посочен в член 2 от Договора за Европейския съюз. Съгласно принципа на пропорционалност, уреден в член 5 от Договора за създаване на Европейската общност, настоящото рамково решение не надхвърля необходимото за постигането на тази цел.
- (43) Обединеното кралство участва в настоящото рамково решение в съответствие с член 5 от Протокола за интегриране на достиженията на правото от Шенген в правната рамка на Европейския съюз, приложен към Договора за Европейския съюз и към Договора за създаване на Европейската общност, и член 8, параграф 2 от Решение 2000/365/ЕО на Съвета от 29 май 2000 г. относно искането на Обединеното кралство Великобритания и Северна Ирландия да участва в някои разпоредби от достиженията на правото от Шенген <sup>(1)</sup>.
- (44) Ирландия участва в настоящото рамково решение в съответствие с член 5 от Протокола за интегриране на достиженията на правото от Шенген в правната рамка на Европейския съюз, приложен към Договора за Европейския съюз и към Договора за създаване на Европейската общност, и член 6, параграф 2 от Решение 2002/192/ЕО на Съвета от 28 февруари 2002 г. относно искането на Ирландия да участва в някои разпоредби от достиженията на правото от Шенген <sup>(2)</sup>.
- (45) По отношение на Исландия и Норвегия настоящото рамково решение представлява развитие на достиженията на правото от Шенген по смисъла на Споразумението, сключено от Съвета на Европейския съюз с Република Исландия и Кралство Норвегия, за асоциирането на тези две държави при въвеждането, прилагането и развитието на достиженията на правото от Шенген <sup>(3)</sup>, което попада в областта, посочена в член 1, букви З и И от Решение 1999/437/ЕО на Съвета <sup>(4)</sup> относно определени условия по прилагането на посоченото споразумение.
- (46) По отношение на Швейцария настоящото рамково решение представлява развитие на разпоредбите на достиженията на правото от Шенген по смисъла на Споразумението между Европейския съюз, Европейската общност и Конфедерация Швейцария относно асоциирането на Конфедерация Швейцария при въвеждането, прилагането и развитието на достиженията на правото от Шенген <sup>(5)</sup>, което попада в областта, посочена в член 1, букви З и И

от Решение 1999/437/ЕО на Съвета, четен във връзка с член 3 от Решение 2008/149/ПВР на Съвета <sup>(6)</sup> относно сключването на посоченото споразумение от името на Европейския съюз и от името на Европейската общност.

- (47) По отношение на Лихтенщайн настоящото рамково решение представлява развитие на разпоредбите на достиженията на правото от Шенген по смисъла на Протокола подписан между Европейския съюз, Европейската общност, Конфедерация Швейцария и Княжество Лихтенщайн относно присъединяването на Княжество Лихтенщайн към Споразумението между Европейския съюз, Европейската общност и Конфедерация Швейцария при въвеждането, прилагането и развитието на достиженията на правото от Шенген, които попадат в областта, посочена в член 1, букви букви З и И от Решение 1999/437/ЕО, четен във връзка с член 3 от Решение 2008/262/ПВР на Съвета <sup>(7)</sup> относно подписването на посочения протокол от името на Европейския съюз.
- (48) Настоящото рамково решение спазва основните права и спазва принципите, възприети по-специално в Хартата на основните права на Европейския съюз <sup>(8)</sup>. Настоящото рамково решение има за цел да гарантира пълно зачитане на правото на неприкосновеност на личния живот и правото на защита на личните данни, отразени в членове 7 и 8 от Хартата,

ПРИЕ НАСТОЯЩОТО РАМКОВО РЕШЕНИЕ:

#### Член 1

##### Цел и обхват

1. Настоящото рамково решение има за цел да осигури високо ниво на защита на основните права и свободи на физическите лица, и по-специално на правото им на неприкосновеност на личния живот във връзка с обработването на лични данни в рамките на полицейското и съдебното сътрудничество по наказателноправни въпроси, предвидено в дял VI от Договора за Европейския съюз, като същевременно гарантира високо ниво на обществена сигурност.

2. В съответствие с настоящото рамково решение държавите-членки защитават основните права и свободи на физическите лица и по-специално правото им на неприкосновеност на личния живот, когато за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания личните данни:

a) са или са били предадени или предоставени между държавите-членки;

<sup>(1)</sup> ОВ L 131, 1.6.2000 г., стр. 43.

