2024/1418

24.5.2024 г.

Делегирано решение № 19/2024 относно правилата за прилагане за работа с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EUCONFIDENTIAL и SECRET UE/EU SECRET

АДМИНИСТРАТИВНИЯТ КОМИТЕТ НА ЕВРОПЕЙСКАТА СМЕТНА ПАЛАТА,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално член 287 от него;

като взе предвид Решение № 41/2021 на Европейската сметна палата относно правилата за сигурност за защита на класифицираната информация на ЕС (КИЕС) ([1]), наричано по-нататък „Решение № 41/2021“;

като взе предвид документа на Европейската сметна палата относно политиката за сигурност на информацията (понастоящем DEC 127/15 FINAL) и документа относно политиката за класифициране на информацията (Съобщение до персонала № 123/20) ([2]);

като взе предвид обсъжданията на Административния комитет на Европейската сметна палата, проведени на заседанието му от 18 март 2024 г.;

като има предвид, че Решение № 41/2021 се прилага за всички служби и помещения на Европейската сметна палата;

като има предвид, че член 1, параграф 3 от Решение № 41/2021 изисква предприемането на мерки, позволяващи служителите на Европейската сметна палата, които имат нужда от достъп до по-високи нива на КИЕС, да могат да правят това в подходящи помещения на други институции, органи или агенции на ЕС;

като има предвид, че съгласно член 1, параграф 3 и член 5, параграф 6 от Решение № 41/2021 Европейската сметна палата може да сключи споразумение за нивото на обслужване с друга институция на ЕС в Люксембург, за да може да работи със и да съхранява информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или по-високо ниво в зона за сигурност на тази институция, и че на 25.9.2023 г. беше подписан Меморандум за разбирателство с Генерална дирекция „Човешки ресурси и сигурност“ на Европейската комисия за използване на защитената зона на дирекцията по сигурността в Люксембург;

като има предвид, че мерките за сигурност за защита на класифицираната информация на ЕС (КИЕС) по време на целия ѝ жизнен цикъл следва да бъдат съобразени конкретно с нейната класификация за сигурност;

като има предвид, че мерките за сигурност за защита на поверителността, интегритета и наличността на информацията, която се съобщава на Европейската сметна палата, трябва да бъдат подходящи за естеството и вида на съответната информация;

като има предвид, че член 3, параграф 3 от Решение № 41/2021 изисква цялата КИЕС да бъде защитена чрез мерки за физическа сигурност, а информацията, класифицирана като CONFIDENTIEL EU/CONFIDENTIAL EU или на по-високо ниво, се защитава допълнително чрез мерки за сигурност на персонала;

като има предвид, че съгласно член 10, параграф 10 от Решение № 41/2021 Административният комитет приема делегирано решение за определяне на правила за прилагане на това Решение; съгласно член 8, параграф 1 член 10, параграф 1 от Решение № 41/2021 тези правила се прилагат в случаи като работа със и съхраняване на КИЕС и нарушения на сигурността;

като има предвид, че чрез своето Решение № 41/2021 Европейската сметна палата гарантира, че нейните мерки за сигурност осигуряват високо ниво на защита на КИЕС и са равностойни на мерките, въведени с цел защита на КИЕС от другите институции, агенции и органи на ЕС;

като има предвид, че на 27 януари 2023 г. влезе в сила опростено административно споразумение, сключено между ЕСП и Комисията, Съвета и ЕСВД.

([1]) ОВ L 256, 19.7.2021 г., стр. 106.
([2]) Публикувани на https://www.eca.europa.eu/bg/Pages/LegalFramework.aspx.

РЕШИ:

ГЛАВА 1

ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и обхват

1. Настоящото решение определя условията за работа с класифицирана информация на ЕС (КИЕС) с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL ([3]) и SECRET UE/EU SECRET ([4]) в съответствие с Решение № 41/2021 на Европейската сметна палата (ЕСП).

2. Настоящото решение се прилага за всички служби и помещения на Европейската сметна палата (ЕСП). То се прилага и за одитните състави и комитетите на ЕСП, които се включват в понятието „служби“ за целите на настоящото решение.

Член 2

Критерии за достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET

1. Достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да бъде предоставен след като:

а) бъде определена необходимостта дадено лице да получи достъп до определена информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, за да може да изпълни професионална дейност или задача за ЕСП;

б) лицето бъде инструктирано за правилата и съответните стандарти и насоки за сигурност с цел защита на информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET;

в) лицето потвърди писмено осведомеността си за своите отговорности за защита на съответната информация; и

г) лицето бъде проучено за надеждност и получи разрешение за достъп от директора на дирекция „Човешки ресурси, финанси и административно обслужване“ на ЕСП до съответното ниво и до определена дата в съответствие с член 4, параграф 4 от Решение № 41/2021.

2. На стажантите в ЕСП не се поверяват задължения, които изискват те да имат достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

3. Достъп се отказва или разрешава на други категории служители в съответствие с таблицата в приложението.

([3]) Съгласно член 1, параграф 2, буква а) от Решение № 41/2021 на Европейската сметна палата информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL е такава „информация и материали, чието неразрешено разкриване би навредило на интересите на Европейския съюз или на една или повече от държавите членки“.

([4]) Съгласно член 1, параграф 2 буква а) от Решение № 41/2021 на Европейската сметна палата, информация с ниво на класификация за сигурност SECRET UE/EU SECRET е такава „информация и материали, чието неразрешено разкриване би навредило сериозно на интересите на Европейския съюз или на една или повече от държавите членки“.

ГЛАВА 2

СЪЗДАВАНЕ НА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ CONFIDENTIEL UE/EU CONFIDENTIAL И SECRET UE/EU SECRET

Член 3

Създател на класифицирана информация

По смисъла на член 2, буква м) от Решение № 41/2021 създателят е 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, като не е задължително съставителят на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET да е един и същ.

