РЕШЕНИЕ (ЕС, Евратом) 2015/444 НА КОМИСИЯТА

от 13 март 2015 година

относно правилата за сигурност за защита на класифицираната информация на ЕС

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 249 от него,

като взе предвид Договора за създаване на Европейската общност за атомна енергия, и по-специално член 106 от него,

като взе предвид приложения към Договорите Протокол № 7 за привилегиите и имунитетите на Европейските общности, и по-специално член 18 от него,

като има предвид, че:

(1) разпоредбите за сигурност на Комисията относно защитата на класифицираната информация на Европейския съюз (КИЕС) трябва да бъдат преразгледани и актуализирани като бъде взето предвид институционалното, организационното, оперативното и технологичното развитие.

(2) Европейската комисия е сключила с правителствата на Белгия, Люксембург и Италия споразумения по въпросите на сигурността за основните си обекти ([1]).

(3) Комисията, Съветът и Европейската служба за външна дейност са решени да прилагат равностойни стандарти за сигурност за защита на КИЕС.

(4) Важно е, когато е подходящо, Европейският парламент и други институции, агенции, органи или служби на ЕС да бъдат свързани с принципите, стандартите и правилата за защита на класифицирана информация, които са необходими, за да се защитят интересите на Съюза и на неговите държавите членки.

(5) Рискът по отношение на КИЕС се управлява като процес. Този процес има за цел да се определят познатите рискове за сигурността, да се набележат мерки за сигурност с оглед свеждане на такива рискове до приемливо ниво съгласно изложените в настоящото решение основни принципи и минимални стандарти и да се прилагат тези мерки в съответствие с концепцията за дълбочинна защита. Ефективността на тези мерки подлежи на постоянна оценка.

(6) В рамките на Комисията физическа сигурност по отношение на защитата на класифицирана информация означава прилагане на физически и технически защитни мерки за предотвратяване на неразрешен достъп до КИЕС.

(7) Управлението на КИЕС представлява прилагане на административни мерки за контрол на КИЕС през жизнения ѝ цикъл в допълнение към мерките, предвидени в глави 2, 3 и 5 на настоящото решение, като по този начин се съдейства за възпиране, разкриване и възстановяване на такава информация при умишлено или случайно компрометиране или загуба. Такива мерки се отнасят по-конкретно до създаването, съхраняването, регистрирането, копирането, превеждането, намаляването на нивото на класификация, декласифицирането, пренасянето и унищожаването на КИЕС и допълват общите правила относно управлението на документите на Комисията (Решения 2002/47/ЕО ([2]), ЕОВС, Евратом и 2004/563/ЕО, Евратом ([3])).

([1]) Вж. Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité от 31 декември 2004 г., Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois от 20 януари 2007 г. и Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale от 22 юли 1959 г.

([2]) Решение 2002/47/ЕО, ЕОВС, Евратом на Комисията от 23 януари 2002 г. за изменение на нейния процедурен правилник (ОВ L 21, 24.1.2002 г., стр. 23.).

([3]) Решение 2004/563/ЕО, Евратом на Комисията от 7 юли 2004 г. за изменение на нейния процедурен правилник (ОВ L 251, 27.7.2004 г., стр. 9).

(8) Разпоредбите на настоящото решение не засягат:

а) Регламент (Евратом) № 3 ([1]);

б) Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета ([2]);

в) Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета ([3]);

г) Регламент (ЕИО, Евратом) № 354/83 на Съвета ([4]),

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

ГЛАВА 1

ОСНОВНИ ПРИНЦИПИ И МИНИМАЛНИ СТАНДАРТИ

Член 1

Определения

За целите на настоящото решение се прилагат следните определения:

(1) „Служба на Комисията“ означава всяка генерална дирекция или служба на Комисията или всеки кабинет на член на Комисията.

(2) „Криптографски (крипто) материал“ означава криптографски алгоритми, криптографски хардуерни и софтуерни модули и продукти, включително данни за прилагането им и свързаните с това документация и материали, служещи за заключване/отключване на информацията.

(3) „Декласификация“ означава премахване на всякаква класификация за сигурност.

(4) „Защита в дълбочина“ означава прилагане на съвкупност от мерки за сигурност, организирани под формата на многослойна защита.

(5) „Документ“ означава всяка записана информация, независимо от нейната физическа форма или характеристики.

(6) „Понижаване нивото на класификация“ означава понижаване на нивото на класификацията за сигурност.

(7) „Работа с КИЕС“ означава всички възможни действия, на които може да бъде подложена КИЕС през жизнения ѝ цикъл. Това включва нейното създаване, регистриране, обработване, пренасяне, понижаването на нивото на класификацията ѝ, декласификацията ѝ и нейното унищожаване. По отношение на комуникационните и информационните системи (КИС) това включва и нейното събиране, излагане, предаване и съхраняване.

(8) „Притежател“ означава надлежно оправомощено лице с добре установена „необходимост да се знае“, което притежава дадена КИЕС и носи съответно отговорност за нейната защита.

(9) „Правила за прилагане“ означава всеки набор от правила или насоки за сигурност, приети в съответствие с Глава 5 от Решение 2015/443 (ЕС, Евратом) на Комисията ([5]).

(10) „Материал“ означава документ, носител на данни или машина или оборудване, който е вече създаден или е в процес на създаване.

(11) „Създател“ означава институция, агенция или орган на ЕС, както и държава членка, трета държава или международна организация, под чието ръководство е създадена и/или въведена в структурите на ЕС класифицирана информация.

(12) „Помещения“ означава всяко недвижимо или равнозначно на него имущество и собственост на Комисията.

([1]) Регламент (Евратом) № 3 от 31 юли 1958 г. за прилагане на член 24 от Договора за създаване на Европейската общност за атомна енергия (ОВ 17, 6.10.1958 г., стр. 406/58).

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

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

([4]) Регламент (ЕИО, Евратом) № 354/83 на Съвета от 1 февруари 1983 г. относно отваряне за обществеността на историческите архиви на Европейската икономическа общност и на Европейската общност за атомна енергия (ОВ L 43, 15.2.1983 г., стр. 1).

([5]) Решение 2015/443 (ЕС, Евратом) на Комисията от 13 март 2015 г. относно сигурността в Комисията (вж. страница 41 от настоящия Официален вестник).

(13) „Процес на управление на риска за сигурността“ означава целият процес на идентифициране, контрол и свеждане до минимум на неопределени събития, които могат да засегнат сигурността на дадена организация или на която и да е от използваните от нея системи. Този процес обхваща всички дейности, свързани с риска, включително оценка, третиране, приемане и съобщаване.

(14) „Правилник за длъжностните лица“ означава Правилникът за длъжностните лица на Европейския съюз и Условията за работа на другите служители на Европейския съюз, приет с Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета ([1]);

(15) „Заплаха“ означава потенциална причина за нежелан инцидент, който може да доведе до вредни последици за дадена организация или за която и да е от използваните от нея системи; такива заплахи могат да бъдат инцидентни или умишлени (злонамерени) и се характеризират с елементи на заплаха, потенциални цели и методи за нападение.

(16) „Уязвимост“ означава слабост от каквото и да било естество, която може да бъде използвана от една или повече заплахи. Уязвимостта може да бъде пропуск или да бъде свързана със слабости в режима на контрол, свързани с неговата строгост, всеобхватност или съгласуваност, и може да има технически, процедурен, физически, организационен или оперативен характер.

Член 2

Предмет и приложно поле

1. С настоящото решение се установяват основните принципи и минималните стандарти за сигурност с оглед защитата на КИЕС.

2. Настоящото решение се прилага от всички служби на Комисията и във всички помещения на Комисията.

3. Независимо от евентуални конкретни указания, касаещи специфични групи служители, настоящото решение се прилага за членовете на Комисията, служителите на Комисията, попадащи в обхвата на Правилника за длъжностните лица и Условията за работа на другите служители на ЕС, командированите национални експерти (КНЕ) в Комисията, доставчиците на услуги и техните служители, стажантите и всички лица, имащи достъп до сгради или други активи на Комисията или до информация, с която Комисията работи.

4. Разпоредбите на настоящото решение не засягат Решение 2002/47/ЕО (ЕОВС, Евратом) и Решение 2004/563/ЕО (Евратом).

Член 3

Определение за КИЕС, нива на класификация за сигурност и грифове

1. „Класифицирана информация на Европейския съюз“ (КИЕС) означава всяка информация или материал, носещи гриф за сигурност на ЕС, неразрешеното разкриване на които би могло да увреди в различна степен интересите на Европейския съюз или на една или повече от държавите членки.

2. Всяка КИЕС се класифицира на някое от следните нива:

а) TRÈS SECRET UE/EU TOP SECRET: информация и материали, неразрешеното разкриване на които би могло да увреди изключително сериозно съществените интереси на Европейския съюз или на една или повече от държавите членки.

б) SECRET UE/EU SECRET: информация и материали, неразрешеното разкриване на които би могло да увреди сериозно съществените интереси на Европейския съюз или на една или повече от държавите членки.

в) CONFIDENTIEL UE/EU CONFIDENTIAL: информация и материали, неразрешеното разкриване на които би могло да увреди съществените интереси на Европейския съюз или на една или повече от държавите членки.

г) RESTREINT UE/EU RESTRICTED: информация и материали, неразрешеното разкриване на които би се отразило неблагоприятно на интересите на Европейския съюз или на една или повече от държавите членки.

3. КИЕС носи гриф за сигурност в съответствие с параграф 2. Може да се добавят и допълнителни обозначения, които не представляват гриф за сигурност, но имат за цел да се посочи сферата на дейност, до която се отнася класифицираната информация, да се идентифицира създателят ѝ, да се ограничи разпределението ѝ, да се ограничи ползването ѝ или да се обозначи доколко тази информация подлежи на предоставяне.

([1]) Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета от 29 февруари 1968 година относно определянето на статута на длъжностните лица на Европейските общности и условията за работа на другите служители, и за създаване на конкретно особени мерки за временно прилагане към длъжностните лица на Комисията (условия за работа на другите служители) (ОВ L 56, 4.3.1968 г., стр. 1).

Член 4

Управление на класификацията

1. Всеки член на Комисията или служба на Комисията прави необходимото създаваната от тях КИЕС да бъде подходящо класифицирана, ясно обозначена като КИЕС и да запазва нивото си на класификация само докато това е необходимо.

2. Без да се засяга член 26 по-долу, нивото на класификация на КИЕС не се понижава или тя не се декласифицира, нито някой от посочените в член 3, параграф 2 грифове се изменя или премахва без предварителното писмено съгласие на създателя на информацията.

3. Където това е подходящо, в съответствие с член 60 по-долу се приемат правила за прилагане по отношение на КИЕС, включително практически насоки за класифициране на информацията.

Член 5

Защита на класифицираната информация

1. На КИЕС се осигурява защита в съответствие с настоящото решение и правилата за неговото прилагане.

2. Притежателят на КИЕС отговаря за нейната защита, в съответствие с разпоредбите на настоящото решение и правилата за неговото прилагане, съгласно правилата, посочени в Глава 4 по-долу.

3. Когато държавите членки въвеждат в структурите или мрежите на Комисията класифицирана информация, обозначена с национален гриф за сигурност, Комисията осигурява защита на тази информация в съответствие с изискванията, приложими към КИЕС на съответстващото ниво, съгласно съдържащата се в Приложение I таблица на съответствията на нивата на класификация за сигурност.

4. За даден масив от КИЕС може да се наложи защита на по-високо ниво на класификация отколкото на отделните му компоненти.

Член 6

Управление на риска за сигурността

1. Мерките за сигурност за защита на КИЕС за целия ѝ жизнен цикъл съответстват по-конкретно на нивото на класификацията ѝ за сигурност, формата и обема на информацията или материалите, местоположението и конструкцията на структурите, в които се намира КИЕС, както и оценката на местно ниво на риска от злонамерени и/или престъпни действия, включително шпионаж, саботаж и тероризъм.

2. Плановете за действие при извънредни ситуации отчитат необходимостта от защита на КИЕС в извънредни ситуации, за да се предотврати неразрешен достъп, разкриване или загуба на интегритета или наличността.

3. В плановете за непрекъснатост на дейността на всички служби се включват мерки за предотвратяване и възстановяване с оглед да се намали въздействието на сериозни системни грешки или инциденти при работа с КИЕС и нейното съхранение.

Член 7

Прилагане на настоящото решение

1. Където това е необходимо, в съответствие с член 60 по-долу се приемат правила за прилагане в допълнение или в подкрепа на настоящото решение.

2. Службите на Комисията предприемат всички необходими мерки в рамките на техните правомощия, за да гарантират прилагането на настоящото решение и на съответните правила за прилагане при работа с КИЕС или при нейното съхраняване.

3. Мерките за сигурност, предприемани при прилагането на настоящото решение съответстват на принципите на сигурността в Комисията, заложени в член 3 на Решение 2015/443 (ЕС, Евратом).

4. Генералният директор на ГД „Човешки ресурси и сигурност“ създава орган по сигурността на Комисията в рамките на ГД „Човешки ресурси и сигурност“. Органът по сигурността на Комисията изпълнява задълженията, възложени му с настоящото решение и правилата за неговото прилагане.