<sup>(2)</sup> ОВ L 64, 7.3.2002 г., стр. 20.

<sup>(3)</sup> ОВ L 176, 10.7.1999 г., стр. 36.

<sup>(4)</sup> ОВ L 176, 10.7.1999 г., стр. 31.

<sup>(5)</sup> ОВ L 53, 27.2.2008 г., стр. 52.

<sup>(6)</sup> ОВ L 53, 27.2.2008 г., стр. 50.

<sup>(7)</sup> ОВ L 83, 26.3.2008 г., стр. 5.

<sup>(8)</sup> ОВ С 303, 14.12.2007 г., стр. 1.

б) са или са били предадени или предоставени от държавите-членки на органи или информационни системи, създадени въз основа на дял VI от Договора за Европейския съюз; или

в) са или са били предадени или предоставени на компетентните органи на държавите-членки от органите или информационните системи, създадени въз основа на Договора за Европейския съюз или на Договора за създаване на Европейската общност.

3. Настоящото рамково решение се прилага при обработване на лични данни, извършвано изцяло или частично чрез автоматични средства, както и при обработване, извършвано по друг начин освен чрез автоматични средства, на лични данни, които съставляват част от система за класиране или са предназначени да бъдат част от такава система.

4. Настоящото рамково решение не засяга основни интереси, свързани с националната сигурност, нито специфични разузнавателни дейности в областта на националната сигурност.

5. Настоящото рамково решение не пречи държавите-членки да предоставят по-големи гаранции от установените в него за защита на събираните или обработвани на национално равнище лични данни.

#### Член 2

#### Определения

За целите на настоящото рамково решение:

а) „лични данни“ означава всяка информация, свързана с физическо лице с установена или установяема самоличност („субект на данните“); лице с установяема самоличност е лице, чиято самоличност може да се установи пряко или косвено, по-специално по идентификационен номер или по един или повече фактори, специфични за неговата физическа, физиологична, психическа, икономическа, културна или социална самоличност;

б) „обработване на лични данни“ и „обработване“ означават всяка операция или съвкупност от операции, извършвани със или без автоматични средства по отношение на личните данни, като събиране, записване, организиране, съхраняване, адаптиране или изменяне, извличане, справка, използване, разкриване чрез предаване, разпространяване или предоставяне по друг начин, подреждане или комбиниране, блокиране, заличаване или унищожаване;

в) „блокиране“ означава обозначаването на съхраняваните лични данни с цел ограничаване на тяхното обработване в бъдеще;

г) „система за класиране на лични данни“ и „система за класиране“ означават всяка структурирана съвкупност от лични данни, достъпни по специфични критерии, независимо дали е централизирана, децентрализирана или разпределена по функционален или географски принцип;

д) „обработващ лични данни“ означава всеки, който обработва лични данни от името на администратора;

е) „получател“ означава всеки, пред който се разкриват данни;

ж) „съгласие на субекта на данните“ означава всеки свободно даден, конкретен и информиран израз на воля, с който субектът на данните изразява съгласието си да бъдат обработвани личните му данни;

з) „компетентни органи“ означава служби или органи, създадени с правни актове, приети от Съвета съгласно дял VI от Договора за Европейския съюз, както и полицейски, митнически, съдебни и други компетентни органи на държавите-членки, които са упълномощени съгласно националното законодателство да обработват лични данни, попадащи в обхвата на настоящото рамково решение;

и) „администратор“ означава физическо или юридическо лице, държавен орган, агенция или друг орган, който сам или съвместно с други определя целите и начините за обработка на лични данни;

й) „обозначаване“ означава маркирането на съхраняваните лични данни, без да се цели ограничаване на тяхното обработване в бъдеще;

к) „права анонимен“ означава изменение на лични данни по такъв начин, че подробностите относно личните и материалните обстоятелства вече да не могат или да могат само с несъразмерен разход на време, финансови средства и труд да бъдат приписани на физическо лице с установена или установяема самоличност.

#### Член 3

#### Принципи на законосъобразност, пропорционалност и цел

1. Личните данни могат да се събират от компетентните органи само за специфични, изрични и законосъобразни цели в рамките на техните задачи и могат да бъдат обработвани само за целта, за която са събрани. Обработването на данни следва да бъде законосъобразно и адекватно, като не е прекомерно по отношение на целите, за които са събрани данните.