Член 4

Определяне на нивото на класификация за сигурност

1. Даден документ се класифицира най-малко на ниво CONFIDENTIEL UE/EU CONFIDENTIAL, ако неразрешеното му разкриване би могло, наред с другото:

а) сериозно да навреди на дипломатическите отношения, т.е. да предизвика официален протест или друга ответна реакция;

б) да накърни сигурността или свободата на личността;

в) да наруши оперативната ефективност или сигурността на наетите служители на държавите членки или други участници или ефективността на важни операции, свързани със сигурността или разузнаването;

г) значително да подкопае финансовата стабилност на водещи организации;

д) да възпрепятства разследването на сериозни престъпления или да улесни извършването на такива;

е) да накърни съществено финансовите, паричните, икономическите и търговските интереси на ЕС или неговите държави членки;

ж) сериозно да възпрепятства разработването или изпълнението на основните политики на ЕС;

з) да прекрати или по друг начин съществено да наруши изпълнението на основни политики на ЕС;

и) да доведе до разкриване на информация, класифицирана на по-високо ниво.

2. Информацията се класифицира най-малко на ниво SECRET UE/EU SECRET, ако неразрешеното ѝ разкриване би могло, наред с другото:

а) да предизвика международно напрежение;

б) сериозно да навреди на отношенията с трети държави или международни организации;

в) пряко да застраши живот или сериозно да наруши обществения ред или сигурността или свободата на личността;

г) да наруши оперативната ефективност или сигурността на наетите служители на държавите членки или други участници или ефективността на изключително важни операции, свързани със сигурността или разузнаването;

д) да причини съществени материални щети на финансовите, паричните, икономическите или търговските интереси на ЕС или неговите държави членки;

е) да доведе до разкриване на информация, класифицирана на по-високо ниво.

3. Създателите могат да решат да определят стандартно ниво на класификация за сигурност за категориите информация, които създават редовно. Те следва да гарантират обаче, че отделните части от информацията са класифицирани на подходящото ниво на класификация за сигурност.

Член 5

Работа с проекти на документи

1. Информацията се класифицира веднага след като бъде изготвена. Лични бележки, предварителни проекти на документи или съобщения, съдържащи информация, която е необходимо да бъде класифицирана на ниво CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се обозначават като такива от самото начало, а изготвянето им и работата с тях трябва да бъдат в съответствие с настоящото решение.

2. Ако окончателният документ вече не дава основание за първоначалното ниво на класификация, неговото ниво на класификация се понижава или премахва след потвърждение от създателя на документа, че това е безопасно.

Член 6

Записване на изходните материали

За да се осигури възможност за упражняване на контрол от създателя на информацията в съответствие с член 14 по-долу, създателите на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET водят отчет за всички класифицирани източници, използвани за изготвянето на класифицирани документи, включително подробности за източниците с първоначален произход от държавите — членки на ЕС, международни организации или трети държави. Когато е целесъобразно, обобщената класифицирана информация се обозначава по начин, позволяващ да се запази самоличността на създателите на използваните изходни материали.

Член 7

Класифициране на части от документ

1. В съответствие с точка 12 от документа относно политиката на ЕСП за класификация на информацията, общото ниво, на което се класифицира даден документ, е не по-ниско от това на най-високо класифицирания елемент от него. Когато се обединява информация от различни източници, се прави преглед на окончателния обобщен документ, 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 за сигурност от това на съставните му части.

2. Документи, съдържащи класифицирана и некласифицирана част, се структурират и обозначават по начин, позволяващ елементите с различна класификация за сигурност и/или степен на чувствителност на информацията да могат лесно да се идентифицират и отделят при необходимост. Това позволява с всяка част да се работи по подходящ начин, в случай че бъде отделена от останалите елементи.

Член 8

Пълно название на грифа за сигурност

1. Информация, която е необходимо да бъде класифицирана, се обозначава като такава и с нея се работи по съответния начин, независимо от физическата форма, под която е представена. Нивото на класификация за сигурност се съобщава ясно на получателите или чрез гриф за сигурност, ако информацията се предоставя в писмен вид (независимо от това дали е на хартиен носител, на преносим носител за съхранение на данни, или в комуникационна и информационна система (КИС), или чрез обявление, ако информацията се предоставя устно (например при разговор или презентация). Класифицираните материали се обозначават физически като такива, за да може да се идентифицира лесно класификацията им за сигурност.

2. Върху документите пълното название на грифа за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET се изписва с главни букви, на френски и английски език (като се започва с названието на френски език), в съответствие с параграф 3. Грифът не се превежда на други езици.

3. Грифът за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET се поставя по следния начин:

а) по средата на горната и долната част на всяка страница от документа;

б) пълното название на грифа за сигурност е на един ред, без интервали от двете страни на наклонената черта;

в) с главни букви, в черен цвят, с шрифт Times New Roman 16 (по възможност, но не по-малко от размер на шрифта 14), който е получер, и с рамка от всички страни.

4. При създаването на документ с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET:

а) върху всяка страница се обозначава ясно нивото на класификация за сигурност;

б) всяка страница се номерира;

в) върху документа се отбелязват референтният номер, регистрационният номер и неговият предмет, които сами по себе си не представляват класифицирана информация, освен ако не са обозначени като такава;

г) всички приложения и притурки се изброяват, когато е възможно — на първата страница; и

д) датата на създаването се посочва в документа.

5. Където е възможно, грифът SECRET UE/EU SECRET се маркира в червено.

Член 9

Съкратени обозначения на грифове за сигурност C-UE/EU-C и S-EU/EU-S

Съкращенията C-UE/EU-C и S-UE/EU-S могат да се използват за обозначаване на нивото на класификация за сигурност на отделни части от даден документ с ниво на класификация за сигурност съответно CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, или когато не е възможно да се постави пълното название на грифа за сигурност, например на малък преносим носител за съхранение на данни. Обозначението може да се използва в основната част на текста, в случай че многократното използване на пълното название на грифа за сигурност би било обременяващо. Съкращението не се използва вместо пълното название на грифовете за сигурност в горната и долната част на всяка страница на документа.