5. Местният служител по сигурността (МСС) на всяка служба на Комисията, посочен в член 20 на Решение 2015/443 (ЕС, Евратом), изпълнява следните общи дейности по защитата на КИЕС в съответствие с настоящото решение, в тясно сътрудничество с генералния директор на ГД „Човешки ресурси и сигурност“:

а) управлява исканията за разрешаване на достъп до класифицирана информация на служители;

б) допринася за обученията и инструктажите в областта на сигурността;

в) осъществява надзор върху ръководителя на регистратурата на съответната служба;

г) докладва за нарушения на сигурността и компрометиране на КИЕС;

д) съхранява резервни ключове с писмено описание на всяка комбинация;

е) изпълнява други задачи, свързани със защитата на КИЕС или определени в правилата за прилагане.

Член 8

Нарушения на сигурността и компрометиране на КИЕС

1. До нарушение на сигурността се стига в резултат на действие или бездействие от физическо лице, което противоречи на правилата за сигурност, установени в настоящото решение и правилата за неговото прилагане.

2. Компрометиране на КИЕС е налице когато в резултат от нарушение на сигурността тя бъде изцяло или частично разкрита пред неоправомощени лица.

3. Всяко нарушение на сигурността или подозрение за такова нарушение се докладва незабавно на органа по сигурността на Комисията.

4. Когато е известно или когато има достатъчно основания да се приеме, че КИЕС е компрометирана или изгубена, се осъществява проучване за надеждност в съответствие с член 13 на Решение 2015/443 (ЕС, Евратом).

5. Предприемат се всички необходими мерки за:

а) информиране на създателя на информацията;

б) осигуряване на разследване на случая от служители, които нямат непосредствено отношение към нарушението, с оглед установяване на фактите;

в) извършване на оценка на потенциалните вреди, причинени на интересите на Съюза или на държавите членки;

г) предприемане на подходящи мерки за предотвратяване на повторно нарушение; и

д) уведомяване на съответните органи за предприетите действия.

6. На всяко лице, отговорно за нарушение на правилата за сигурност, установени в настоящото решение, могат да бъдат наложени дисциплинарни мерки в съответствие с Правилника за длъжностните лица. Всяко лице, отговорно за компрометиране или загуба на КИЕС, подлежи на дисциплинарно и/или съдебно производство в съответствие с приложимите закони, правила и подзаконови актове.

ГЛАВА 2

МЕРКИ ЗА СИГУРНОСТ ПО ОТНОШЕНИЕ НА ПЕРСОНАЛА

Член 9

Определения

За целите на настоящата глава се прилагат следните определения:

(1) „Разрешение за достъп до КИЕС“ означава решение на органа по сигурността на Комисията, взето въз основа на уверение, предоставено от компетентен орган на държава членка, че дадено длъжностно лице на Комисията, друг служител или командирован национален експерт може да получи достъп до КИЕС на определено ниво (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо) до конкретна дата, при условие че бъде установена „необходимост да се знае“ за това лице и то е преминало през съответен инструктаж за своите отговорности; за лицето, отговарящо на това описание, се казва, че има „издадено разрешение за достъп“.

(2) „Издаване на разрешение за достъп на служител“ означава прилагане на мерки за гарантиране, че достъп до КИЕС се предоставя единствено на лица, които:

а) е необходимо да знаят;

б) са получили разрешение за достъп за съответното ниво, когато е необходимо, и

в) са преминали през инструктаж за своите отговорности.

(3) „Разрешение за достъп на служител“ (РДС) означава изявление на компетентния орган на държава членка, което се прави след приключване на проучване за надеждност, извършено от компетентните органи на държавата членка, с което се удостоверява, че дадено лице може да получи достъп до КИЕС на определено ниво (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо) до конкретна дата, при условие че бъде установена „необходимост да се знае“ за това лице и то е преминало през съответен инструктаж за своите отговорности.

(4) „Удостоверение за разрешение за достъп на служител“ (УРДС) означава удостоверение, издадено от компетентен орган, с което се удостоверява, че дадено лице притежава валидно удостоверение за разрешение за достъп или издадено от органа по сигурността на Комисията разрешение за достъп, в което се посочва нивото на класификация на КИЕС, до което лицето може да има достъп (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), датата, до която е валидно съответното удостоверение или разрешение, и датата, на която изтича валидността на самото удостоверение.

(5) „Проучване за надеждност“ означава процедури за проучване, извършвани от компетентния орган на държава членка в съответствие с нейните национални законови и подзаконови актове с цел да се получи уверение, че няма известна неблагоприятна информация, която да попречи на дадено лице да бъде издадено разрешение за достъп до определено ниво на класификация (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо).

Член 10

Основни принципи

1. Физическо лице получава достъп до класифицирана информация само след като:

(1) бъде установена неговата „необходимост да знае“;

(2) е преминало инструктаж за правилата за сигурност за защита на КИЕС и съответните стандарти и насоки за сигурност и е приело своята отговорност за защитата на такава информация;

(3) е проучено за надеждност за съответното ниво или е съответно надлежно оправомощено по силата на изпълняваните от него функции в съответствие с националните законови и подзаконови актове;

2. Всички лица, на които за изпълнение на служебните задължения може да е необходим достъп до КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, преминават проучване за надеждност за съответното ниво, преди да им бъде предоставен достъп до такава КИЕС. Засегнатото лице декларира в писмен вид, че е съгласно да бъде подложено на проучване за надеждност за издаване на разрешение за достъп. Липсата на подобно съгласие означава, че лицето не може да бъде назначено да изпълнява длъжност, функция или задача, включваща достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо.

3. Процедурите за проучване на персонала за надеждност имат за цел да се определи дали може да се даде разрешение за достъп до КИЕС на дадено физическо лице, като се имат предвид неговата лоялност и надеждност.

4. Лоялността и надеждността на дадено лице за целите на издаването на разрешение за достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се определят чрез провеждане на проучване за надеждност от компетентните органи на държава членка в съответствие с нейните национални законови и подзаконови актове.

5. Органът по сигурността на Комисията единствен отговаря за връзките с националните органи за сигурност (НОС) или други компетентни национални органи в контекста на всички въпроси, свързани с проучванията за надеждност. Всички контакти между службите на Комисията и НОС и други компетентни органи се осъществяват посредством органа по сигурността на Комисията.

Член 11

Процедура за издаване на разрешение за достъп

1. Всеки генерален директор или ръководител на служба в рамките на Комисията определя длъжностите в неговата служба, за които заемащите ги лица трябва да имат достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, за да изпълняват своите задължения и поради това е необходимо да им бъде издадено разрешение за достъп.

2. Непосредствено след като бъде установено, че дадено лице предстои да бъде назначено на длъжност, изискваща достъп до информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, МСС на съответната служба на Комисията уведомява органа по сигурността на Комисията, който предава въпросника за проучването за надеждност на лицето, съставен от НОС на държавата членка, чийто гражданин е лицето, назначено в структурите на европейските институции. Лицето декларира в писмен вид съгласието си да бъде подложено на процедурата на проучването за надеждност и в най-кратък срок връща на органа по сигурността на Комисията попълнения въпросник.

3. Органът по сигурността на Комисията препраща попълнения въпросник за проучването за надеждност на НОС на държавата членка, чийто гражданин е лицето, назначено в структурите на европейските институции, с искане за провеждане на проучване за надеждност за нивото на класификация на КИЕС, за което е лицето се нуждае от разрешение за достъп.

4. Когато на органа по сигурността на Комисията стане известна информация от значение за проучването за надеждност на лице, подало искане за разрешение за достъп, органът по сигурността на Комисията уведомява за това съответния НОС в съответствие с приложимите правила и разпоредби.

5. След приключването на проучването за надеждност и във възможно най-кратък срок след като бъде уведомен от съответния НОС за цялостната му оценка на резултатите от проучването за надеждност органът по сигурността на Комисията:

а) може да издаде разрешение за достъп до КИЕС на засегнатото лице и да разреши достъп до КИЕС до съответното ниво на класификация до определена дата, посочена от него, но за не повече от 5 години, когато в резултат от проучването за надеждност се стигне до уверение, че за лицето не са известни неблагоприятни данни, които поставят под въпрос лоялността и надеждността му;

б) когато проучването за надеждност не завърши с такова уверение, уведомява в съответствие с приложимите правила и регламенти засегнатото лице, което може да поиска да бъде изслушано от органа по сигурността на Комисията, който на свой ред може да поиска от съответния НОС да предостави повече информация в съответствие с националните му законови и подзаконови актове. В случай, че резултатите от проучването за надеждност бъдат потвърдени, разрешение за достъп до КИЕС не се издава.

6. Проучването за надеждност заедно с получените резултати се подчиняват на действащите законови и подзаконови актове на съответната държава членка в тази област, включително на актовете, отнасящи се до обжалването. Решенията на органа по сигурността на Комисията подлежат на обжалване в съответствие с Правилника за длъжностните лица.

7. Комисията приема разрешенията за достъп до КИЕС, издадени от всяка друга институция, орган или агенция на Съюза, при условие че тези разрешения все още са валидни. Разрешението обхваща всяка задача, възложена на съответното лице в рамките на Комисията. Институцията, органът или агенцията на Съюза, в която лицето започва работа, уведомява съответния НОС за промяната на работодателя.

8. Ако лицето не започне работа в рамките на 12 месеца от съобщаването на резултата от проучването за надеждност на органа по сигурността на Комисията или когато е налице прекъсване от 12 месеца, през които то не е било на работа в Комисията или в друга институция, орган или агенция на Съюза или в националната администрация на държава членка, органът по сигурността на Комисията се обръща към съответния НОС за потвърждаване на валидността и целесъобразността на разрешението за достъп.

9. Когато на органа по сигурността на Комисията стане известна информация, че физическо лице, притежател на валидно разрешение за достъп, представлява риск за сигурността, органът по сигурността уведомява за това компетентния НОС в съответствие с приложимите правила и разпоредби.

10. Когато НОС уведоми органа по сигурността на Комисията, че оттегля уверение, дадено в съответствие с параграф 5, буква а) за лице, разполагащо с валидно разрешение за достъп до КИЕС, органът по сигурността на Комисията може да отправи искане за всякакъв вид пояснения, които НОС може да предостави съгласно националните законови и подзаконови актове. Ако неблагоприятната информация бъде потвърдена от съответния НОС, разрешението за достъп се оттегля и лицето се изключва от достъп до КИЕС и от длъжности, където е възможен такъв достъп или където то може да представлява опасност за сигурността.

11. Всяко решение за отнемане или временно преустановяване на разрешение за достъп до КИЕС на всяко лице, попадащо в приложното поле на настоящото решение и, когато това е уместно, основанията за него, се съобщават на засегнатото лице, което може да поиска да бъде изслушано от органа по сигурността на Комисията. Информацията, предоставена от НОС, се подчинява на действащите законови и подзаконови актове на съответната държава членка. Решенията, взети в тази връзка от органа по сигурността на Комисията, подлежат на обжалване в съответствие с Правилника за длъжностните лица.

12. Службите на Комисията се уверяват, че националните експерти, командировани в тях на длъжност, изискваща разрешение за достъп до КИЕС, са предоставили преди назначаването си валидно РДС или удостоверение за разрешение за достъп на служител (УРДС), в съответствие с националните законови и подзаконови актове, на органа по сигурността на Комисията, който на основание на това разрешение издава разрешение за достъп до КИЕС до нивото на класификация, посочено в националното разрешение за достъп, като валидността му не може да надвишава продължителността на командироването.

Достъп до КИЕС на лица, надлежно оправомощени по силата на изпълняваните от тях функции

13. Членовете на Комисията, които имат достъп до КИЕС по силата на изпълняваните от тях функции въз основа на Договора преминават инструктаж във връзка със задълженията им по защитата на КИЕС.

Регистри на удостоверения за надеждност и разрешения за достъп

14. Документите, свързани с проучванията за надеждност и издадените разрешения за достъп до КИЕС се съхраняват от органа по сигурността на Комисията в съответствие с настоящото решение. Като минимум регистрите съдържат информация за нивото на КИЕС, до което може да бъде даден достъп на лицето, датата на издаване на разрешението за достъп и срокът му на валидност.

15. Органът по сигурността на Комисията може да издаде УРДС, в което са посочени нивото на класификация на КИЕС, до което лицето може да получи достъп (CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо), срокът на валидност на съответното разрешение за достъп до КИЕС и датата на изтичане на валидността на самото удостоверение.

Подновяване на разрешението за достъп

16. След първоначалното издаване на разрешение за достъп и при условие че лицето не е прекъсвало работата си в Европейската комисия или в друга институция, орган или агенция на Съюза и все още има нужда от достъп до КИЕС, разрешението за достъп до КИЕС се подлага на преразглеждане с цел неговото подновяване, което по правило се извършва на всеки пет години, считано от датата на уведомлението за последното проучване за надеждност, въз основа на което е издадено.

17. Органът по сигурността на Комисията може да удължи срока на валидност на издадено разрешение за достъп с до 12 месеца, ако от съответния НОС не е получена неблагоприятна информация в рамките на два месеца, считано от датата на представяне на искането за подновяване и съответния въпросник за проучването за надеждност. В случай, че при изтичането на този 12-месечен срок съответният НОС или компетентен национален орган не е уведомил органа по сигурността на Комисията за своето становище, на лицето се възлагат задачи, за чието изпълнение не е необходимо разрешение за достъп.

Член 12

Инструктажи във връзка с издаването на разрешение за достъп

1. След преминаването на инструктаж във връзка с издаването на разрешение за достъп, организиран от органа по сигурността на Комисията, всички лица, на които е издадено разрешение за достъп декларират писмено, че са запознати със задълженията си по отношение на защитата на КИЕС и последиците от компрометиране на КИЕС. Органът по сигурността на Комисията съхранява тези декларации.