2. По-нататъшното обработване за друга цел е разрешено, когато:

а) не е несъвместимо с целите, за които са били събрани данните;

б) компетентните органи са упълномощени да обработват такива данни за друга такава цел в съответствие с приложимите законови разпоредби; и

в) обработването е необходимо и пропорционално на тази друга цел.

Компетентните органи могат да обработят изпратените лични данни по-нататък за исторически, статистически или научни цели, при условие че държавите-членки осигурят подходящи гаранции, като например да направят данните анонимни.

## Член 4

**Коригиране, заличаване и блокиране**

1. Личните данни се коригират, ако са неточни и, когато това е възможно и необходимо, се допълват или актуализират.
2. Личните данни се заличават или правят анонимни, когато вече не са необходими за целите, за които са били законно събрани или са обект на по-нататъшно законосъобразно обработване. Настоящата разпоредба не засяга архивирането на тези данни в отделна база данни за подходящ период в съответствие с националното законодателство.
3. Личните данни се блокират, вместо да се заличават, ако са налице разумни основания да се смята, че заличаването им би могло да засегне законните интереси на субекта на данните. Блокираните данни се обработват само за целта, която е пречила заличаването им.
4. Когато личните данни се съдържат в съдебно решение или регистър, свързан с издаването на съдебно решение, коригирането, заличаването или блокирането се извършват в съответствие с националните правила за съдебните производства.

## Член 5

**Определяне на срокове за заличаване и преглед**

За заличаването на лични данни или за периодичен преглед на необходимостта от съхранението на тези данни се определят подходящи срокове. Съблюдаването на тези срокове се гарантира чрез процедурни мерки.

## Член 6

**Обработване на специални категории данни**

Обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на данни, свързани със здравето или сексуалния живот, е разрешено само когато това е строго необходимо и когато националното законодателство осигурява адекватни гаранции.

## Член 7

**Автоматизирани индивидуални решения**

Решение, което предизвиква неблагоприятни правни последици за субекта на данните или съществено го засяга и което се основава единствено на автоматизирано обработване на данни за целите на оценяването на определени лични аспекти, свързани със субекта на данните, е позволено само когато е разрешено от закон, който установява мерки за гарантиране на законните интереси на субекта на данните.

## Член 8

**Проверка на качеството на данните, които се изпращат или предоставят**

1. Компетентните органи предприемат всички разумни стъпки, за да гарантират, че лични данни, които са неточни,

непълни или вече не са актуални, не се изпращат или не се предоставят. За тази цел компетентните органи, доколкото това е практически възможно, проверяват качеството на личните данни преди тяхното изпращане или предоставяне. Доколкото е възможно, при всяко предаване на данни се добавя наличната информация, което позволява получаващата държава-членка да оцени степента на точност, пълнота, актуалност и надеждност. Ако личните данни са предадени, без да са поискани, получаващият орган незабавно проверява дали тези данни са необходими за целта, за която са предадени.

2. Ако се окаже, че са изпратени неверни данни или данни, които са предадени незаконосъобразно, получателят трябва да бъде уведомен незабавно. Данните трябва незабавно да бъдат коригирани, заличени или блокирани в съответствие с член 4.

## Член 9

**Срокове**

1. При предаване или предоставяне на данните изпращащият орган може, в съответствие с националното законодателство и съгласно членове 4 и 5, да посочи сроковете за запазване на данни, след изтичането на които получателят трябва да заличи или да блокира данните или да извърши преглед дали те все още са необходими. Това задължение не се прилага, ако към момента на изтичане на тези срокове данните са необходими за текущо разследване, наказателно преследване на престъпления или изпълнение на наказания.

2. Когато изпращащият орган не е посочил срок в съответствие с параграф 1, се прилагат сроковете, посочени в членове 4 и 5, за запазване на данни, предвидени в националното законодателство на получаващата държава-членка.

## Член 10

**Вписване и документиране**

1. Всяко предаване на лични данни се вписва или документираща с цел проверка на законосъобразността на обработването на данните, самонаблюдение и осигуряване на подходяща цялост и сигурност на данните.

2. Вписванията или документацията, изготвени съгласно параграф 1, се съобщават при поискване на компетентния надзорен орган за упражняване на контрол върху защитата на данните. Компетентният надзорен орган използва тази информация само за упражняване на контрол върху защитата на данните и за гарантиране на подходящото им обработване, както и на целостта и сигурността на данните.