Член 10

Други обозначения за сигурност

1. Документите с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET могат да бъдат обозначени с други грифове, или „обозначения за сигурност“, които указват например областта, за която се отнася документът, или конкретното разпространение въз основа на принципа „необходимост да се знае“. Например:

RELEASABLE TO LIECHTENSTEIN

2. Върху документите с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да се постави забележка за сигурност със специални инструкции за работа с документите и тяхното управление.

Когато е възможно, на първата страница на документа се добавят указания за премахване на нивото на класификация (декласификация) в момента на неговото създаване. Например може да се използва следният гриф:

SECRET UE/EU SECRET until [dd.mm.yyyy] and RESTREINT UE/EU RESTRICTED thereafter

Член 11

Електронно обработване

1. Документите с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се създават посредством електронни средства, когато са налични такива.

2. При създаването на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET служителите на ЕСП използват КИС, акредитирана най-малко за съответното ниво на класификация за сигурност. В случай на съмнение трябва да се потърси съвет от служителя по сигурността на информацията в ЕСП (наричан по-долу „ССИ“).

3. Документите с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, в т.ч. проектите на документи (вж. член 5), не трябва да се изпращат по електронна поща, не се разпечатват, нито се сканират на стандартни принтери или скенери, и с тях не се работи на лични устройства на членовете на персонала. Само принтерите или копирните машини, свързани към самостоятелни компютри, които са защитени от електромагнитно излъчване, или към акредитирана система, могат да се използват за разпечатване на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

Член 12

Регистриране за целите на сигурността

1. Информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET се регистрира за целите на сигурността преди разпространение и при получаване. Тя се регистрира:

— когато пристига или напуска зоната за сигурност на Европейската комисия в Люксембург, за чието използване ЕСП е сключила меморандум за разбирателство; и

— при постъпването ѝ в КИС или при излизането ѝ от нея.

2. Информацията може да се регистрира на хартиен носител или в електронни дневници.

3. Ако информацията се обработва по електронен път в КИС, регистрацията може да бъде обхванатa и от процеси в рамките на самата КИС. В такъв случай КИС трябва да включва мерки за гарантиране на целостта на записите.

4. Ръководителят на регистратурата води регистър, съдържащ най-малко следната информация за всеки документ:

а) датата, на която е бил регистриран окончателният класифициран документ;

б) нивото на класификация за сигурност;

в) когато е приложимо, крайната дата на нивото на класификация за сигурност;

г) наименованието на службата първоизточник;

д) получателя или получателите;

е) предмета на информацията;

ж) референтния номер на документа, даден от службата, създала информацията;

з) регистрационния номер;

и) броя разпространени екземпляри;

й) когато е възможно, регистъра на източниците, използвани за създаване на документа;

к) датата на понижаване или премахване на нивото на класификация на документа; и

л) данните за унищожаването (място, дата, метод, надзор, удостоверение за унищожаване).

Член 13

Разпространение

Изпращачът на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET решава на кого да разпространи информацията въз основа на принципа „необходимост да се знае“. Изготвя се списък за разпространение с цел да се гарантира правилно прилагане на принципа „необходимост да се знае“.

ГЛАВА 3

РАБОТА СЪС СЪЩЕСТВУВАЩА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ CONFIDENTIEL UE/EU CONFIDENTIAL И SECRET UE/EU SECRET

Член 14

Контрол от създателя на информацията

1. Създателят упражнява „контрол от първоизточника“ върху информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, която е създал. Изисква се предварително писмено съгласие на създателя, преди:

а) нивото на класификация на информацията да бъде премахнато или понижено;

б) информацията да бъде използвана за цели, различни от установените от създателя;

в) информацията да бъде разпространена до трета държава или международна организация; или

г) информацията да бъде разкрита на страна извън ЕСП, но в рамките на ЕС.

2. Притежателите на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET са надлежно оправомощени лица, които получават достъп до класифицираната информация, за да могат да изпълняват задълженията си. Те отговарят за правилния начин на работа, съхранение и защита на тази информация в съответствие с Решение № 41/2021. За разлика от създателите на класифицирана информация, на притежателите на такава информация не е разрешено да вземат решения за понижаване или премахване на нивото на класификация или последващо предоставяне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

3. Ако създателят на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET не може да бъде установен, службата на ЕСП, която притежава тази класифицирана информация, упражнява контрол от създателя. В случай че притежателят на информацията счете за необходимо да предостави информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET на трета държава или международна организация, ЕСП се консултира с една от страните по споразумение за сигурност на информацията със същата трета държава или международна организация ([5]).

Член 15

Комуникационна и информационна система, подходяща за работа с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/E

Работата и предаването на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се извършва по възможност по електронен път. В съответствие с член 6 от Решение № 41/2021 за тази цел могат да се използват само КИС и оборудване, които са били акредитирани от друга институция, агенция или орган на ЕС, или от ЕСП.

Член 16

Конкретни мерки във връзка с информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET на преносими носители за съхранение на данни

1. Използването на преносими носители за съхранение на данни, като USB устройства, CD, DVD или карти с памет (включително SSD ([6])), се контролира и отчита стриктно. Могат да се използват само преносими носители за съхранение на данни, предоставени от ЕСП или от друга институция, агенция или орган на ЕС, одобрени от ССИ и криптирани с продукт, одобрен от ССИ. За прехвърлянето на класифицирана информация не могат да се използват лични преносими носители за съхранение на данни, нито такива, които са били разпространени свободно на конференции, семинари и др. Когато е възможно, следва да се използват съобразени с Tempest преносими носители за съхранение на данни в съответствие с указанията на ССИ.

([5]) За повече подробности вж. член 35.

([6]) SSD означава полупроводниково устройство за съхранение на данни, твърдотелно устройство или диск.

2. Когато с даден класифициран документ се работи или той се съхранява по електронен път на преносим носител за съхранение на данни, грифът за сигурност трябва да се вижда ясно като част от самата информация, която се показва, както и в наименованието на файла и върху носителя за съхранение на данни.