2. Всички лица, които имат разрешение за достъп до КИЕС или от които се изисква да работят с КИЕС, получават първоначална информация и биват впоследствие редовно информирани относно заплахите за сигурността и са длъжни незабавно да докладват на органа по сигурността на Комисията за всеки подход или дейност, които считат за подозрителни или необичайни.

3. Всички лица, които престават да изпълняват задължения, изискващи достъп до КИЕС, биват информирани за задълженията им да продължат да опазват КИЕС, за което при нужда подписват декларация.

Член 13

Временни разрешения за достъп

1. При извънредни обстоятелства, когато това е надлежно оправдано от интереса на работата и до завършване на цялостното проучване за надеждност, органът по сигурността на Комисията, след консултация с НОС на държавата членка, чийто гражданин е лицето и в зависимост от резултата от предварителната проверка за удостоверяване, че няма неблагоприятна информация, може да разреши на лицето временен достъп до КИЕС за изпълнение на конкретни задължения, без това да засяга разпоредбите относно подновяването на разрешенията за достъп. Временното разрешение за достъп до КИЕС има еднократна валидност, която не надвишава шест месеца и не дава право на достъп до информация с ниво на класификация за сигурност TRES SECRET UE/EU TOP SECRET.

2. След като преминат инструктаж в съответствие с член 12, параграф 1, всички лица, на които е издадено временно разрешение за достъп декларират писмено, че са запознати със задълженията си по отношение на защитата на КИЕС и последиците от компрометирането на КИЕС. Органът по сигурността на Комисията съхранява тези декларации.

Член 14

Участие в класифицирани заседания, организирани от Комисията

1. Службите на Комисията, отговарящи за организирането на заседания, на които ще се обсъжда информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо информират чрез своя МСС или чрез организатора на заседанието органа по сигурността на Комисията достатъчно рано за датата, часа, мястото и участниците в такива заседания.

2. При спазване на разпоредбите на член 11, параграф 13 лица, на които е възложено да участват в заседания, организирани от Комисията, на които ще се обсъжда информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, се допускат до участие само след потвърждаване на статуса им на лица с разрешение за достъп. Достъп до такива заседания се отказва на лица, за които на органа по сигурността на Комисията не е представен УРДС или друго доказателство за наличие на разрешение за достъп, както и на участници от Комисията, които не притежават разрешение за достъп.

3. Преди организирането на класифицирано заседание отговорникът за организирането му или МСС на службата на Комисията, която организира заседанието, изискват от външните участници да представят на органа по сигурността на Комисията УРДС или друго доказателство за наличие на разрешение за достъп. Органът по сигурността на Комисията информира МСС или организатора на заседанието за получените УРДС или други доказателства за разрешения за достъп. Когато е приложимо, може да се използва единен списък с имена, който да предоставя съответно доказателство за разрешение за достъп.

4. Когато компетентните органи уведомят органа по сигурността на Комисията за оттегляне на УДС на лице, чиито задължения налагат участието му в заседания, организирани от Комисията, органът по сигурността на Комисията уведомява МСС на службата на Комисията, отговорна за организирането на заседанието.

Член 15

Потенциален достъп до КИЕС

Куриерите, охранителите и придружителите преминават през проучване за надеждност на съответното ниво или се проучват по други начини в съответствие с националните законови и подзаконови актове, биват инструктирани относно процедурите за сигурност за защита на КИЕС и получават указания за задълженията им във връзка със защитата на поверената им информация.

ГЛАВА 3

ФИЗИЧЕСКА СИГУРНОСТ ЗА ЗАЩИТА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ

Член 16

Основни принципи

1. Мерките за физическа сигурност са предназначени за предотвратяване на тайно или насилствено проникване на нарушител, за възпиране, препятстване и разкриване на неразрешени действия и за даване на възможност за категоризиране на персонала по отношение на достъпа до КИЕС на основата на принципа „необходимост да се знае“. Тези мерки се определят чрез процедура за оценка на риска, в съответствие с настоящото решение и правилата за неговото прилагане.

2. По-конкретно, мерките за физическа сигурност са предназначени да предотвратяват неразрешен достъп до КИЕС, като:

а) гарантират, че работата с КИЕС и нейното съхранение се извършват по подходящ начин;

б) дават възможност за разграничаване на служителите по отношение на достъпа до КИЕС на основание „необходимост да се знае“ и, където това е подходящо, според вида на разрешението им за достъп;

в) възпират, препятстват и разкриват неразрешени действия; и

г) предотвратяват или забавят тайно или насилствено проникване на нарушители.

3. Мерки за физическа сигурност се въвеждат във всички помещения, сгради, офиси, зали и други зони, в които се работи с КИЕС или се съхранява такава, включително в зони, в които се помещават комуникационни и информационни системи съгласно определението в Глава 5.

4. Зони, в които се съхранява КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо, се определят като зони за сигурност в съответствие с настоящата глава и се одобряват от органа по акредитиране сигурността на Комисията.

5. За защита на КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се използват единствено устройства или оборудване одобрени от органа по сигурността на Комисията.

Член 17

Изисквания и мерки за физическа сигурност

1. Мерките за физическа сигурност се избират въз основа на оценка на заплахите, изготвена от органа по сигурността на Комисията, при необходимост в консултация с други служби на Комисията, други институции, агенции или органи на Съюза и/или компетентните органи на държавите членки. Комисията прилага процес на управление на риска за защита на КИЕС в помещенията си, за да гарантира, че съобразно оценения риск се осигурява съразмерно равнище на физическа защита. В процеса на управление на риска се вземат предвид всички необходими фактори, и по-специално:

а) нивото на класификация на КИЕС;

б) формата и обемът на КИЕС, като се отчита, че за големи количества или масиви от КИЕС може да се наложи прилагане на по-строги защитни мерки;

в) заобикалящата среда и конструкцията на сградите или зоните, в които се съхранява КИЕС; и

г) оценката на заплахите, произтичащи от действия на разузнавателни служби, насочени срещу Съюза, неговите институции, органи или агенции, или държавите членки, както и от саботажи, терористична, подривна или друг вид престъпна дейност.

2. Органът по сигурността на Комисията, като прилага концепцията за защита в дълбочина, определя подходящото съчетание от мерки за физическа сигурност, които да се приложат. За тази цел органът по сигурността на Комисията разработва минимални стандарти, норми и критерии, посочени в правилата за прилагане.

3. Органът по сигурността на Комисията има право да извършва претърсване на влизащите или излизащите, което действа като възпиращ фактор по отношение на неразрешено внасяне на материали или изнасяне на КИЕС от помещения или сгради.

4. При наличие на риск от пренебрегване на КИЕС, било то по случайност, съответните служби на Комисията предприемат подходящи мерки, определени от органа по сигурността на Комисията, за справяне с този риск.

5. Изискванията за физическа сигурност и функционалните спецификации на нови съоръжения се определят със съгласието на органа по сигурността на Комисията като част от планирането и проектирането на тези съоръжения. Изискванията за физическа сигурност на съществуващи съоръжения се прилагат в съответствие с минималните стандарти, нормите и критериите, посочени в правилата за прилагане.

Член 18

Оборудване за физическа защита на КИЕС

1. За физическа защита на КИЕС се създават два вида физически защитени зони:

а) административни зони; и

б) зони за сигурност (включително технически зони за сигурност).

2. Органът по акредитиране на сигурността на Комисията определя дали дадена зона отговаря на изискванията за административна зона, зона за сигурност или техническа зона за сигурност.

3. За административните зони:

а) се определя видимо очертан периметър, който да позволява проверка на лицата и при възможност — на превозните средства;

б) непридружен достъп се разрешава само на лица, надлежно оправомощени от органа по сигурността на Комисията или друг компетентен орган; и

в) всички останали лица се придружават по всяко време или подлежат на равностойни проверки.

4. За зоните за сигурност:

а) се определя видимо очертан и защитен периметър, чрез който се контролират всички влизания и излизания чрез пропуски или система за индивидуално разпознаване;

б) достъп без придружител се предоставя само на лица, които имат разрешение за достъп и са конкретно оправомощени да влизат в зоната на основание „необходимост да се знае“;

в) всички останали лица се придружават по всяко време или подлежат на равностойни проверки.

5. Когато влизането в зона за сигурност представлява на практика пряк достъп до класифицираната информация в нея, се прилагат следните допълнителни изисквания:

а) обозначава се ясно най-високото ниво на класификация за сигурност на информацията, която обикновено се намира в зоната;

б) всички посетители трябва да имат конкретно разрешение за влизане в зоната, те се придружават непрекъснато и са преминали през съответното проучване за надеждност, освен ако не са взети мерки да се гарантира, че достъпът до КИЕС е невъзможен.

6. Зони за сигурност, защитени срещу подслушване, се определят за технически зони за сигурност. Прилагат се следните допълнителни изисквания:

а) такива зони се оборудват с алармени системи против проникване (IDS), стоят заключени, когато не се ползват, и са под охрана, когато се ползват. Контролът на ключовете за тях се осъществява в съответствие с член 20;

б) всички лица и материали, влизащи в такива зони, подлежат на контрол;

в) органът по сигурността на Комисията осъществява редовни физически и/или технически проверки на тези зони. Такива проверки се извършват и след всяко неразрешено влизане или при подозрение за такова влизане; и

г) в такива зони няма неразрешени линии за комуникации, неразрешени телефони или други неразрешени комуникационни средства и електрическо или електронно оборудване.

7. Независимо от параграф 6, буква г), преди да се използват в зони, в които се провеждат заседания или се извършва дейност, включваща работа с информация с ниво на класификация за сигурност SECRET UE/EU SECRET и по-високо, и където степента на заплаха за КИЕС се оценява като висока, комуникационните средства и електрическото или електронното оборудване най-напред се проверяват от органа по сигурността на Комисията, за да се гарантира, че с това оборудване не може да се предаде, неволно или неправомерно, разбираема информация отвъд периметъра на зоната за сигурност.

8. Зоните за сигурност, в които няма денонощно присъствие на дежурен персонал, се проверяват, когато това е уместно, в края на установеното работно време и на произволни интервали извън установеното работно време, освен ако не е инсталирана алармена система против проникване.

9. Зони за сигурност и технически зони за сигурност могат да бъдат временно създадени в рамките на административна зона за целите на класифицирано заседание или други подобни цели.

10. МСС на съответната служба на Комисията изготвя оперативни процедури за сигурност (ОПС) за всяка зона за сигурност, за която отговаря, като посочва, в съответствие с разпоредбите на настоящото решение и правилата за неговото прилагане:

а) нивото на класификация на КИЕС, с която може да се работи и която може да се съхранява в зоната;

б) мерките за наблюдение и защита, които да се поддържат;

в) лицата, които имат право на непридружен достъп до зоната на основание „необходимост да се знае“ и разрешение за достъп;

г) ако е уместно, процедури за придружаване или за защита на КИЕС, когато се разрешава достъп на други лица до зоната;

д) всякакви други подходящи мерки и процедури.

11. В рамките на зоните за сигурност се изграждат блиндирани помещения. Стените, подовете, таваните, прозорците и вратите с ключалки се одобряват от органа по сигурността на Комисията и осигуряват защита, равностойна на тази на сейф от категорията, одобрена за съхранение на КИЕС със същото ниво на класификация за сигурност.

Член 19

Физически защитни мерки за работна с КИЕС и нейното съхранение

1. С КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED може да се работи:

а) в зона за сигурност,

б) в административна зона, при условие че КИЕС е защитена срещу достъп от страна на неоправомощени лица, или

в) извън зона за сигурност или административна зона, при условие че притежателят пренася КИЕС в съответствие с член 31 и се е ангажирал да спазва компенсаторните мерки, посочени в мерките за прилагане, за да се гарантира, че КИЕС е защитена срещу достъп от страна на неоправомощени лица.

2. КИЕС с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED се съхранява в подходящи заключващи се офис мебели в административна зона или в зона за сигурност. Тя може да се съхранява временно извън административна зона или зона за сигурност, при условие че притежателят се е ангажирал да спазва компенсаторните мерки, посочени в правилата за прилагане.

3. С КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET може да се работи:

а) в зона за сигурност;

б) в административна зона, при условие че КИЕС е защитена срещу достъп от страна на неоправомощени лица; или

в) извън зона за сигурност или административна зона, при условие че притежателят:

i) се е ангажирал да спазва компенсаторните мерки, посочени в правилата а прилагане, за да се гарантира, че КИЕС е защитена срещу достъп от страна на неоправомощени лица;

ii) непрекъснато контролира лично КИЕС; и

iii) в случай че документите са на хартиен носител, е уведомил за това съответната регистратура.

4. КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се съхранява в зона за сигурност в сейф или блиндирано помещение.

5. С КИЕС с ниво на класификация за сигурност TRES SECRET UE/EU TOP SECRET се работи в зона за сигурност, създадена и поддържана от органа по сигурността на Комисията и акредитирана за това ниво на класификация от органа по акредитиране на сигурността на Комисията.

6. КИЕС с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се съхранява в зона за сигурност, акредитирана за това ниво на класификация от органа по акредитиране на сигурността на Комисията, при някое от следните условия:

а) в сейф, съобразно разпоредбите на член 18, с една или повече от следните допълнителни мерки за контрол:

(1) постоянна защита или проверки от охранители или дежурни служители с разрешение за достъп;

(2) одобрена алармена система против проникване, в съчетание със служители за охрана и реагиране;

или

б) в блиндирани помещения, оборудвани с алармени системи против проникване, в съчетание със служители за охрана и реагиране.