## Член 11

**Обработване на лични данни, получени или предоставени от друга държава-членка**

Личните данни, получени или предоставени от компетентния орган на друга държава-членка, могат, в съответствие с изискванията на член 3, параграф 2, да бъдат обект на по-нататъшно обработване само за следните цели, различни от целите, за които са били изпратени или предоставени:

- а) предотвратяване, разследване, откриване или наказателно преследване на престъпления или изпълнение на наказания, различни от тези, за които са били изпратени или предоставени;
- б) други съдебни и административни производства, пряко свързани с предотвратяването, разследването, откриването и наказателното преследване на престъпления или изпълнението на наказания;
- в) предотвратяване на непосредствена и сериозна заплаха за обществената сигурност; или
- г) всяка друга цел, само с предварителното съгласие на изпращащата държава-членка или със съгласието на субекта на данните, дадено в съответствие с националното законодателство.

Компетентните органи могат да подложат изпратените лични данни на по-нататъшно обработване за исторически, статистически или научни цели, при условие че държавите-членки осигурят подходящи гаранции, като например да направят данните анонимни.

#### Член 12

##### Спазване на национални ограничения, свързани с обработването

1. Когато съгласно законодателството на изпращащата държава-членка спрямо обмена на данни между компетентните органи на тази държава-членка се прилагат специфични ограничения при специфични обстоятелства, изпращащият орган уведомява получателя за тези ограничения. Получателят гарантира, че тези ограничения, свързани с обработването, се спазват.

2. При прилагане на параграф 1 държавите-членки не прилагат ограничения по отношение на предаването на данни на други държави-членки или на служби или органи, създадени по силата на дял VI от Договора за Европейския съюз, различни от тези, които се прилагат при подобно предаване на данни на национално равнище.

#### Член 13

##### Предаване на компетентни органи в трети държави или на международни структури

1. Държавите-членки предвиждат личните данни, изпратени или предоставени от компетентния орган на друга държава-членка, да могат да бъдат предавани на трети държави или международни структури само ако:

- а) това е необходимо за предотвратяването, разследването, откриването и наказателното преследване на престъпления или изпълнението на наказания;

- б) получаващият орган в третата държава или получаващата международна структура носи отговорност за предотвратяването, разследването, откриването или наказателното преследване на престъпления или изпълнението на наказания;
- в) държавата-членка, от която са получени данните, е дала своето съгласие за тяхното предаване в съответствие с националното си законодателство; и
- г) съответната трета държава или международна структура осигурява адекватно ниво на защита за планираното обработване на данни.

2. Предаване без предварително съгласие в съответствие с параграф 1, буква в) е разрешено само ако предаването на данните е от съществено значение за предотвратяването на непосредствена и сериозна заплаха за обществената сигурност на държава-членка или на трета държава или за основни интереси на държава-членка, и предварителното съгласие не може да бъде получено своевременно. Органът, който отговаря за даването на съгласие, трябва да бъде уведомен незабавно.

3. Чрез дерогация от параграф 1, буква г) лични данни могат да бъдат предавани, ако:

- а) националното законодателство на държавата-членка, предаваща данните, предвижда това поради:
- i) законни специфични интереси на субекта на данните; или
- ii) законни приоритетни интереси, особено важни обществени интереси; или
- б) третата държава или получаващата международна структура предоставя гаранции, които се считат за адекватни от съответната държава-членка съгласно националното ѝ законодателство.

4. Адекватността на равнището на защита, посочено в параграф 1, буква г), се оценява в контекста на всички обстоятелства около операцията или съвкупността от операции по предаване на данни. Специално внимание се обръща на естеството на данните, целта и продължителността на предлаганата операция или операции по обработването им, държавата на произхода и държавата или международната структура на крайното местоназначение на данните, правните норми, както общи, така и секторни, които са в сила във въпросната трета държава или международна структура, и професионалните правила и мерките за сигурност, които се прилагат.

#### Член 14

##### Предаване на частни страни в държави-членки

1. Държавите-членки гарантират, че личните данни, получени или предоставени от компетентния орган на друга държава-членка, могат да бъдат предадени на частни страни само в случай че:



- а) компетентният орган на държавата-членка, от която са получени данните, е дал съгласие за предаването в съответствие с националното си законодателство;
- б) няма законни специфични интереси на субекта на данните, които да възпрепятстват предаването; и
- в) в определени случаи предаването е от съществено значение за компетентния орган, предаващ данните на частна страна за:
- изпълнението на законно възложена му задача;
  - предотвратяването, разследването, откриването и наказателното преследване на престъпления или изпълнението на наказания;
  - предотвратяването на непосредствена и сериозна заплаха за обществената сигурност; или
  - предотвратяването на сериозно нарушение на правата на физически лица.