3. Служителите трябва да имат предвид, че когато големи количества класифицирана информация се съхраняват на преносим носител за съхранение на данни, може да е необходимо устройствата да бъдат с по-високо ниво на класификация за сигурност.

4. Само надлежно акредитирани КИС могат да се използват за предаване на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET към или от преносими носители за съхранение.

5. Преди да се свали такава информация на преносим носител за съхранение на данни, се предприемат специални мерки, за да се гарантира, че на този носител няма вируси и зловреден софтуер.

6. Когато е приложимо, с преносимите носители за съхранение на данни се работи в съответствие с оперативни процедури за сигурност, свързани с използваната система за криптиране.

7. Документи на преносими носители за съхранение на данни, които вече не са необходими или са били прехвърлени на подходяща КИС, се отстраняват или изтриват по сигурен начин с помощта на одобрени продукти или методи. Освен ако не се съхраняват в подходящ сейф, преносимите носители за съхранение на данни се унищожават, когато вече не са необходими. Всяко унищожаване или изтриване се осъществява по метод, който е в съответствие с правилата за сигурност на ЕСП. Поддържа се инвентарен опис на преносимите носители за съхранение на данни и тяхното унищожаване се регистрира.

Член 17

Работа със и съхранение на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET

1. В съответствие с член 5, параграфи 5 и 6 от Решение № 41/2021 работата с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се осъществява в зона за сигурност ([7]). Достъп до такава информация имат и служителите на ЕСП в зоните за сигурност на друга институция на ЕС.

2. Съгласно член 5, параграф 6 от Решение № 41/2021 и ако има изрично съгласие от създателя, с такава информация може по изключение да се работи в административната зона ([8]) на ЕСП, при условие че КИЕС е защитена от достъп на неоправомощени лица.

3. По време на криза или в случай на извънредна ситуация с такава информация може да се работи извън зона за сигурност или административна зона, при условие че притежателят се е ангажирал да приложи компенсаторни мерки, които включват най-малко следното:

— Документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU не се четат на обществени места.

— КИЕС се съхранява по всяко време под личния контрол на притежателя.

— В случай на документи на хартиен носител, притежателят е уведомил регистратурата за КИЕС във възможно най-кратък срок и в зависимост от естеството на кризата или извънредната ситуация, че работата с класифицираните документи се осъществява извън зона за сигурност или административна зона.

— Когато не се четат или обсъждат, документите се съхраняват в подходящ сейф.

— Когато документите се четат или обсъждат, вратите на помещението са затворени.

— Подробностите за документите не могат да се обсъждат по незащитена телефонна линия или по електронна поща.

— Притежателят не може да фотокопира или сканира документите. Само регистратурата за КИЕС може да предоставя допълнителни екземпляри.

([7]) Съгласно определението в член 18 на Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53).

([8]) Както е определено в приложението към Решение № 41/2021.

— Работата с документите и временното им съхраняване извън административна зона или зона за сигурност е разрешено само ако това е абсолютно необходимо, след което те се връщат в регистратурата за КИЕС.

— При връщането на документите се изисква подпис.

— Притежателят не трябва нито да изхвърля класифицираните документи, нито да ги унищожава.

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

5. Допълнителна информация може да бъде поискана от ССИ.

6. Всички предполагаеми или действителни инциденти, свързани със сигурността, които засягат даден документ, се докладват на ССИ във възможно най-кратък срок.

Член 18

Копиране и превод на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET

1. Копие или писмен превод на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да се прави по указание на притежателя, при условие че създателят е дал изрично съгласие и не е поставил предупредителни обозначения. Не се правят повече копия, отколкото са строго необходими. ЕСП може също така да поиска от създателя да предостави копие, преведено на английски език.

2. Когато се възпроизвежда само част от даден класифициран документ, се прилагат същите условия като тези за копията на целия документ. Откъсите също се класифицират на същото ниво, освен ако създателят изрично не е ги класифицирал на по-ниско ниво или обозначил като некласифицирани.

3. Мерките за сигурност, приложими към оригиналната информация, се прилагат и за нейните копия и писмени преводи.

Член 19

Общи принципи за пренасяне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET

1. Когато е възможно, информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, която трябва да бъде изнесена извън дадена зона за сигурност или административна зона в съответствие с разпоредбите на член 17, параграф 2, се изпраща по електронен път посредством надлежно акредитирани средства и/или се защитава посредством одобрени криптографски продукти.

2. В зависимост от наличните средства и конкретните обстоятелства информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да бъде физически пренасяна на ръка на хартиен носител или на преносим носител за съхранение на данни. Използването на преносими носители за съхранение на данни за прехвърляне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се предпочита пред изпращането на документи на хартиен носител.

3. В съответствие с член 6, параграф 8 от Решение№ 41/2021 преносимите носители за съхранение на данни се криптират с помощта на продукт, одобрен за защита на КИЕС или от Съвета, или от генералния секретар на Съвета, в качеството му на орган за криптографско одобрение, или от друга институция, агенция или орган на ЕС. С информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET на преносими носители за съхранение на данни, които не са защитени с така одобрен продукт за криптиране, се работи по същия начин като с тази на хартиен носител.

4. Пратките могат да съдържат повече от един елемент на КИЕС, при условие че се спазва принципът „необходимост да се знае“.

5. Използваната опаковка следва да гарантира, че съдържанието не се вижда. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се пренася в два слоя непрозрачна опаковка, като плик, непрозрачна папка или куфарче. Външната опаковка е запечатана и трябва да не разкрива по никакъв начин естеството на съдържанието, нито неговото ниво на класификация; Вътрешният слой на опаковката се обозначава с надписа CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET. И върху двата слоя се посочват името, длъжността и адресът на предвидения получател, както и адрес за връщане, в случай че доставката не може да бъде осъществена.

6. Служителите или куриерите, пренасящи на ръка информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, са оправомощени за целите на сигурността и им се издава удостоверение за куриер.