Член 20

Контрол на ключовете и комбинациите, използвани за защита на КИЕС

1. Процедурите за контрол на ключовете и шифровите комбинации за офисите, залите, блиндираните помещения и сейфовете се установяват в правилата за прилагане в съответствие с член 60 по-долу. Тези процедури осигуряват защита срещу неразрешен достъп.

2. Шифровите комбинации се запаметяват от възможно най-малък брой лица на основание „необходимост да се знае“. Шифровите комбинации за сейфовете и блиндираните помещения, в които се съхранява КИЕС, се променят:

а) при получаване на нов сейф;

б) винаги когато има смяна на служител, на когото е известна комбинацията;

в) в случай на компрометиране или подозрение за компрометиране на информация;

г) когато дадена ключалка е преминала през поддръжка или ремонт; и

д) най-малко на всеки 12 месеца.

ГЛАВА 4

УПРАВЛЕНИЕ НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС

Член 21

Основни принципи

1. Всички документи, представляващи КИЕС, се управляват в съответствие с политиката на Комисията по отношение на управлението на документацията и впоследствие се регистрират, завеждат, съхраняват и накрая се унищожават, прави им се извадка или се прехвърлят в историческия архив в съответствие с общия за Комисията списък за съхранение на досиета на Европейската комисия.

2. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо се регистрира за целите на сигурността преди нейното разпространение и при получаването ѝ. Информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET се регистрира в специални регистратури.

3. В Комисията се създава система от регистратури на КИЕС в съответствие с разпоредбите на член 27.

4. Службите и помещенията на Комисията, в които се работи с КИЕС или се съхранява такава, подлежат на редовни проверки от органа по сигурността на Комисията.

5. КИЕС се предава между различните служби и помещения извън физически защитените зони, както следва:

а) по правило КИЕС се предава чрез електронни средства, защитени чрез криптографски продукти, одобрени в съответствие с Глава 5;

б) когато не се използват средствата, посочени в буква а), КИЕС се пренася или:

i) на електронен носител (напр. USB памет, компактдиск, твърд диск), защитен чрез криптографски продукти, одобрени в съответствие с Глава 5; или

ii) във всички останали случаи, според предписанията на правилата за прилагане.

Член 22

Класификация и обозначения

1. Информацията се класифицира, когато е необходимо да бъде защитена от съображения за поверителност, в съответствие с член 3, параграф 1.

2. Създателят на КИЕС отговаря за определянето на нивото на класификацията за сигурност, в съответствие със съответните правила за прилагане, както и за първоначалното разпространение на информацията.

3. Нивото на класификация на КИЕС се определя в съответствие с член 3, параграф 2 и при спазване на съответните правила за прилагане.

4. Класификацията за сигурност се посочва ясно и точно, независимо дали КИЕС е на хартия, в устна, електронна или друга форма.

5. Отделни части от даден документ (т.е. страници, параграфи, раздели, приложения, допълнения, добавки и притурки) може да изискват различно ниво на класификация за сигурност, за което се поставя съответният гриф, включително когато се съхраняват в електронен вид.

6. Нивото, на което се класифицира даден документ или файл, е не по-ниско от най-високото ниво на класификация за сигурност на негов елемент. Когато се обединява информация от различни източници, се прави преглед на окончателния продукт, за да се определи цялостното ниво на класификация за сигурност, тъй като може да е необходимо той да бъде с по-високо ниво на класификация от това на съставните му части.

7. Доколкото е възможно, документите, съдържащи части с различни нива на класификация, се структурират така, че частите с различни нива на класификация да могат лесно да се идентифицират и отделят при необходимост.

8. Класификацията на писмо или записка, включващи приложения, съответства на най-високата степен на класификация на тези приложения. Създателят ясно обозначава нивото на класификация на основния документ без приложенията, като използва подходящ гриф, например:

CONFIDENTIEL UE/EU CONFIDENTIAL

без приложение(я) RESTREINT UE/EU RESTRICTED.

Член 23

Обозначения

В допълнение към един от грифовете за сигурност, посочени в член 3, параграф 2, КИЕС може да носи допълнителни обозначения, като:

а) знак за идентифициране на създателя на информацията;

б) предупредително обозначение, кодови думи или акроними, уточняващи областта, до която се отнася документът, конкретното разпределение на документа на основание „необходимост да се знае“ или ограниченията за ползването му;

в) обозначение, уточняващо условията за предоставяне;

г) когато е приложимо, датата или конкретното събитие, след които нивото на класификация може да бъде понижено или премахнато.

Член 24

Съкратено обозначаване на класификацията

1. За обозначаване на нивото на класификация на отделни параграфи от текста могат да се използват стандартни съкращения на нивата на класификация. Пълното название на грифовете за сигурност не се заменя със съкратени обозначения.

2. В класифицирани документи на ЕС за обозначаване на нивото на класификация на раздели или части от текст, по-малки от една страница, могат да се използват следните стандартни съкращения:

TRÉS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Член 25

Създаване на КИЕС

1. При създаване на класифициран документ на ЕС:

а) върху всяка страница се отбелязва ясно нивото на класификация;

б) всяка страница се номерира;

в) върху документа се отбелязват регистрационният му номер и за какво се отнася, които сами по себе си не представляват класифицирана информация, освен ако не са обозначени като такава;

г) върху документа се поставя дата;

д) на всяка страница на документи с ниво на класификация за сигурност SECRET UE/EU SECRET или по-високо се обозначава номерът на копието, ако документите се разпространяват в няколко екземпляра.

2. При невъзможност за прилагане на параграф 1 към КИЕС се вземат други подходящи мерки в съответствие с правилата за прилагане.

Член 26

Понижаване на нивото на класификация и декласификация на КИЕС

1. При създаването на информацията създателят обозначава, когато е възможно, дали класификацията на КИЕС може да бъде понижена или премахната на определена дата или след настъпване на определено събитие.

2. Всяка служба на Комисията извършва редовен преглед на КИЕС, на която е създател, за да установи дали нивото на класификация продължава да е приложимо. Посредством правилата за прилагане се създава система за преразглеждане на нивото на класификация на регистрираната КИЕС, създадена от Комисията, не по-рядко от всеки пет години. Такъв преглед не се налага, ако от самото начало създателят е посочил, че нивото на класификация на информацията ще бъде автоматично понижено или че класификацията ще бъде премахната и информацията носи съответното обозначение.

3. Информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, създадена от Комисията, се декласифицира автоматично след тридесет години, в съответствие с Регламент (ЕИО, Евратом) № 354/83 на Съвета, изменен с Регламент (ЕО, Евратом) № 1700/2003 на Съвета ([1]).

Член 27

Система от регистратури на КИЕС в Комисията

1. Без да се засягат разпоредбите на член 52, параграф 5 по-долу, във всяка служба на Комисията, която работи с КИЕС или съхранява КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, се създава местна регистратура на КИЕС, за да се гарантира, че с КИЕС се работи в съответствие с разпоредбите на настоящото решение.

2. Управляваната от генералния секретариат регистратура на КИЕС е централната регистратура на КИЕС на Комисията. Тя действа като:

— местна регистратура на КИЕС за генералния секретариат на Комисията;

— регистратура на КИЕС за кабинетите на членовете на Комисията, освен ако те не разполагат с отделна местна регистратура;

— регистратура на КИЕС за генералните дирекции или службите, които не разполагат с местна регистратура на КИЕС;

— основен входен и изходен пункт за всичката информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED и по-високо, включително SECRET UE/EU SECRET, която Комисията и нейните служби обменят с трети страни и международни организации и, при наличие на специфични условия, с други институции, агенции и органи на Съюза.

3. Органът по сигурността на Комисията определя регистратура, която да играе ролята на централен орган за получаване и изпращане на информация с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET. При необходимост могат да се определят и подчинени регистратури, в които да се работи с такава информация с цел регистрация.

4. Тези подчинени регистратури не могат да предават документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET пряко на други регистратури, подчинени на същата централна регистратура за документи с класификация TRÉS SECRET UE/EU TOP SECRET, или на външни получатели без изричното писмено одобрение на последната.

5. Регистратурите на КИЕС имат статут на зони за сигурност по смисъла на Глава 3 и се акредитират от органа по акредитиране на сигурността на Комисията (ОАС).

Член 28

Ръководител на регистратурата

1. Всяка регистратура на КИЕС се управлява от ръководител на регистратурата (РР).

2. Ръководителят на регистратурата е преминал подходяща проверка за надеждност.

3. МСС на съответната служба на комисията осъществява надзор върху работата на ръководителя на регистратурата по отношение на прилагането на разпоредбите относно работата с КИЕС и спазването на приложимите правила, стандарти и насоки за сигурност.

4. Като част от задълженията си по управлението на поверената му регистратура на КИЕС ръководителят на регистратурата поема следните общи задачи в съответствие с разпоредбите на настоящото решение и съответните правила за прилагане, стандарти и насоки:

— ръководи дейностите, свързани с регистрирането, съхраняването, възпроизвеждането, превеждането, предаването, изпращането и унищожаването или прехвърлянето в историческия архив на КИЕС;

— проверява периодично необходимостта от запазване на нивото на класификация на информацията;

— изпълнява всякакви други задачи, свързани със защитата на КИЕС, определени в правилата за прилагане.

Член 29

Регистрация на КИЕС за целите на сигурността

1. За целите на настоящото решение регистрация за целите на сигурността (наричана по-долу „регистрация“) означава прилагането на процедури за отбелязване на жизнения цикъл на КИЕС, включително нейното разпространение.

([1]) Регламент (ЕО, Евратом) № 1700/2003 на Съвета от 22 септември 2003 година за изменение на Регламент (ЕИО, Евратом) № 354/83 относно отваряне за обществеността на историческите архиви на Европейската икономическа общност и на Европейската общност за атомна енергия (ОВ L 243, 27.9.2003 г., стр. 1).

2. Всяка информация или материал с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо се регистрира в определени за целта регистратури при постъпването ѝ в дадена организационна единица и при излизането ѝ от нея.

3. При работа с КИЕС или при съхраняване на КИЕС посредством комуникационна и информационна система (КИС), процедурите по регистрацията може да се изпълняват от процеси в самата КИС.

4. Регистрацията на КИЕС за целите на сигурността е уредена по-подробно в правилата за прилагане.

Член 30

Копиране и превеждане на класифицирани документи на ЕС

1. Документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET не може да се копират или превеждат без предварителното писмено съгласие на създателя им.

2. Когато създателят на документи с ниво на класификация за сигурност SECRET UE/EU SECRET и по-ниско не е поставил предупредителни обозначения за тяхното копиране или превеждане, документите могат да бъдат копирани или превеждани по указание на притежателя.

3. Мерките за сигурност, приложими към оригиналния документ, се прилагат и за неговите копия и преводи.

Член 31

Пренасяне на КИЕС

1. КИЕС се пренася по начин, който я предпазва от неразрешено разкриване по време на пренасянето.

2. При пренасянето на КИЕС се предприемат защитни мерки, които:

— са съразмерни с нивото на класификация за сигурност на пренасяната КИЕС; и

— са адаптирани към конкретните условия на пренасянето ѝ, по-конкретно дали КИЕС се пренася:

  — в рамките на сграда на Комисията или на самостоятелна група от сгради на Комисията;

  — между сгради на Комисията, намиращи се в една и съща държава членка;

  — в рамките на Съюза;

  — от територията на Съюза до територията на трета държава; и

  — са адаптирани към естеството и формата на КИЕС.

3. Тези защитни мерки се уреждат подробно в правилата за прилагане или, в случай на проекти и програми по смисъла на член 42, като неразделна част от съответните инструкции за сигурност на програмата или проекта (ИСП).

4. Правилата за прилагане или ИСП включват разпоредби, съразмерни с нивото на класификация на КИЕС, относно:

— начина на пренасяне, като пренасяне на ръка, пренасяне от дипломатически или военен куриер, пренасяне с пощенска служба или платена куриерска услуга;

— опаковането на КИЕС;

— техническите контрамерки за КИЕС, пренасяна на електронен носител;

— всички останали процедурни, физически или електронни мерки;

— процедурите за регистрация;

— използването на служители, преминали проучване за надеждност.

5. Когато КИЕС се пренася на електронен носител и независимо от разпоредбите на член 21, параграф 5, защитните мерки, посочени в съответните правила за прилагане могат да бъдат допълнени с подходящи технически контрамерки, одобрени от органа по сигурността на Комисията, така че да се сведе до минимум рискът тя да бъде загубена или компрометирана.

Член 32

Унищожаване на КИЕС

1. Класифицирани документи на ЕС, които вече не са необходими, могат да бъдат унищожени, като се вземат предвид разпоредбите за архивиране и правилата и разпоредбите на Комисията за управлението на документацията и архивирането, и по-специално общият за Комисията списък за съхранение.

2. КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и по-високо се унищожават от ръководителя на отговарящата за тях регистратура на КИЕС по указание на притежателя или на компетентен орган. Ръководителят на регистратурата актуализира съответно дневниците и останалата информация за регистрацията.

3. Унищожаването на документи с ниво на класификация за сигурност SECRET UE/EU SECRET или TRÉS SECRET UE/EU TOP SECRET се извършва от ръководителя на регистратурата в присъствието на свидетел, който притежава разрешение за достъп до ниво на класификация за сигурност най-малко на нивото на документа, който се унищожава.