2. Компетентният орган, предаващ данните на частна страна, уведомява последната за целите, за които данните могат да бъдат изрично използвани.

#### Член 15

##### Информирание по искане на компетентния орган

При поискване получателят информира компетентния орган, изпратил или предоставил личните данни, за тяхната обработка.

#### Член 16

##### Информация за субекта на данните

1. Държавите-членки гарантират, че субектът на данните е информиран относно събирането или обработването на лични данни от техните компетентни органи в съответствие с националното законодателство.

2. Когато между държавите-членки се предават или предоставят лични данни, всяка държава-членка може, в съответствие с разпоредбите на националното си законодателство, посочени в параграф 1, да поиска другата държава-членка да не информира субекта на данните. В такъв случай втората държава-членка не информира субекта на данните без предварителното съгласие на първата държава-членка.

#### Член 17

##### Право на достъп

1. Всеки субект на данни има право, след отправяне на искания на разумни интервали, да получи без ограничение и без прекомерно забавяне или разходи:

- а) поне потвърждение от администратора или от националния надзорен орган, дали данни, свързани с него, са били предадени или предоставени, и информация относно получа-

телите или категориите получатели, пред които са разкрити данните, както и информация за данните, които са в процес на обработване; или

- б) поне потвърждение от националния надзорен орган, че са извършени всички необходими проверки.

2. Държавите-членки могат да приемат законодателни мерки, ограничаващи достъпа до информация съгласно параграф 1, буква а) в случаите, когато такова ограничение, при зачитане на законните интереси на засегнатото лице, съставлява необходима и пропорционална мярка:

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

- б) за да се избегне повлияване върху предотвратяването, откриването, разследването и наказателното преследване на престъпления или изпълнението на наказания;

- в) за защита на обществената сигурност;

- г) за защита на националната сигурност;

- д) за защита на субекта на данните или правата и свободите на другите.

3. Всеки отказ или ограничаване на достъпа се изпраща в писмен вид на субекта на данните. Същевременно му се съобщават и фактическите или правните основания за решението. Това информирание може да бъде пропуснато, ако съществува причина съгласно параграф 2, букви а)—д). Във всички тези случаи субектът на данните бива уведомен, че може да обжалва пред компетентния национален надзорен орган, пред съдебен орган или пред съд.

#### Член 18

##### Право на коригиране, заличаване или блокиране

1. Субектът на данните има право да очаква администраторът да изпълни своите задължения в съответствие с членове 4, 8 и 9 относно коригирането, заличаването или блокирането на лични данни, произтичащи от настоящото рамково решение. Държавите-членки определят дали субектът на данните може да упражни това право пряко пред администратора или чрез посредничеството на компетентния национален надзорен орган. Ако администраторът откаже да извърши коригирането, заличаването или блокирането, отказът трябва да бъде съобщен в писмен вид на субекта на данните, който трябва да бъде информиран за възможностите, предвидени в националното законодателство, за подаване на жалба или търсене на средство за правна защита. След разглеждане на жалбата или средството за правна защита субектът на данните бива уведомен дали администраторът е действал правилно. Държавите-членки могат също да предвидят субектът на данните да бъде уведомен от компетентния национален надзорен орган, че е извършен преглед.

2. Ако точността на част от личните данни бъде оспорена от субекта на данните и тази точност или неточност не може да бъде проверена, може да се направи обозначаване на тази част от данните.

#### Член 19

##### Право на обезщетение

1. Всяко лице, което е претърпяло вреди в резултат на незаконосъобразна операция по обработване или на действие, което е несъвместимо с националните разпоредби, приети съгласно настоящото рамково решение, има право да получи обезщетение за претърпените вреди от администратора или от друг компетентен съгласно националното право орган.

2. Когато компетентен орган на държава-членка е предал лични данни, получателят, в контекста на своята отговорност по отношение на увредената страна в съответствие с националното право, не може да използва в своя защита неточността на предадените данни. Ако получателят изплати обезщетение за причинените вреди вследствие използване на неправилно предадени данни, предаващият компетентен орган възстановява на получателя сумата, изплатена за вредите, като отчита всякаква евентуална вина на получателя.