7. Пликовете и опаковките не трябва да се отварят по време на пренасянето. Предоставеното на куриера одобрение за сигурност не му дава право на достъп до класифицираната информация в пратката.

8. Съгласно член 5, параграф 12 от Решение № 41/2021 създателят може също така да наложи допълнителни мерки за физическа сигурност, за да защити информацията срещу неразрешено разкриване по време на транспортирането.

9. Всички предполагаеми или действителни инциденти, свързани със сигурността, по отношение на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, която се пренася от служители или куриери, се докладват на ССИ за последващо разследване във възможно най-кратък срок.

Член 20

Пренасяне на ръка на преносими носители за съхранение на данни

1. Преносимите носители за съхранение на данни, които се използват за пренос на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, се придружават от спедиционна бележка, в която се посочват подробности за преносимите носители за съхранение на информация и за всички съдържащи се в тях файлове, така че получателят да може да извърши необходимите проверки и да потвърди получаването.

2. На устройствата се съхранява само КИЕС, която се пренася. Цялата класифицирана информация, качена на едно устройство, трябва да бъде предназначена за един и същ получател. Изпращачите следва да отчитат факта, че големи количества класифицирана информация, съхранявани на едно и също устройство, може да изискват по-високо ниво на класификация за сигурност за устройството като цяло.

3. За пренасяне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET се използват само преносими носители за съхранение на данни с подходящ гриф за сигурност.

4. Всяка информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, съхранявана на преносими носители за съхранение, се регистрира за целите на сигурността.

Член 21

Пренасяне на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET в рамките на отделните служби и в помещенията на ЕСП

1. Оправомощените за целите на сигурността служители могат да носят документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET в рамките на отделните служби и в помещенията на ЕСП, но документите не трябва да напускат притежателя си или да се четат публично.

2. Документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU не се изпращат по вътрешната поща.

Член 22

Пренасяне на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET в рамките на Европейския съюз

1. Информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да се пренася от служители или куриери на ЕСП или на институцията, агенцията или органа на ЕС, който е създател на информацията, навсякъде в рамките на ЕС, при условие че те изпълняват следните указания:

а) За предаването на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се използват непрозрачни пликове или опаковка. Външната опаковка е запечатана и не разкрива по никакъв начин естеството на съдържанието, нито неговото ниво на класификация.

б) Информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET не трябва да напуска притежателя си.

в) Пликът или опаковката не трябва да се отварят по пътя и информацията не трябва да се чете на обществени места.

2. Служителите на регистратурата, които желаят да изпратят информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL до други места в ЕС, могат да организират предаването ѝ по един от следните начини:

а) национални пощенски услуги с проследяване на пратката или някои платени куриерски услуги, които гарантират лично пренасяне на ръка, при условие че отговарят на изискванията, определени в член 24 от настоящото решение; или

б) военен, правителствен или дипломатически куриер, в координация със служителите от регистратурата за класифицирана информация.

3. Служителите, които желаят да изпратят информация с ниво на класификация SECRET UE/EU SECRET до други държави — членки на ЕС, могат да уредят с ръководителя на регистратурата тази информация да се предаде само на военен, правителствен или дипломатически куриер, а не на пощенска служба или платен куриер.

4. Всички служители на ЕСП или служебни куриери, пренасящи информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, носят куриерско удостоверение за всяка пратка. Удостоверението се издава от ръководителя на регистратурата и в него се посочва, че приносителят е оправомощен да пренася пратката.

Член 23

Пренасяне на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET от или до територията на трета държава

1. Информация с ниво на класификация CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET може да се пренася на ръка от служители на ЕСП или на институцията, органа или агенцията на ЕС, която е създател на информацията, между територията на ЕС и територията на трета държава.

2. Служителите на регистратурата могат да организират пренасяне чрез военен или дипломатически куриер.

3. Когато пренасят на ръка документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, които са на хартиен носител или на преносим носител за съхранение на данни, служителите изпълняват всички допълнителни мерки, изброени по-долу:

— При пътувания с обществен транспорт класифицираната информация се поставя в куфарче или в чанта, за която отговаря лично нейният приносител. Това куфарче или чанта не се оставя в багажното отделение.

— Вътрешната опаковка е с официален печат, който указва, че пратката е официална и не трябва да се подлага на проверки за сигурност.

— Приносителят носи със себе си удостоверение за куриер, което се издава от ръководителя на регистратурата и което удостоверява, че той е оправомощен да пренася пратка с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

Член 24

Пренасяне от платени куриери

1. За целите на настоящото решение терминът „платени куриери“ включва национални пощенски служби и куриерски фирми, предлагащи услуга, при която информацията се доставя срещу заплащане и може или да се пренесе лично на ръка или да се проследи.

2. Платените куриери могат да предават информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL в рамките на държава — членка на ЕС, или между две държави членки. Платените куриери могат да предават информация с ниво на класификация SECRET UE/EU SECRET в рамките на дадена държава членка, но не и в чужбина.

3. Платените куриерски служби се инструктират да доставят пратки с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET само на ръководителя на регистратурата, на надлежно оправомощения му заместник или на предвидения получател.

4. Платените куриери могат да използват услугите на подизпълнител. Независимо от това куриерската фирма носи отговорност за спазването на настоящото решение.

Член 25

Подготовка на КИЕС за експедиране чрез платени куриерски служби

1. При подготовката на пратки с класифицирана информация изпращачът взема под внимание факта, че платените куриерски служби доставят пратки с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET само до ръководителя на регистратурата, негов надлежно оправомощен заместник или предвидения получател.

2. Пратките с информация, изпратени чрез одобрена платена куриерска служба, се подготвят и опаковат, както следва:

а) Информацията се поставя в непрозрачен двоен плик (като вътрешният плик е такъв, че всеки опит за неговото отваряне ще бъде очевиден) или друг подходящо обезопасен опаковъчен материал.

б) Нивото на класификация трябва да бъде ясно обозначено на вътрешния плик или слой от опаковката.