4. Регистраторът и свидетелят, когато се изисква присъствие на такъв, подписват удостоверение за унищожаване, което се завежда в регистратурата. Ръководителят на съответната регистратура на КИЕС съхранява удостоверенията за унищожаване на документи с ниво на класификация за сигурност TRÉS SECRET UE/EU TOP SECRET за срок от най-малко 10 години, а на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET — за срок от най-малко пет години.

5. Класифицирани документи, включително с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, се унищожават по начини, определени в правилата за прилагане и отговарящи на съответните стандарти на ЕС или равностойни на тях.

6. Компютърни средства за съхранение на КИЕС се унищожават в съответствие с процедурите, установени в правилата за прилагане.

Член 33

Унищожаване на КИЕС в извънредни ситуации

1. Службите на Комисията, които притежават КИЕС, изготвят планове въз основа на местните условия за опазване на класифицирани материали на ЕС при криза, включващи при необходимост планове за спешно унищожаване и евакуация. Те издават необходимите указания за предотвратяване на попадането на КИЕС в ръцете на неоправомощени лица.

2. Мерките за безопасно съхраняване и/или унищожаване на материали с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET по време на криза не следва при никакви обстоятелства да се отразяват неблагоприятно на безопасното съхраняване или на унищожаването на материали с ниво на класификация са сигурност TRÉS SECRET UE/EU TOP SECRET, включително и на шифриращото оборудване, чието третиране има предимство пред всички останали задачи.

3. При извънредна ситуация и наличие на непосредствен риск от неразрешено разкриване КИЕС се унищожава от притежателя ѝ по начин, който прави невъзможно цялостното или частичното възстановяване на информацията. Създателят на информацията и регистърът, от който е получена информацията, биват информирани за извънредната ситуация, наложила унищожаването на КИЕС.

4. Унищожаването на КИЕС е уредено по-подробно в правилата за прилагане.

ГЛАВА 5

ЗАЩИТА НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ НА ЕС В КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ СИСТЕМИ (КИС)

Член 34

Основни принципи на осигуреността на информацията

1. Осигуреност на информацията (ОИ) в областта на комуникационните и информационните системи е увереността, че тези системи ще осигурят защита на информацията, с която се работи в тях, и че ще функционират както и когато е необходимо, под контрола на легитимни ползватели.

2. Ефективната осигуреност на информацията гарантира подходящи равнища на:

автентичност:	гаранцията, че информацията е истинска и произтича от bona fide източници;
достъпност:	характеристиката на информацията да бъде достъпна и използваема при поискване от оправомощена единица;
поверителност:	характеристиката, че информацията не е разкрита на неоправомощени лица, единици или процеси;
цялост:	характеристиката, че информацията и активите са запазили точността и пълнотата си;
невъзможност за отказ:	способността да се докаже, че дадено действие или събитие действително е настъпило, така че това действие или събитие да не може впоследствие да бъде отречено.

3. ОИ се основава на процес за управление на риска.

Член 35

Определения

За целите на настоящата глава се прилагат следните определения:

а) „Акредитация“ означава издаването от органа по акредитиране на сигурността (ОАС) на официално разрешение и одобрение комуникационна и информационна система от да обработва КИЕС в нейната операционна среда, след официалното потвърждаване на плана за сигурност и правилното му прилагане.

б) „Процес на акредитация“ означава необходимите стъпки и задачи преди акредитирането от органа по акредитиране на сигурността. Тези стъпки и задачи се конкретизират в стандарт за процес на акредитация.

в) „Комуникационна и информационна система“ (КИС) означава всяка система, даваща възможност за работа с информация в електронна форма. Една комуникационна и информационна система обхваща всички активи, необходими за нейното функциониране, включително инфраструктура, организация, персонал и информационни ресурси.

г) „Остатъчен риск“ означава рискът, който продължава да съществува след прилагане на мерките за сигурност, предвид факта, че не може да се противодейства на всички заплахи и че не всички видове уязвимост могат да бъдат премахнати.

д) „Риск“ означава възможността дадена заплаха да използва вътрешни или външни видове уязвимост на дадена организация или на някоя от системите, които тази организация използва, и по този начин да нанесе вреди на организацията и на нейните материални или нематериални активи. Рискът се измерва като съчетание от вероятността от осъществяване на заплахи и тяхното въздействие.

е) „Приемане на риска“ означава решение за приемане на продължаващото съществуване на остатъчен риск след третиране на риска.

ж) „Оценка на риска“ — състои се от установяване на заплахите и видовете уязвимост и от анализ на свързаните с тях рискове, т.е. анализ на вероятността и въздействието.

з) „Съобщаване за риска“ — изразява се в повишаване на осведомеността за рисковете сред общностите от ползватели на КИС, информиране за такива рискове на органите, които дават одобрение, и докладване за тях на оперативните органи.

и) „Третиране на риска“ — изразява се в смекчаване, отстраняване, намаляване (чрез подходящо съчетание от технически, физически, организационни или процедурни мерки), прехвърляне или наблюдение на риска.

Член 36

Работа с КИЕС в КИС

1. КИС работят с КИЕС в съответствие с концепцията за ОИ.

2. За КИС, в които се работи с КИЕС, съответствието с политиката на сигурност по отношение на информационните системи на Комисията, посочена в Решение C(2006) 3602 ([1]) на Комисията, означава че:

а) подходът „планирай-направи-провери-действай“ се прилага към осъществяването на политиката за сигурност на информационните системи през целия жизнен цикъл на информационната система;

б) нуждите на сигурността трябва да бъдат определени чрез оценка на въздействието върху работата;

в) информационната система и данните в нея трябва да бъдат подложени на официална класификация на активите;

([1]) Решение C(2006) 3602 на Комисията от 16 август 2006 г. относно сигурността на информационните системи, използвани от Европейската комисия.

г) трябва да се прилагат всички задължителни мерки за сигурност, определени в политиката за сигурност на информационните системи;

д) трябва да се прилага процес за оценка на риска, състоящ се от следните стъпки: определяне на заплахите и уязвимостите; оценка на риска; третиране на риска; приемане на риска и съобщаване на риска;

е) изготвен е, прилага се, проверява се и се преразглежда план за сигурност, включващ политиката за сигурност и оперативните процедури за сигурност.

3. Всички служители, участващи в проектирането, разработването, изпитването, функционирането, управлението или ползването на КИС, в които се работи с КИЕС, уведомяват ОАС за всички потенциални слабости в сигурността, инциденти, нарушения на сигурността или случаи на компрометиране на сигурността, които биха могли да окажат въздействие върху защитата на КИС и/или съдържащата се в тях КИЕС.

4. Когато защитата на КИЕС се осигурява от криптографски продукти, такива продукти се одобряват, както следва:

а) отдава се предпочитание на продукти, одобрени от Съвета или от Генералния секретар на Съвета в качеството му на орган за криптографско одобрение на Съвета, по препоръка на Експертната група по сигурността на Комисията;

б) когато това е обосновано от специфични оперативни съображения, органът за криптографско одобрение (ОКО) на Комисията може, по препоръка на Експертната група по сигурността на Комисията, да отмени изискванията по буква а) и да издаде временно одобрение за конкретен период.

5. При предаване, обработване и съхраняване на КИЕС чрез електронни средства се използват одобрени криптографски продукти. Въпреки това изискване, при извънредни обстоятелства могат да се прилагат специфични процедури или специфични технически конфигурации след одобряването им от ОКО.

6. С цел защита на КИС, в които се работи с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо по начин, който да не допуска информацията да бъде компрометирана чрез неумишлени електромагнитни излъчвания се прилагат мерки за сигурност на информацията („мерки за сигурност по TEMPEST“). Тези мерки за сигурност са съизмерими с риска от експлоатация и нивото на класификация на информацията.

7. Органът по сигурността на Комисията изпълнява следните функции:

— орган по ОИ (ООИ);

— орган по акредитиране на сигурността (ОАС);

— орган по TEMPEST (ОТ);

— орган за криптографско одобрение (ОКО);

— орган за разпределение на криптографски материали (ОРКМ).

8. Органът по сигурността на Комисията определя оперативен орган по ОИ за всяка система.

9. Отговорностите на функциите, описани в параграфи 7 и 8, се определят в правилата за прилагане.

Член 37

Акредитация на КИС, работещи с КИЕС

1. Всички КИС, в които се работи с КИЕС, преминават през процес на акредитация, основаващ се на принципите на ОИ, чиято задълбоченост трябва да бъде съразмерна с равнището на необходимата защита.

2. Процесът на акредитация включва официално валидиране от органа по акредитиране на сигурността на плана за сигурност на съответната КИС, за да се получат гаранции, че:

а) посоченият в член 36, параграф 2 процес на управление на риска се осъществява правилно;

б) собственикът на системата е информиран за остатъчния риск и го е приел;

в) е постигнато достатъчно ниво на защита на КИС и на КИЕС, в която се работи в нея, в съответствие с настоящото решение.

3. Органът по акредитиране на сигурността на Комисията издава декларация за акредитация, в която се определя най-високото ниво на класификация за сигурност на КИЕС, с която може да се работи в дадена КИС, както и съответните изисквания и условия за това. Това не засяга задачите, възложени на Съвета по акредитиране на сигурността по смисъла на член 11 от Регламент (ЕС) № 512/2014 на Европейския парламент и на Съвета ([1]).

4. Акредитацията на КИС на Комисията, в които участват няколко страни, се извършва от съвместен Съвет по акредитиране на сигурността (САС). Той се състои от представител на ОАС на всяка участваща страна и се председателства от представител на ОАС на Комисията.

5. Процесът на акредитация се състои от редица задачи, които се изпълняват от участващите страни. Отговорност за изготвянето на акредитационните досиета и документи носи изцяло собственикът на КИС.

6. Отговорност за акредитацията носи ОАС на Комисията, който във всеки момент от жизнения цикъл на КИС има право:

а) да поиска да бъде извършен процес на акредитация;

б) да одитира или инспектира КИС;

в) в случай, че е настъпила липса на съответствие с условията на експлоатация, да поиска да бъде разработен и ефективно приложен план за подобряване на сигурността в рамките на добре разчетен във времето график, като евентуално оттегли разрешението за експлоатация на КИС до възстановяването на съответствието с условията на експлоатация.

7. Процесът на акредитация се установява чрез стандарт за процес на акредитация на КИС, в които се работи с КИЕС, който се приема в съответствие с член 10, параграф 3 от Решение C(2006) 3602.

Член 38

Извънредни обстоятелства

1. Независимо от разпоредбите на настоящата глава, описаните по-долу специални процедури могат да се прилагат в извънредни ситуации, например по време на предстояща или настояща криза, конфликт, състояние на война или при извънредни оперативни обстоятелства.

2. КИЕС може да се предава, като се използват криптографски продукти, одобрени за по-ниско ниво на класификация за сигурност, или без да се криптира, със съгласието на компетентния орган, в случай че евентуално забавяне би причинило очевидно по-голяма вреда от тази, произтичаща от разкриване на класифицирания материал, и ако:

а) изпращачът и получателят не притежават необходимите уреди за криптиране; и

б) класифицираният материал не може да бъде изпратен своевременно с други средства.

3. Класифицираната информация, предавана при описаните в параграф 1 обстоятелства, не носи грифове за сигурност или обозначения, които да я отличават от некласифицираната информация или от информацията, която може да бъде защитена с наличен криптографски продукт. Получателите се уведомяват незабавно за нивото на класификация с други средства.

4. Впоследствие се изготвя доклад до компетентния орган и до Експертната група по сигурността на Комисията.

ГЛАВА 6

ИНДУСТРИАЛНА СИГУРНОСТ

Член 39

Основни принципи

1. Индустриалната сигурност представлява прилагане на мерки за гарантиране на защитата на КИЕС

а) в рамките на класифицирани договори, от страна на:

i) кандидатите или оферентите по време на процедурата за възлагане на поръчката;

ii) изпълнителите или подизпълнителите по време на жизнения цикъл на класифицираните договори;

([1]) Регламент (ЕС) № 512/2014 на Европейския парламент и на Съвета от 16 април 2014 година за изменение на Регламент (ЕС) № 912/2010 за създаване на Европейската агенция за ГНСС (ОВ L 150, 20.5.2014 г., стр. 72).

б) в рамките на класифицирани споразумения за безвъзмездно финансиране, от страна на:

i) кандидатите в процедурите за отпускане на безвъзмездно финансиране;

ii) бенефициерите по време на жизнения цикъл на класифицираните споразумения за безвъзмездно финансиране.

2. Такива договори или споразумения за безвъзмездно финансиране не включват информация с ниво на класификация за сигурност TRES SECRET UE/EU TOP SECRET.

3. Освен ако не е посочено друго, разпоредбите на настоящата глава по отношение на класифицираните договори или изпълнителите се прилагат и за класифицираните договори за подизпълнение или подизпълнителите.

Член 40

Определения

За целите на настоящата глава се прилагат следните определения:

а) „Класифициран договор“ означава рамков договор или договор по смисъла на Регламент (ЕО, Евратом) № 1605/2002 ([1]), сключен от Комисията или някоя от нейните служби с изпълнител за доставка на движими или недвижими активи, изпълнение на строително-ремонтни дейности или предоставяне на услуги, чието изпълнение налага или включва създаване на КИЕС, работа с КИЕС или съхраняване на КИЕС.