#### Член 20

##### Средства за правна защита

Без да се засягат каквито и да е административни средства за защита, които могат да бъдат предвидени преди сезиране на съдебния орган, субектът на данните има право на правна защита срещу всякакво нарушение на правата, гарантирани му съгласно приложимото национално право.

#### Член 21

##### Поверителност на обработването

1. Всяко лице, което има достъп до лични данни, попадащи в обхвата на настоящото рамково решение, може да обработва такива данни единствено ако това лице е член на компетентния орган или действа по негови указания, освен ако не е задължено по закон да направи това.

2. Лицата, работещи за компетентен орган на държава-членка, са обвързани с всички разпоредби относно защитата на данните, които се прилагат за въпросния компетентен орган.

#### Член 22

##### Сигурност на обработването

1. Държавите-членки предвиждат, че компетентните органи трябва да прилагат подходящи технически и организационни мерки за защита на личните данни срещу случайно или незаконосъобразно унищожаване или случайна загуба, промяна, неразрешено разкриване или достъп, по-специално когато обработването е свързано с предаване по мрежа или предоставяне

чрез даване на пряк автоматизиран достъп, както и срещу всякакви други незаконосъобразни форми на обработка, като отчитат по-специално рисковете от обработването и естеството на данните, които следва да бъдат защитени. Предвид съвременното ниво на развитие и разходите по прилагането им, тези мерки гарантират ниво на сигурност, съответстващо на рисковете, свързани с обработването и с естеството на данните, които трябва да бъдат защитени.

2. По отношение на автоматизираното обработване на данни всяка държава-членка прилага мерки, имащи за цел:

- a) отказване на достъп на неупълномощени лица до оборудването за обработка на данни, което се използва за обработка на лични данни (контрол на достъпа до оборудване);
- b) препятстване на неразрешеното четене, копиране, изменение или отстраняване на информационни носители (контрол на информационните носители);
- v) препятстване на неразрешеното въвеждане на данни и неразрешената проверка, изменение или заличаване на съхранени лични данни (контрол на съхраняването);
- г) препятстване на използването на автоматизирани системи за обработка на данни от неупълномощени лица чрез устройства за предаване на информация (контрол на ползвателите);
- д) гарантиране, че лицата, на които е разрешено да използват автоматизираната система за обработка на данни, имат достъп само до данните, които са обхванати от тяхното разрешение за достъп (контрол на достъпа до данни);
- e) гарантиране на възможността за проверка и установяване на това на кого са били или могат да бъдат изпращани или предоставяни лични данни чрез оборудване за предаване на данни (контрол на комуникацията);
- ж) гарантиране на възможността за последваща проверка и установяване какви лични данни са били въведени в автоматизираните системи за обработка на данни, както и кога и от кого са били въведени (контрол на въвеждането);
- з) препятстване на неразрешено четене, копиране, изменение и заличаване на лични данни в хода на тяхното предаване или при пренасянето на информационни носители (контрол на пренасянето);
- и) гарантиране на възстановяването на инсталираните системи в случай на прекъснато функциониране (възстановяване);
- й) гарантиране на изпълнението на функциите на системата, докладването за появили се във функциите дефекти (надеждност), както и недопускане на увреждане на съхраняваните данни вследствие от неправилно функциониране на системата (цялост).

3. Държавите-членки предвиждат, че обработващите личните данни могат да бъдат назначени само след като гарантират, че спазват изискваните технически и организационни мерки по параграф 1 и спазват указанията по член 21. Компетентният орган извършва наблюдение върху обработващия личните данни в това отношение.

4. Лични данни могат да бъдат обработвани от обработващ личните данни само въз основа на правен акт или писмен договор.

#### Член 23

##### Предварителна консултация

Държавите-членки гарантират, че с компетентните национални надзорни органи са проведени консултации преди обработването на лични данни, които ще съставляват част от нова система за класиране, която предстои да бъде създадена, когато:

- a) се обработват специалните категории данни, посочени в член 6; или
- б) видът обработка, по-специално използването на нови технологии, механизъм или процедури, е свързан в противен случай със специфичен риск за основните права и свободи, и по-специално неприкосновеността на личния живот, на субекта на данните.

#### Член 24

##### Санкции

Държавите-членки приемат подходящи мерки, за да гарантират пълното изпълнение на разпоредбите на настоящото рамково решение и в частност установяват ефективни, съразмерни и възпиращи санкции, които да се налагат в случай на нарушаване на разпоредбите, приети в съответствие с настоящото рамково решение.