в) Външната опаковка е запечатана и не носи гриф за сигурност.

г) Както вътрешните, така и външните пликове или слоеве от опаковки трябва да са ясно адресирани до посочено лице при предвидения получател и да съдържат адрес за връщане.

д) Във вътрешния плик или във вътрешния слой на опаковката се поставя формуляр на регистрационна разписка, който се попълва и връща от получателя. В регистрационната разписка, която сама по себе си не е класифицирана информация, се посочват референтният номер, датата и номерът на копието на документа, но не се посочва предметът на документа.

е) Външният плик или опаковка трябва да съдържат разписка за доставка. В разписката за доставка, която сама по себе си не е класифицирана информация, се посочва референтният номер, датата и номерът на копието на документа, но не трябва да се посочва предметът на документа.

ж) Куриерската служба трябва да вземе и предостави на изпращача доказателство за получаването на пратката в регистрационния дневник или да получи разписки или номерата на пратките.

3. Преди да изпрати пратката, изпращачът договаря с посочения получател подходяща дата и час за доставка.

4. Изпращачът носи цялата отговорност за всяка пратка, изпратена чрез платена куриерска служба. В случай че дадена пратка се изгуби или не се достави навреме, изпращачът информира ССИ и ръководителя на регистратурата, които ще проследят развитието на инцидента, свързан със сигурността.

Член 26

Други специфични условия за работа

1. Спазват се всички допълнителни условия, предвидени в споразумение за сигурност на информацията или административни договорености. При съмнение служителите следва да се допитат до ССИ или ръководителя на регистратурата.

2. Изискването за две опаковки може да отпадне за класифицирана информация, която е защитена посредством одобрени криптографски продукти. Въпреки това, за да може да се посочи адрес и тъй като върху преносимите носители за съхранение на данни следва да има ясно указан гриф за сигурност, тези носители се пренасят в поне един запечатан непрозрачен плик, но може да е необходимо да се приложат допълнителни мерки за физическа защита, като например да се използват пликове с въздушни мехурчета.

ГЛАВА 4

КЛАСИФИЦИРАНИ ЗАСЕДАНИЯ

Член 27

Подготовка на заседания с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET

1. Заседанията, на които трябва да се обсъжда информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се провеждат само в заседателна зала, която е акредитирана за съответното ниво или за по-високо ниво. ЕСП може да използва заседателни зали в зона за сигурност на друга институция на ЕС. Когато не е налична такава зала, служителите се консултират със ССИ.

2. По принцип дневният ред на заседанията не следва да бъде класифициран. Ако в дневния ред на дадено заседание се споменават класифицирани документи, самият дневен ред не се класифицира автоматично. Точките от дневния ред се формулират по начин, който не излага на риск интересите на ЕС или на някоя държава членка.

3. Организаторите на заседанието напомнят на участниците, че всички коментари по дадена точка от дневния ред, съдържаща информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, не трябва да се изпращат по електронната поща или друго средство, което не е било надлежно акредитирани в съответствие с член 11 от настоящото решение.

4. Организаторите на заседанията се стремят да групират последователно в дневния ред точките с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, така че да се осигури гладкото протичане на заседанието. Само лица, за които е установена необходимост „да се знае“, притежаващи разрешение за достъп до съответното ниво и надлежно оправомощени, могат да присъстват по време на обсъждането на класифицирани точки от дневния ред.

5. В поканите за заседания следва да се съдържа предварително предупреждение, че дневният ред ще включва класифицирани теми и че ще се прилагат подходящи мерки за сигурност.

6. Организаторите на заседанията напомнят на участниците, че преносимите електронни устройства трябва да бъдат оставени извън заседателната зала, когато се обсъждат точки, съдържащи информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

7. Организаторите на заседанието изготвят пълен списък на участниците преди заседанието. В съответствие с член 4, параграф 6 от Решение № 41/2021 те също така своевременно информират ССИ за датите, часовете и местата на заседанията, както и списъците на участниците в тях.

Член 28

Достъп на участниците до заседание с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET

1. Организаторите на заседанието информират ССИ и ръководителя на регистратурата за всички външни посетители, които ще присъстват на заседание с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, организирано от ЕСП.

2. За да могат да присъстват на обсъждането на точки от дневния ред с информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, от участниците ще се изиска да докажат, че притежават валидно разрешение за достъп на персонала за съответното ниво.

Член 29

Електронно оборудване в зали за заседания с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET

Само информационни системи, акредитирани в съответствие с член 11 от настоящото решение, могат да бъдат използвани, когато се предава информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, например в хода на презентация или видеоконферентна връзка.

Член 30

Процедури, които се спазват по време на заседания с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET

1. В началото на обсъждането на класифицирана информация председателят обявява на участниците в заседанието, че се преминава към режим на класифицирана информация. Вратите се затварят.

2. В началото на обсъждането на участниците и устните преводачи, в зависимост от случая, се дава само необходимият брой документи срещу подпис.

3. Документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET не се оставят без надзор през почивките по време на заседанието.

4. В края на заседанието на участниците и устните преводачи се напомня да не оставят без надзор в залата никакви класифицирани документи, нито класифицирани бележки, които може да са водили. Всички документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, които не са нужни на участниците в края на заседанието, както и всички документи, използвани от устните преводачи, се връщат на ръководителя на регистратурата срещу подпис, за да бъдат унищожени в одобрени шредери ([9]).

5. По време на заседанието се отбелязва списъкът на участниците, заедно с описание на всяка класифицирана информация, споделена с държавите членки и предоставена устно на трети държави или международни организации, с цел тези данни да бъдат отразени в резултатите от работата.

Член 31

Устни и писмени преводачи

Само устни и писмени преводачи, които имат разрешение за достъп и са оправомощени и за които се прилага Правилникът за длъжностните лица или Условията за работа на другите служители на Европейския съюз ([10]), или които имат договорно правоотношение с ЕСП или друга институция на ЕС, имат достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET.

([9]) За повече подробности вж. член 42, параграф 6.