б) „Класифициран договор за подизпълнение“ означава договор, сключен от изпълнител на Комисията с друг изпълнител (т.е. подизпълнител) за доставка на движими или недвижими активи, изпълнение на строително-ремонтни дейности или предоставяне на услуги, чието изпълнение налага или включва създаване на КИЕС, работа с КИЕС или съхраняване на КИЕС.

в) „Класифицирано споразумение за безвъзмездно финансиране“ означава споразумение, по силата на което Комисията отпуска безвъзмездно финансиране по смисъла на част I, дял VI от Регламент (ЕО, Евратом) № 1605/2002, чието изпълнение налага или включва създаване на КИЕС, работа с КИЕС или съхраняване на КИЕС.

г) „Определен орган по сигурността“ (ООС) означава орган, отговорен пред националния орган по сигурността (НОС) на държава членка, който отговаря за информиране на индустриални или други единици за националната политика по всички въпроси на индустриалната сигурност и за предоставяне на указания и съдействие при нейното изпълнение. Функциите на ООС може да се изпълняват от НОС или от друг компетентен орган.

Член 41

Процедура за класифицирани договори или споразумени за безвъзмездно финансиране

1. Всяка служба на Комисията, в качеството си на възложител, гарантира, че при възлагане на класифицирани договори или споразумения за безвъзмездно финансиране в договора са включени минималните стандарти за индустриална сигурност, установени в настоящата глава, или е направена препратка към тях.

2. За целите на параграф 1 компетентните служби на Комисията се консултират с генерална дирекция „Човешки ресурси и сигурност“, и по-специално с дирекция „Сигурност“ в нея, за да се уверят, че моделите на договори за изпълнение и подизпълнение и моделите на споразумения за безвъзмездно финансиране включват разпоредби, отразяващи основните принципи и минималните стандарти за защита на КИЕС, които трябва да се спазват от изпълнителите и подизпълнителите и от бенефициерите на споразуменията за безвъзмездно финансиране.

3. Комисията сътрудничи тясно с НОС, ООС или всеки друг компетентен орган на съответните държави членки.

4. Когато възложител има намерение да обяви процедура за възлагане на класифициран договор или сключване на споразумение за безвъзмездно финансиране, той се консултира с органа по сигурността на Комисията по въпросите, свързани с класифицирания характер и елементи на процедурата на всички етапи от нея.

5. Моделите и примерите за класифицирани договори за изпълнение и подизпълнение, класифицирани споразумения за безвъзмездно финансиране, обявления за поръчки, насоки за обстоятелствата, при които се изисква „удостоверение за сигурност на структура“ (УСС), инструкции за сигурност на проект или програма (ИСП), приложения относно аспектите на сигурността (ПАС), посещения, предаване и пренасяне на КИЕС по класифициранни договори или класифицирани споразумения за безвъзмездно финансиране се установяват в правилата за прилагане по отношение на индустриалната сигурност, след консултация с Експертната група по сигурността на Комисията.

([1]) Регламент (ЕО, Евратом) № 1605/2002 на Съвета от 25 юни 2002 г. относно Финансовия регламент, приложим за общия бюджет на Европейските общности (ОВ L 248, 16.9.2002 г., стр. 1).

6. Комисията може да сключи класифицирани договори или споразумения за безвъзмездно финансиране, с които се възлага изпълнението на задачи, включващи или налагащи достъп до КИЕС или работа с КИЕС или съхранение на КИЕС от икономически оператори, регистрирани в държава членка или в трета държава, която е сключила споразумение или административна договореност в съответствие с Глава 7 от настоящото решение.

Член 42

Елементи на сигурността в класифициран договор или споразумение за безвъзмездно финансиране

1. Класифицираните договори или споразумения за безвъзмездно финансиране включват следните елементи на сигурността:

Инструкции за сигурност на програмата или проекта

а) „Инструкции за сигурност на програмата или проекта“ (ИСП) означава списък от процедури за сигурност, които се прилагат за конкретна програма или проект с цел стандартизиране на процедурите за сигурност. Те подлежат на преразглеждане във всеки един момент от осъществяването на програмата или проекта.

б) Генерална дирекция „Човешки ресурси и сигурност“ разработва примерни ИСП, които службите на Комисията, отговарящи за програми или проекти, включващи работа с КИЕС или съхранение на КИЕС използват при разработването, където това е подходящо, на свои специфични ИСП.

в) Специфични ИСП се разработват по-специално за програми и проекти, характеризиращи се със значителен обхват, мащаб или сложност или с множество или многообразни изпълнители, бенефициери и други партньори и заинтересовани страни, например по отношение на правния им статут. Специфични ИСП се разработват от службата или службите на Комисията, управляващи програмата или проекта, в тясно сътрудничество с генерална дирекция „Човешки ресурси и сигурност“.

г) Генерална дирекция „Човешки ресурси и сигурност“ представя примерните и специфичните ИСП за консултация с Експертната група по сигурността на Комисията.

Приложение относно аспектите на сигурността

а) „Приложение относно аспектите на сигурността“ (ПАС) означава съвкупност от специални договорни условия, изготвени от възложителя, които представляват неразделна част от всеки класифициран договор, включващ достъп до КИЕС или създаване на КИЕС, и в които се определят изискванията за сигурност или елементите на договора, изискващи защита на сигурността.

б) Свързаните с договора изисквания за сигурност се описват в ПАС. Когато това е уместно, ПАС включва ръководството за класифициране за целите на сигурността и представлява неразделна част от класифицирания договор за изпълнение или подизпълнение или класифицираното споразумение за безвъзмездно финансиране.

в) В ПАС се съдържат разпоредби, изискващи от изпълнителя или бенефициера да спазва минималните стандарти, установени в настоящото решение. Възложителят гарантира, че в ПАС е посочено, че неспазването на тези минимални стандарти може да бъде достатъчно основание за прекратяване на договора или споразумението за безвъзмездно финансиране.

2. Ръководството за класифициране за целите на сигурността (РКЦС) е задължителен елемент на сигурността и се включва в ИПС и ПАС:

а) „Ръководство за класифициране за целите на сигурността“ (РКЦС) означава документ, който описва елементите на програма, проект, договор или споразумение за безвъзмездно финансиране, които са класифицирани, като определя приложимите нива на класификация за сигурност. РКЦС може да бъде допълвано през целия период на времетраене на програмата, проекта, договора или споразумението за безвъзмездно финансиране, като нивото на класификация на елементите на информацията може да бъде променяно или понижавано; РКЦС, в случай че такова съществува, е част от ПАС.

б) Преди да обяви търг за възлагане на класифициран договор или да възложи такъв договор, службата на Комисията, в качеството си на възложител, определя класификацията за сигурност на информацията, която се предоставя на участниците в търга и на изпълнителите, както и класификацията за сигурност на информацията, която се създава от изпълнителя. За тази цел тя изготвя РКЦС, което да се използва при осъществяването на договора, в съответствие с разпоредбите на настоящото решение и правилата за неговото прилагане, след консултация с органа по сигурността на Комисията.

в) При определяне на нивото на класификация за сигурност на различните елементи на класифицирания договор се прилагат следните принципи:

i) при изготвянето на РКЦС службата на Комисията, в качеството си на възложител, взема предвид всички релевантни аспекти на сигурността, включително нивото на класификация за сигурност, определено за информацията, която е предоставена и одобрена за ползване при изпълнението на договора от създателя на информацията;

ii) общото ниво на класификация за сигурност на договора не може да бъде по-ниско от най-високото ниво на класификация за сигурност на който и да е от неговите елементи; и

iii) при нужда възложителят, посредством органа по сигурността на Комисията, влиза във връзка с НОС, ООС или друг заинтересован компетентен орган по сигурността на държавите членки, в случай на промени на нивото на класификация на информацията, създадена от изпълнителите или предоставена им при изпълнението на договора, както и при извършване на по-нататъшни промени в РКЦС.

Член 43

Достъп до КИЕС на служителите на изпълнителите и бенефициерите

Възложителят или органът, отпускащ безвъзмездното финансиране, гарантира, че класифицираният договор или класифицираното споразумение за безвъзмездно финансиране включва разпоредби, в които се посочва, че служителите на изпълнител, подизпълнител или бенефициер, които се нуждаят от достъп до КИЕС за целите на изпълнението на класифицирания договор за изпълнение или подизпълнение или на споразумението за безвъзмездно финансиране, ще получат такъв достъп само ако:

а) той е получил разрешение за достъп до съответното ниво на класификация или е надлежно оправомощен по друг начин след като за него е била установена „необходимост да се знае“;

б) лицата са информирани за приложимите правила и процедури по сигурността за защита на КИЕС и са потвърдили, че осъзнават своята отговорност за защитата на такава информация;

в) лицата са преминали проучване за надеждност за необходимото ниво за информация, класифицирана CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, извършено от съответния НОС, ООС или друг компетентен орган.

Член 44

Удостоверение за сигурност на структура

1. „Удостоверение за сигурност на структура“ (УСС) означава административно определяне от НОС, ООС или друг компетентен орган, че дадена структура може да осигури адекватна защита на КИЕС на определено ниво на класификация за сигурност.

2. УСС, издадено от НОС или ООС или друг компетентен орган на държава членка в уверение на това, че в съответствие с националните законови и подзаконови актове определен икономически оператор може да защити КИЕС на подходящо ниво на класификация (CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET) в своите структури се предоставя на органа по сигурността на Комисията, който го препраща на службата на Комисията, изпълняваща ролята на възложител или орган, отпускащ безвъзмездното финансиране, преди на кандидат, участник в търг, изпълнител или кандидат за безвъзмездно финансиране да бъде предоставена КИЕС или да му бъде даден достъп до такава.

3. Когато е уместно, възложителят уведомява, посредством органа по сигурността на Комисията, съответния НОС, ООС или друг компетентен орган по сигурността, че за изпълнението на договора се изисква удостоверение за сигурност на структура. УСС или РДС се изисква когато в процеса на възлагане на договора или на сключване на споразумението за безвъзмездно финансиране трябва да се предостави КИЕС с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

4. Възложителят или органът, отпускащ безвъзмездното финансиране не сключва класифициран договор или споразумение за безвъзмездно финансиране с предпочитан участник в търга или кандидат, преди да е получил потвърждение от НОС, ООС или друг компетентен орган по сигурността на държавата членка, в която е регистриран съответният изпълнител или подизпълнител, че е издадено съответното удостоверение за сигурност на структура, ако такова е необходимо.

5. Когато органът по сигурността на Комисията бъде уведомен от НОС, ООС или друг компетентен орган, издал УСС, за настъпването на промени, засягащи УСС, той информира службата на Комисията, изпълняваща функциите на възложител или орган, отпускащ безвъзмездно финансиране. При договори за подизпълнение се уведомява съответно НОС, ООС или друг компетентен орган по сигурността.

6. Оттеглянето на УСС от съответния НОС, ООС или друг компетентен орган по сигурността представлява достатъчно основание за възложителя или органа, отпускащ безвъзмездното финансиране да прекрати класифициран договор или да изключи от процедурата по възлагането кандидат, оферент или участник. При съставянето на моделите на договори и споразумения за безвъзмездно финансиране се включва разпоредба в този смисъл.

Член 45

Разпоредби за класифицирани договори и споразумени за безвъзмездно финансиране

1. Когато по време на процедурата по възлагане на кандидат, оферент или участник се предоставя КИЕС, поканата за представяне на оферта съдържа разпоредба, задължаваща кандидата, оферента или участника, който не е представил оферта или предложение или не е избран, да върне всички класифицирани документи в рамките на определен период от време.

2. Възложителят или органът, отпускащ безвъзмездното финансиране уведомяват, посредством органа по сигурността на Комисията, компетентния НОС, ООС или друг компетентен орган по сигурността за възлагането на класифициран договор или споразумение за безвъзмездно финансиране, както и за съответните данни, като името на изпълнителя или изпълнителите или бенефициерите, срокът на изпълнение на договора и максималното ниво на класификация.

3. При прекратяване на такива договори или споразумения за безвъзмездно финансиране възложителят или органът, отпускащ безвъзмездното финансиране уведомява своевременно, посредством органа по сигурността на Комисията, НОС, ООС или друг компетентен орган на държавата членка, в която е регистриран изпълнителят или бенефициерът.

4. По правило при прекратяване на класифициран договор или споразумение за безвъзмездно финансиране от изпълнителя или бенефициера се изисква да върне на възложителя или на органа, отпускащ безвъзмездното финансиране всяка държана от него КИЕС.

5. Конкретните разпоредби за разпореждането с КИЕС по време на изпълнението на класифицирания договора или класифицираното споразумение за безвъзмездно финансиране или при неговото прекратяване се посочват в ПАС.

6. Когато на изпълнителя или бенефициера бъде разрешено да задържи КИЕС след прекратяването на класифицирания договор или споразумение за безвъзмездно финансиране, изпълнителят или бенефициерът продължава да спазва минималните стандарти, съдържащи се в настоящото решение и да защитава конфиденциалността на КИЕС.

Член 46

Специфични разпоредби за класифицирани договори

1. Условията, свързани със защитата на КИЕС, при които изпълнителят може да възлага договора за подизпълнение, се определят в условията за търга и в класифицирания договор.

2. За да предостави за подизпълнение части от класифициран договор, изпълнителят получава разрешение от възложителя. Договор за подизпълнение, включващ достъп до КИЕС не може да се сключва с подизпълнител, регистриран в трета страна, освен ако не е налице регулаторна рамка за сигурността на информацията по смисъла на Глава 7.