#### Член 25

##### Национални надзорни органи

1. Всяка държава-членка гарантира, че един или повече обществени органи отговарят за консултирането и следенето на прилагането на нейна територия на разпоредбите, приети от държавите-членки съгласно настоящото рамково решение. Тези органи се ползват с пълна независимост при упражняване на функциите, които са им възложени.

2. В частност на всеки орган следва да бъдат предоставени:

- a) правомощия за разследване, като право на достъп до данни, съставляващи предмет на операциите по обработка, както и правомощия за събиране на цялата информация, необходима за изпълнението на надзорните му функции;
- б) ефективни правомощия за намеса, като например право на изразяване на становища преди извършването на операции по обработване на данни и гарантиране на подходяща публичност на тези становища; правомощия да се разпорежда

за блокиране, заличаване или унищожаване на данни, за налагане на временна или окончателна забрана за обработка, за отпращане на предупреждение или строга забележка на администратора, както и за отнасяне на въпроса до националния парламент или други политически институции;

- в) правомощие да участва в съдебни производства, когато са нарушени националните разпоредби, приети в съответствие с настоящото рамково решение, или да довежда до знанието на съдебните органи това нарушение. Решенията на надзорния орган, които са предмет на жалби, могат да бъдат обжалвани по съдебен ред.

3. Всеки надзорен орган разглежда искове, подадени от което и да е лице, отнасящи се до защитата на неговите права и свободи във връзка с обработването на лични данни. Засегнатото лице следва да бъде уведомено за резултата от иска.

4. Държавите-членки гарантират, че членовете и персоналът на надзорния орган са обвързани с разпоредбите за защита на данните, приложими за въпросния компетентен орган, и че дори и след прекратяване на техните трудови правоотношения са обвързани със задължението за опазване на професионална тайна по отношение на поверителната информация, до която имат достъп.

#### Член 26

##### Отношение към споразумения с трети държави

Настоящото рамково решение не засяга задълженията и ангажиментите на държавите-членки или на Съюза, произтичащи от двустранни и/или многостранни споразумения с трети държави, които съществуват към момента на приемане на настоящото рамково решение.

При прилагането на тези споразумения предаването на трета държава на лични данни, получени от друга държава-членка, се извършва при спазване на член 13, параграф 1, буква в) или параграф 2, както е подходящо.

#### Член 27

##### Оценяване

1. Държавите-членки докладват на Комисията до 27 ноември 2013 г. относно националните мерки, предприети за осигуряване на пълно спазване на настоящото рамково решение, и по-специално по отношение на тези разпоредби, които вече трябва да се спазват, когато данните са събрани. Комисията разглежда по-конкретно последиците от тези разпоредби за обхвата на настоящото рамково решение, както е предвидено в член 1, параграф 2.

2. В едногодишен срок Комисията докладва на Европейския парламент и на Съвета за резултата от оценяването, посочено в параграф 1, и прилага към доклада си всякакви подходящи предложения за изменения на настоящото рамково решение.

**Член 28****Връзка с предишни актове на Съюза**

Когато в актове, приети съгласно дял VI от Договора за Европейския съюз преди датата на влизане в сила на настоящото рамково решение и уреждащи обмена на лични данни между държавите-членки или достъпа на определени органи на държавите-членки до информационни системи, създадени по силата на Договора за създаване на Европейската общност, са въведени специфични условия по отношение използването на такива данни от получаващата държава-членка, тези условия имат предимство пред разпоредбите на настоящото рамково решение относно използването на данни, получени или предоставени от друга държава-членка.

**Член 29****Изпълнение**

1. Държавите-членки вземат необходимите мерки, за да се съобразят с разпоредбите на настоящото рамково решение преди 27 ноември 2010 г.
2. До същата дата държавите-членки предават на генералния секретариат на Съвета и на Комисията текста на разпоредбите, с

които транспонират в тяхното национално законодателство наложените им с настоящото рамково решение задължения, както и информация относно надзорните органи, посочени в член 25. Въз основа на доклад, съставен от Комисията чрез използване на тази информация, Съветът оценява степента, до която държавите-членки са спазили настоящото рамково решение, преди 27 ноември 2011 г.

**Член 30****Влизане в сила**

Настоящото рамково решение влиза в сила на двадесетия ден след публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 27 ноември 2008 година.

За Съвета

Председател

M. ALLIOT-MARIE