([10]) Регламент № 31 (ЕИО), установяващ Правилника за длъжностните лица и Условията за работа на другите служители, изменен (ОВ 45, 14.6.1962 г., стр. 1385/62) (ELI: http://data.europa.eu/eli/reg/1962/31 (1)/2023—01—01).

ГЛАВА 5

СПОДЕЛЯНЕ И ОБМЕН НА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ CONFIDENTIEL UE/EU CONFIDENTIAL И SECRET UE/EU SECRET

Член 32

Съгласие на създателя на класифицирана информация

Ако ЕСП не е създателят на класифицираната информация, за която се иска предоставяне или споделяне, или на съдържащия се в нея изходен материал, службата на ЕСП, която притежава класифицираната информация, най-напред иска писмено съгласие от създателя на информацията за нейното предоставяне. Ако създателят на информацията не може да бъде установен, службата на ЕСП, която притежава класифицираната информация, упражнява контрол от създателя.

Член 33

Споделяне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET с други структури на ЕС

1. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да се споделя с друга институция, агенция, орган или служба на ЕС само ако за получателя е установена необходимост да знае и структурата има съответна правна договореност с ЕСП.

2. В рамките на ЕСП регистратурата за КИЕС по правило е основният входен и изходен пункт за обмен на класифицирана информация с други институции, агенции, органи и служби на ЕС.

Член 34

Обмен на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET с държавите членки

1. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET може да се споделя с държавите членки, ако за получателя е установена необходимост да знае и той е получил разрешение за достъп.

2. Класифицираната информация на държавите членки, която носи равностойния национален гриф за сигурност ([11]) и която е била предоставена на ЕСП, получава същото ниво на защита като информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET.

Член 35

Обмен на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET с трети държави и международни организации

1. Информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се предоставя на трета държава или международна организация само ако за получателя е установена необходимост да знае и държавата или международната организация разполага с подходяща правна или административна рамка, като например споразумение за сигурност на информацията или административна договореност с ЕСП. Разпоредбите на всяко такова споразумение или договореност имат предимство пред разпоредбите на настоящото решение.

2. Регистратурата за КИЕС по правило е основният входен и изходен пункт за всяка информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, обменяна между ЕСП и трети държави или международни организации.

([11]) В приложение I към Решение (ЕС, Евратом) 2015/444 е включена таблица за съответствие на грифовете на държавите членки.

3. Всяка класифицирана информация, получена от трета държава или международна организация, се регистрира за целите на сигурността. Поради тази причина служителите се свързват с регистратурата за КИЕС, ако получат класифицирана информация извън обичайния канал на регистратурата.

4. За да се осигури проследимост, информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се регистрира:

— при постъпването ѝ в зоната за сигурност или при излизането ѝ от нея; и

— при постъпването ѝ в КИС или при излизането ѝ от нея.

5. Информацията може да се регистрира на хартиен носител или в електронни дневници.

6. Регистрационните процедури за работа с класифицирана информация в рамките на акредитирана КИС, могат да се извършват от процеси в рамките на самата КИС. В такъв случай КИС включва мерки за гарантиране на целостта на записите в регистрационните файлове.

7. На класифицирана информация, получена от трета държава или международна организация, се предоставя ниво на защита, равностойно на това, с което се ползва КИЕС, носеща равностоен гриф за сигурност според посоченото в съответното споразумение за сигурност на информацията или административна договореност.

Член 36

Извънредно ad hoc предоставяне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET

1. Когато ЕСП или някоя от нейните служби прецени, че съществува извънредна необходимост от предоставяне на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET на трета държава, международна организация или структура на ЕС, но не е налице споразумение за сигурност на информацията или административна договореност, се прилага извънредната ad hoc процедура за предоставяне на класифицирана информация.

2. Службите на ЕСП се свързват със ССИ и създателя на информацията. ЕСП се консултира с една от страните по споразумение за сигурност на информацията със същата трета държава, международна организация или структура на ЕС.

3. След тази консултация, въз основа на предложение на генералния секретар, колегията на членовете на ЕСП може да разреши предоставянето на съответната информация.

ГЛАВА 6

КРАЙ НА ЖИЗНЕНИЯ ЦИКЪЛ НА ИНФОРМАЦИЯ С НИВО НА КЛАСИФИКАЦИЯ ЗА СИГУРНОСТ CONFIDENTIEL UE/EU CONFIDENTIAL И SECRET UE/EU SECRET

Член 37

Кога се понижава или премахва нивото на класификация

1. Информацията остава класифицирана само докато е необходима нейната защита. Понижаване на нивото на класификация означава определяне на по-ниско ниво на класификация за сигурност. Премахване на нивото на класификация (декласификация) означава, че информацията повече няма да се смята за класифицирана. При създаването на информацията създателят посочва, когато е възможно, дали нивото на класификация на КИЕС може да бъде понижено или премахнато на определена дата или след настъпването на определено събитие. В противен случай създателят преразглежда информацията и оценява рисковете на всеки пет години с оглед да определи дали първоначалното ниво на класификация все още е подходящо.

2. За документите на ЕСП също може да се прилага понижаване или премахване на нивото на класификация на ad hoc основа, например след искане за достъп от обществеността.

Член 38

Отговорност за понижаване и премахване на нивото на класификация

1. Към информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET не се прилага понижаване или премахване на нивото на класификация без разрешението на създателя.

2. Службата на ЕСП, която е създала даден класифициран документ, отговаря за взимането на решение дали може да понижи или премахне нивото на класификация. В рамките на ЕСП всички искания за премахване на нивото на класификация се изпращат за консултация до главния ръководител или директора на службата — създател на информацията, или на ръководителя на задача. Ако службата е съставила класифицирана информация от различни източници, тя първо иска съгласието на всички други страни, които са предоставили изходен материал, включително на държавите членки, други органи на ЕС, трети държави и международни организации.