3. Изпълнителят носи отговорност за осигуряване на спазването на установените в настоящото решение минимални стандарти за сигурност по време на извършването на всички подизпълнителски дейности и не предоставя КИЕС на подизпълнителя без предварителното писмено съгласие на възложителя.

4. За създател на КИЕС, създадена от изпълнител или подизпълнител или с която те работят, се счита Комисията, а правата на създателя се упражняват от възложителя.

Член 47

Посещения във връзка с класифицирани договори

1. Когато за изпълнението на класифициран договор или споразумение за безвъзмездно финансиране служители на Комисията или на изпълнителите или на бенефициерите е необходимо да получат на взаимна основа достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET в помещенията си, се уреждат посещения, като се поддържа връзка с НОС, ООС или друг съответен компетентен орган по сигурността. Органът по сигурността на Комисията се уведомява за тези посещения. В контекста на конкретни програми и проекти, обаче, НОС, ООС или друг компетентен орган по сигурността може договори също така процедура за пряко организиране на такива посещения.

2. Всички посетители притежават подходящо разрешение за достъп и отговарят на изискването за „необходимост да се знае“ за достъп до КИЕС, свързана с класифицирани договор.

3. На посетителите се дава достъп единствено до КИЕС, свързана с целите на посещението.

4. По-подробни разпоредби се съдържат в правилата за прилагане.

5. Спазването на разпоредбите по отношение на посещенията във връзка с класифицирани договори, установени с настоящото решение и правилата за неговото прилагане, посочени в параграф 4, е задължително.

Член 48

Предаване и пренасяне на КИЕС във връзка с класифицирани договори или класифицирани споразумения за безвъзмездно финансиране

1. По отношение на предаването на КИЕС чрез електронни средства се прилагат съответните разпоредби на Глава 5 от настоящото решение.

2. По отношение на пренасянето на КИЕС се прилагат съответните разпоредби на Глава 4 от настоящото решение и правилата за неговото прилагане, в съответствие с националните законови и подзаконови актове.

3. При определяне на мерките за сигурност при транспортиране на класифицирани материали като товар се прилагат следните принципи:

а) сигурността се осигурява на всеки етап по време на транспорта от пункта на произход до крайното местоназначение;

б) степента на защита, предоставена за дадена пратка, се определя от най-високото ниво на класификация за сигурност на материала, който се съдържа в нея;

в) преди трансграничен пренос на материали, класифицирани като CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, изпращачът изготвя план за пренос, който се одобрява от НОС, ООС или друг съответен компетентен орган по сигурността;

г) пътуванията, доколкото това е възможно, се извършват от пункт до пункт и толкова бързо, колкото позволяват обстоятелствата;

д) винаги когато това е възможно, маршрутите следва да преминават само през държави членки. Маршрути през държави, които не са членки на ЕС, следва да се използват единствено когато са разрешени от НОС, ООС или други компетентни органи по сигурността на държавите както на изпращача, така и на получателя.

Член 49

Предаване на КИЕС на изпълнители или бенефициери, намиращи се в трети държави

Предаването на КИЕС на изпълнители и подизпълнители, намиращи се в трети държави, се извършва в съответствие с мерките за сигурност, договорени между органа по сигурността на Комисията, службата на Комисията, изпълняваща ролята на възложител или орган, отпускащ безвъзмездно финансиране и НОС, ООС или друг компетентен орган по сигурността на съответната трета държава, в която е регистриран изпълнителят или бенефициерът.

Член 50

Работа с информация с ниво на класифиция за сигурност RESTREINT UE/EU RESTRICTED във връзка с класифицирани договори или класифицирани споразумения за безвъзмездно финансиране

1. Защитата на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, с която се работи или която се съхранява по класифицирани договори или споразумения за безвъзмездно финансиране, се основава на принципите на пропорционалността и разходната ефективност.

2. Във връзка с класифицирани договори или класифицирани споразумения за безвъзмездно финансиране, включващи работа с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED или съхраняване на такава, не се изисква УСС или РДС.

3. Когато даден договор или споразумение за безвъзмездно финансиране включва работа с информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED в рамките на КИС, с която оперира изпълнител или бенефициер, възложителят или органът, отпускащ безвъзмездното финансиране, след като се консултира с органа по сигурността на Комисията, гарантира включването в договора или споразумението за безвъзмездно финансиране на необходимите технически и административни изисквания за акредитацията или одобряването на въпросната КИС, съизмерими с оценката на риска, като се вземат предвид всички приложими фактори. Обхватът на акредитацията или одобрението на такава КИС се договаря между органа по сигурността на Комисията и съответния НОС или ООС.

ГЛАВА 7

ОБМЕН НА КЛАСИФИЦИРАНА ИНФОРМАЦИЯ С ДРУГИ ИНСТИТУЦИИ, АГЕНЦИИ, ОРГАНИ И СЛУЖБИ НА СЪЮЗА, С ДЪРЖАВИ ЧЛЕНКИ, С ТРЕТИ ДЪРЖАВИ И МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

Член 51

Основни принципи

1. Когато Комисията или нейна служба установи необходимост от обмен на КИЕС с друга институция, агенция, орган или служба на Съюза или с трета държава или международна организация, се предприемат необходимите действия за създаване на подходяща правна или административна рамка, която може да включва споразумения за сигурността на информацията или административни договорености, които се сключват в съответствие с приложимите разпоредби.

2. Без да се засяга член 57, КИЕС се обменя с друга институция, агенция, орган или служба на Съюза или с трета държава или международна организация единствено ако е налице такава подходяща правна или административна рамка и ако има достатъчно гаранции, че институцията, агенцията, органът или службата на Съюза или третата държава или международната организация прилага равностойно основни принципи за защита на класифицираната информация.

Член 52

Обмен на КИЕС с други институции, агенции, органи и служби на Съюза

1. Преди да сключи административни договорености за обмен на КИЕС с друга институция, агенция, орган или служба на Съюза, Комисията иска гаранции, че съответната институция, агенция, орган или служба на Съюза:

а) разполага с регулаторна рамка за защита на КИЕС, в която са посочени основни принципи и минимални стандарти, равностойни на установените с настоящото решение и правилата за неговото прилагане;

б) прилага стандарти за сигурност и насоки по отношение на сигурността на персонала, физическата сигурност, управлението на КИЕС и сигурността комуникационните и информационните системи (КИС), гарантиращи ниво на защита на КИЕС равностойно на осигуряваното от Комисията;

в) обозначава създадената от него информация като КИЕС.

2. Генерална дирекция „Човешки ресурси и сигурност“, в тясно сътрудничество с други компетентни отдели на Комисията, е водещата служба на Комисията при сключването на административни договорености за обмен на КИЕС с други институции, агенции, органи или служби.

3. По правило административните договорености се сключват чрез размяна на писма, подписани от генералния директор на ГД „Човешки ресурси и сигурност“ от името на Комисията.

4. Преди сключване на административна договореност за обмен на КИЕС органът по сигурността на Комисията извършва посещение за оценка на регулаторната рамка за защита на КИЕС и за да се увери в ефективността на мерките, прилагани за защита на КИЕС. Административната договореност влиза в сила и обменът на КИЕС започва само ако резултатът от това посещение за оценка е задоволителен и направените при него препоръки са изпълнени. Провеждат се редовни последващи посещения за проверка на спазването на административната договореност и дали съществуващите мерки за сигурност продължават да отговарят на договорените основни принципи и минимални стандарти.

5. В Комисията по правило регистратурата на КИЕС, която се управлява от генералния секретариат, е основният входен и изходен пункт при обмен на класифицирана информация с други институции, агенции, органи и служби на Съюза. При все това, когато това е по-целесъобразно за защитата на КИЕС по съображения, свързани със сигурността, организацията или оперативната дейност, като входни и изходни пунктове за класифицирана информация по въпроси от правомощията на съответните служби на Комисията действат местни регистратури на КИЕС, създадени в службите на Комисията в съответствие с настоящото решение.

6. Експертната група по сигурността на Комисията бива информирана за процеса на сключване на административни договорености по смисъла на параграф 2.

Член 53

Обмен на КИЕС с държави членки

1. КИЕС може да се обменя с държави членки и да им бъде разкривана, при условие че те защитават тази информация в съответствие с изискванията, приложими към класифицираната информация, обозначена с национален гриф за сигурност на съответното ниво по таблицата за съответствие на нивата на класификация за сигурност в Приложение I.

2. Когато държавите членки въвеждат в структурите или мрежите на Европейския съюз класифицирана информация, обозначена с национален гриф за сигурност, Комисията осигурява защита на тази информация в съответствие с изискванията, приложими към КИЕС на съответстващото ниво, съгласно съдържащата се в Приложение I таблица на съответствията на нивата на класификация за сигурност.

Член 54

Обмен на класифицирана информация с трети държави и международни организации

1. Когато Комисията установи наличие на дългосрочна необходимост от обмен на класифицирана информация с трети държави или международни организации, се предприемат необходимите мерки за установяване на подходяща правна или административна рамка за тази цел, която може да включва споразумения за сигурност и информация или административни споразумения, сключени в съответствие с приложимите разпоредби.

2. Споразуменията за сигурност на информацията и административните договорености, посочени в параграф 1, съдържат разпоредби, които гарантират, че когато трети държави или международни организации получават КИЕС, тя е защитена по начин, съответстващ на нейното ниво на класификация и отговарящ на минимални стандарти, равностойни на установените в настоящото решение.

3. Комисията може да сключва административни договорености в съответствие с член 56 когато нивото на класификация на КИЕС като правило не надвишава RESTREINT UE/EU RESTRICTED.

4. Административните договорености за обмен на класифицирана информация, посочени в параграф 3, съдържат разпоредби, които гарантират, че когато трети държави или международни организации получават КИЕС, тя е защитена по начин, съответстващ на нейното ниво на класификация и отговарящ на минимални стандарти, равностойни на установените в настоящото решение. При сключването на споразумения за сигурност на информацията или административни договорености се провеждат консултации с Експертната група по сигурността на Комисията.

5. Решението да се предостави на трета държава или международна организация КИЕС, създадена в Комисията, се взема от службата на Комисията, която е създател на тази КИЕС, поотделно за всеки конкретен случай, в зависимост от естеството и съдържанието на тази информация, „необходимостта да се знае“ от получателя и предимствата, които това дава на Съюза. Ако исканата класифицирана информация или съдържащият се в нея изходен материал не са създадени от Комисията, службата на Комисията, която притежава тази класифицирана информация най-напред иска писмено съгласие за нейното предоставяне от създателя на информацията. В случай, че създателят на информацията не може да бъде установен, службата на Комисията, която притежава тази класифицирана информация поема неговите задължения след консултация с Експертната група по сигурността на Комисията.

Член 55

Споразумения за сигурност на информацията

1. Споразумения за сигурност на информацията с трети държави или международни организации се сключват в съответствие с разпоредбите на член 218 от ДФЕС.

2. Споразуменията за сигурност на информацията:

а) установяват основните принципи и минималните стандарти, които уреждат обмена на класифицирана информация между Съюза и дадена трета държава или международна организация;

б) предвиждат договорености за техническото изпълнение, които се постигат между компетентните органи по сигурността на съответните институции и органи на Съюза и компетентния орган по сигурността на въпросната трета държава или международна организация. Тези договорености отчитат нивото на защита, предоставено от прилаганите в съответната трета държава или международна организация разпоредби, структури и процедури за сигурност;

в) предвиждат, преди да се пристъпи към обмен на класифицирана информация по въпросното споразумение, да бъде получено уверение, че получаващата страна е в състояние да защитава и да опазва предоставената ѝ информация по подходящ начин.

3. Когато бъде установена необходимост от обмен на класифицирана информация съгласно член 51, параграф 1, Комисията се консултира с Европейската служба за външна дейност, генералния секретариат на Съвета и други институции и органи на Съюза, ако е целесъобразно, за да определи дали да внесе в Съвета препоръка съгласно член 218, параграф 3 от ДФЕС.

4. КИЕС не се обменя с електронни средства, освен ако това не е изрично предвидено в споразумението за сигурност на информацията или в договореностите за техническото изпълнение.

5. В Комисията по правило регистратурата на КИЕС, която се управлява от генералния секретариат, е основният входен и изходен пункт при обмен на класифицирана информация с трети държави и международни организации. При все това, когато това е по-целесъобразно за защитата на КИЕС по съображения, свързани със сигурността, организацията или оперативната дейност, като входни и изходни пунктове за класифицирана информация по въпроси от правомощията на съответните служби на Комисията действат местни регистратури на КИЕС, създадени в службите на Комисията в съответствие с настоящото решение.

6. За оценка на ефективността на разпоредбите, структурите и процедурите за сигурност в съответната трета държава или международна организация Комисията участва в посещения за оценка в сътрудничество с други институции, агенции или органи на Съюза по взаимно споразумение със съответната трета държава или международна организация. При тези посещения за оценка се оценява:

а) регулаторната рамка, приложима към защитата на класифицирана информация;

б) специфични елементи на политиката за сигурност и начина, по който сигурността е организирана в третата държава или международната организация, които могат да окажат въздействие върху нивото на класифицираната информация, която може да бъде обменяна;

в) въведените мерки и процедури за сигурност; и

г) процедурите за разрешаване на достъп до нивото на КИЕС, която се предоставя.

Член 56

Административни договорености

1. Когато в контекста на политическата или правната рамка на Съюза е налице дългосрочна необходимост от обмен на информация с ниво на класификация за сигурност по правило не по-високо от RESTREINT UE/EU RESTRICTED с трета държава или международна организация и когато органът по сигурността на Комисията, след консултация с Експертната група по сигурността на Комисията, е установил, че въпросната договаряща страна не разполага с достатъчно развита система за сигурност, за да е възможно тя да встъпи в споразумение за сигурност на информацията, Комисията може да сключи административна договореност със съответните органи на въпросната трета държава или международна организация.

2. Такива административни договорености по правило се сключват чрез размяна на писма.

3. Преди сключването на договореност се провежда посещение за оценка. Експертната група по сигурността на Комисията бива информирана за резултата от посещението за оценка. В случай, че извънредни обстоятелства налагат спешен обмен на класифицирана информация, КИЕС може да бъде предоставена при условие че са положени всички усилия за провеждане на посещение за оценка в най-кратък срок.

4. КИЕС не се обменя чрез електронни средства, освен в случаите, когато това е изрично предвидено в административната договореност.

Член 57

Извънредно *ad hoc* предоставяне на КИЕС

1. Когато няма сключено споразумение за сигурност на информацията или административна договореност и когато Комисията или нейна служба установи извънредна необходимост в контекста на политическата или правната рамка на Съюза да бъде предоставена КИЕС на трета държава или на международна организация, органът по сигурността на Комисията, доколкото това е възможно, проверява чрез органите по сигурността на съответната трета държава или международна организация дали нейните разпоредби, структури и процедури по отношение на сигурността са такива, че предоставената ѝ КИЕС ще бъда защитена по стандарти не по-малко строги от установените с настоящото решение.

2. Решението да се предостави КИЕС на съответната трета държава или международна организация се взема, след консултация с Експертната група по сигурността на Комисията, по предложение от члена на Комисията, отговарящ за въпросите на сигурността.

3. След като Комисията вземе решение да предостави КИЕС и при условие че е получено писменото одобрение на създателя на информацията, включително създателите на съдържащите се в нея изходни материали, компетентният отдел на Комисията препраща съответната информация с обозначение, че подлежи на предоставяне, в което се посочва третата държава или международната организация, на която се предоставя. Преди или при самото предоставяне на КИЕС въпросната трета страна писмено потвърждава, че поема задължение за защита на получената от нея КИЕС в съответствие с основните принципи и минималните стандарти, установени в настоящото решение.

ГЛАВА 8

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 58

Замяна на предходно решение

С настоящото решение се отменя и заменя Решение 2001/844/ЕО, ЕОВС, Евратом на Комисията ([1]).

Член 59

Класифицирана информация, създадена преди влизането в сила на настоящото решение

1. Цялата КИЕС, класифицирана в съответствие с Решение 2001/844/ЕО, ЕОВС, Евратом продължава да бъде защитена съгласно съответните разпоредби от настоящото решение.

2. Цялата класифицирана информация, притежавана от Комисията на датата на влизане в сила на Решение 2001/844/ЕО, ЕОВС, Евратом, с изключение на класифицираната информация по Евратом:

а) ако е създадена от Комисията, продължава по подразбиране да се счита за прекласифицирана с ниво на класификация RESTREINT UE, освен ако авторът ѝ не е решил да ѝ даде друго ниво на класификация до 31 януари 2002 г. и е информирал за това всички получатели на документа;

б) ако е създадена от автори извън Комисията, запазва първоначалната си класификация и по този начин се третира като равностойна по степен КИЕС, освен ако авторът не даде съгласие за нейното декласифициране или понижаване на нивото ѝ на класификация.

Член 60

Правила за прилагане и насоки за сигурност

1. При необходимост Комисията приема отделно решение, с което оправомощава члена на Комисията, отговарящ за въпросите на сигурността, да приеме правила за прилагане на настоящото решение, при пълно спазване на вътрешния процедурен правилник.

2. След като бъде оправомощен чрез горепосоченото решение, членът на Комисията, отговарящ за въпросите на сигурността може да разработи насоки за сигурност, с които се установяват указания за сигурност и най-добри практики в обхвата на приложното поле на настоящото решение и правилата за неговото прилагане.

3. Комисията може да делегира задачите, упоменати в първия и втория параграф на настоящия член на генералния директор на ГД „Човешки ресурси и сигурност“ посредством отделно решение за делегиране, при пълно спазване на вътрешния процедурен правилник.

Член 61

Влизане в сила

Настоящото решение влиза в сила в деня след публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 13 март 2015 година.

За Комисията

Председател

Jean-Claude JUNCKER

([1]) Решение 2001/844/ЕО, ЕОВС, Евратом на Комисията от 29 ноември 2001 г. за изменение на нейния процедурен правилник (ОВ L 317, 3.12.2001 г., стр. 1).

ПРИЛОЖЕНИЕ I

ТАБЛИЦА ЗА СЪОТВЕТСТВИЕ НА НИВАТА НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ

ЕС	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Евратом	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Белгия	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	бележка ([1]) по-долу
България	Строго секретно	Секретно	Поверително	За служебно ползване
Чешка република	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Дания	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Германия	Streng geheim	Geheim	VS ([2]) — Vertraulich	VS — Nur für den Dienstgebrauch
Естония	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Ирландия	Top Secret	Secret	Confidential	Restricted
Гърция	Άκρως Απόρρητο Съкр.: ΑΑΠ	Απόρρητο Съкр.: (ΑΠ)	Εμπιστευτικό Съкр.: (ΕΜ)	Περιορισμένης Χρήσης Съкр.: (ΠΧ)
Испания	Secreto	Reservado	Confidencial	Difusión Limitada
Франция	Très Secret Défense	Secret Défense	Confidentiel Défense	бележка ([3]) по-долу
Хърватия	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Италия	Segretissimo	Segreto	Riservatissimo	Riservato
Кипър	Άκρως Απόρρητο Съкр.: ΑΑΠ	Απόρρητο Съкр.: (ΑΠ)	Εμπιστευτικό Съкр.: (ΕΜ)	Περιορισμένης Χρήσης Съкр.: (ΠΧ)
Латвия	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Литва	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Люксембург	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Унгария	„Szigorúan titkos!“	„Titkos!“	„Bizalmas!“	„Korlátozott terjesztésű!“
Малта	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Нидерландия	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Австрия	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Полша	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Португалия	Muito Secreto	Secreto	Confidencial	Reservado

ЕС	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Румъния	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Словения	Strogo tajno	Tajno	Zaupno	Interno
Словакия	Prísne tajné	Tajné	Dôverné	Vyhradené
Финландия	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Швеция ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Обединено кралство	UK TOP SECRET	UK SECRET	Няма равностойно обозначение ([5])	UK OFFICIAL — SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding не се счита за ниво на класификация за сигурност в Белгия. Белгия работи със и защитава информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED по начин, който е не по-малко стриктен от стандартите и процедурите, описани в правилата за сигурност на Съвета на Европейския съюз.

([2]) Германия: VS = Verschlusssache.

([3]) Франция не използва ниво на класификация за сигурност „RESTREINT“ в националната си система. Франция работи със и защитава информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED по начин, който е не по-малко стриктен от стандартите и процедурите, описани в правилата за сигурност на Съвета на Европейския съюз.

([4]) Швеция: нивата на класификация за сигурност на горния ред се използват от органите в областта на отбраната, а на долния ред — от други органи.

([5]) Обединеното кралство работи със и защитава класифицирана информация с ниво „CONFIDENTIEL UE/EU CONFIDENTIAL“ в съответствие с изискванията за сигурност за защита на ниво „UK SECRET“.

ПРИЛОЖЕНИЕ II

СПИСЪК НА СЪКРАЩЕНИЯТА

Съкращение	Значение
КО	Криптографски орган
ОКО	Орган за криптографско одобрение
CCTV	Вътрешна система за видеонаблюдение
ОРКМ	Орган за разпределение на криптографски материали
КИС	Комуникационни и информационни системи, работещи с КИЕС
ООС	Определен орган по сигурността
КИЕС	Класифицирана информация на ЕС
УСС	Удостоверение за сигурност на структура
ОИ	Осигуреност на информацията
ООИ	Орган по осигуреността на информацията
АСП	Алармена система против проникване
ИТ	Информационни технологии
МСС	Местен служител по сигурността
НОС	Национален орган по сигурността
РДС	Разрешение за достъп на служител
УРДС	Удостоверение за разрешение на достъп на служител
ИПС	Инструкции за сигурност за програма или проект
РР	Ръководител на регистратура
ОАС	Орган по акредитиране на сигурността
ПАС	Приложение относно аспектите на сигурността
РКЦС	Ръководство за класификация за целите на сигурността
ОПС	Оперативни процедури за сигурност
ОТ	Орган по TEMPEST
ДФЕС	Договор за функционирането на Европейския съюз

ПРИЛОЖЕНИЕ III

СПИСЪК НА НАЦИОНАЛНИТЕ ОРГАНИ ЗА СИГУРНОСТ

БЕЛГИЯ

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Тел.: Secretariat: +32 25014542
Факс: +32 25014596
Ел. адрес: nvo-ans@diplobel.fed.be

БЪЛГАРИЯ

State Commission on Information Security/Държавна комисия по сигурността на информацията
90 Cherkovna Str./ул. Черковна № 90
1505 Sofia/София 1505
Тел.: +359 29333600
Факс: +359 29873750
Ел. адрес: dksi@government.bg
Уебсайт: www.dksi.bg

ЧЕШКА РЕПУБЛИКА

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Тел.: +420 257283335
Факс: +420 257283110
Ел. поща: czech.nsa@nbu.cz
Уебсайт: www.nbu.cz

ДАНИЯ

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Тел.: +45 33148888
Факс: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Тел.: +45 33325566
Факс: +45 33931320

ГЕРМАНИЯ

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Тел.: +49 30186810
Факс: +49 30186811441
Ел. поща: oesIII3@bmi.bund.de

ЕСТОНИЯ

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Тел.: +372 7170113 0019, +372 7170117
Факс: +372 7170213
Ел. поща: nsa@mod.gov.ee

ГЪРЦИЯ

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; + 30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Тел.: +30 2106572045
+ 30 2106572009
Факс: +30 2106536279, +30 2106577612

ИСПАНИЯ

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Тел.: +34 913725000
Факс: +34 913725808
Ел. поща: nsa-sp@areatec.com

ФРАНЦИЯ

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Тел.: +33 171758177
Факс: + 33 171758200

ХЪРВАТИЯ

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Тел.: +385 14681222
Факс: + 385 14686049
Уебсайт: www.uvns.hr

ИРЛАНДИЯ

National Security Authority
Department of Foreign Affairs
76 — 78 Harcourt Street
Dublin 2
Тел.: +353 14780822
Факс: +353 14082959

ИТАЛИЯ

Presidenza del Consiglio dei Ministri
D.I.S. — U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Тел.: +39 0661174266
Факс: +39 064885273

КИПЪР

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Тел.: +357 22807569, +357 22807643,
+357 22807764
Факс: +357 22302351
Ел. поща: cynsa@mod.gov.cy

ЛАТВИЯ

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Тел.: +371 67025418
Факс: +371 67025454
Ел. поща: ndi@sab.gov.lv

ЛИТВА

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Тел.: +370 706 66701, +370 706 66702
Факс: +370 706 66700
Ел. поща: nsa@vsd.lt

LUXEMBOURG

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Тел.: +352 24782210 central
+ 352 24782253 direct
Факс: +352 24782243

УНГАРИЯ

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Тел.: +36 (1) 7952303
Факс: +36 (1) 7950344

Postal address:
H-1357 Budapest, PO Box 2
Ел. поща: nbf@nbf.hu
Уебсайт: www.nbf.hu

МАЛТА

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Тел.: +356 21249844
Факс: +356 25695321

НИДЕРЛАНДИЯ

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Тел.: +31 703204400
Факс: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Тел.: +31 703187060
Факс: +31 703187522

АВСТРИЯ

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Тел.: +43 1531152594
Факс: +43 1531152615
Ел. поща: ISK@bka.gv.at

ПОЛША

Agencja Bezpieczeństwa Wewnętrznego — ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa
Тел.: +48 22 58 57 944
Факс: +48 22 58 57 443
Ел. поща: nsa@abw.gov.pl
Уебсайт: www.abw.gov.pl

ПОРТУГАЛИЯ

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Тел.: +351 213031710
Факс: +351 213031711

РУМЪНИЯ

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA — ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Тел.: +40 212245830
Факс: +40 212240714
Ел. поща: nsa.romania@nsa.ro
Уебсайт: www.orniss.ro

СЛОВЕНИЯ

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Тел.: +386 14781390
Факс: +386 14781399
Ел. поща: gp.uvtp@gov.si

СЛОВАКИЯ

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Тел.: +421 268692314
Факс: +421 263824005
Уебсайт: www.nbusr.sk

ФИНЛАНДИЯ

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Тел.: 16055890
Факс: +358 916055140
Ел. поща: NSA@formin.fi

ШВЕЦИЯ

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Тел.: +46 84051000
Факс: +46 87231176
Ел. поща: ud-nsa@foreign.ministry.se

ОБЕДИНЕНО КРАЛСТВО

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Тел. 1: +44 2072765649
Тел. 2: +44 2072765497
Факс: +44 2072765651
Ел. поща: UK-NSA@cabinet-office.x.gsi.gov.uk