3. Когато службата на ЕСП, която е създател на информацията, вече не съществува и нейните функции са поети от друга служба, решението за понижаване или премахване на нивото на класификация се взема от тази друга служба. Когато службата, която е създател на информацията, вече не съществува и нейните функции не са поети от друга служба, решението за понижаване или премахване на нивото на класификация се взема съвместно от директорите на ЕСП.

4. Службата, отговаряща за понижаването или премахването на нивото на класификация, си сътрудничи с регистратурата за КИЕС относно практическите действия по понижаване или премахване на нивото на класификация.

Член 39

Чувствителна некласифицирана информация

Когато при прегледа на даден документ се вземе решение за премахване на нивото на класификация, се обмисля обозначаването му с гриф „чувствителна некласифицирана информация“ по смисъла на точка 16 от документа за политиката на ЕСП относно сигурността на информацията ([12]) и точка 4 от Насоките за класифициране и работа с класифицирана информация, която не е КИЕС.

Член 40

Как се указва понижаването или премахването на нивото на класификация на даден документ

1. Първоначалният гриф за сигурност в горната и долната част на всяка страница трябва да бъде видимо зачеркнат (не отстранен) чрез функцията „зачертаване“ за електронните формати или ръчно за разпечатките.

2. На първата (заглавната) страница се поставя печат, който указва понижено или премахнато ниво на класификация, и се попълват данните на органа, отговорен за понижаването и премахването на нивото на класификация, и съответната дата.

3. Първоначалните получатели на информацията с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се уведомяват за понижаването или премахването на нивото на класификация. Първоначалните получатели отговарят за уведомяването на всички последващи адресати, до които са изпратили първоначалната информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET, или които са били поставени в копие на тази информация.

4. Архивната служба на ЕСП се известява за всички решения за премахване на нивото на класификация.

5. За всички писмени преводи на класифицирана информация се прилагат същите процедури за понижаване или премахване на нивото на класификация като тези за оригиналната езикова версия.

([12]) Публикуван на https://www.eca.europa.eu/bg/Pages/LegalFramework.aspx.

Член 41

Частично понижаване или премахване на нивото на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET

1. Възможно е и частично понижаване или премахване на нивото на класификация (напр. на приложения, само на някои параграфи). Процедурата е идентична с тази за понижаване или премахване на нивото на класификация на целия документ.

2. Частичното премахване на класификацията на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET води до създаването на декласифицирано извлечение.

3. В декласифицираното извлечение частите, които остават класифицирани, се заменят с обозначението:

PART NOT TO BE DECLASSIFIED

което се поставя или в самия текст (ако частта, която продължава да бъде класифицирана, е част от параграф), или като отделен параграф (ако частта, която продължава да бъде класифицирана, представлява най-малко един пълен параграф).

4. Ако нивото на класификация на цяло приложение не може да бъде премахнато и следователно това приложение бъде изключено от извлечението, това се посочва изрично в текста.

Член 42

Рутинно унищожаване или изтриване на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET

1. ЕСП следва да не натрупва големи количества класифицирана информация.

2. Службите, които създават КИЕС, правят преглед на документите на всеки 5 години с оглед на тяхното евентуално унищожаване или изтриване. Тази разпоредба се прилага на редовни интервали както за информацията на хартиен носител, така и за информацията, съхранявана в КИС.

3. Служителите не унищожават документи на хартиен носител с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, които вече не са им необходими, а вместо това се обръщат към ръководителя на регистратурата с искане да бъдат унищожени документите, при спазване на изискванията за архивиране на оригиналния документ.

4. От служителите не се изисква да информират създателя на информацията, ако унищожат копия на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET.

5. За проектите на материали, съдържащи класифицирана информация, се прилагат същите методи за изхвърляне като тези за окончателните документи с класифицирана информация.

6. За унищожаването на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET се използват само одобрени шредери. Подходящи за унищожаване на документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL са шредери от ниво 5 по DIN 66399. Подходящи за унищожаване на документи с ниво на класификация за сигурност SECRET UE/EU SECRET са шредери от ниво 6 по DIN 66399.

7. Отпадъците от одобрени шредери може да се изхвърлят като обикновени офисни отпадъци.

8. Ръководителят на регистратурата изготвя удостоверения за унищожаване и актуализира съответно електронните дневници и друга информация, свързана с регистрация.

9. Всички носители и устройства, съдържащи информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, се прочистват по подходящ начин, когато достигнат края на работния си живот. Електронните данни се унищожават или изтриват от информационните ресурси и свързаните с тях устройства за съхранение по начин, който дава достатъчна увереност, че информацията не може да бъде възстановена. При прочистването се премахват всички данни от устройствата за съхранение, както и всички етикети, грифове и регистрационни файлове за дейността.

10. Компютърните носители за съхранение на данни се предават на ССИ за унищожаване и изхвърляне, след като бъде информиран ръководителят на регистратурата.

Член 43

Евакуация и унищожаване на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET при извънредни ситуации

1. В съответствие с Меморандума за разбирателство между ЕСП и Генерална дирекция „Човешки ресурси и сигурност“ на Европейската комисия относно използването на нейната зона за сигурност, в случай на непредвидена ситуация се прилага установената процедура на Европейската комисия при извънредни ситуации, за да се опази класифицираната информация. Ако е необходимо, местният служител по сигурността в Люксембург на дирекция „Сигурност“ на Европейската комисия получава достъп до сейфа на ЕСП, за да приложи установената процедура на Европейската комисия при извънредни ситуации и да задейства евентуалните планове за спешна евакуация и унищожаване с цел опазване на КИЕС, която е изложена на значителен риск да попадне в ръцете на неоправомощени лица по време на криза. По реда на предимството и в зависимост от характера на спешната ситуация се пристъпва към:

i) преместване на КИЕС на алтернативно безопасно място, по възможност в зона за сигурност в същата сграда;

ii) евакуиране на КИЕС на алтернативно безопасно място, когато е възможно — зона за сигурност в друга сграда, за предпочитане институция на ЕС;

iii) унищожаване на КИЕС, по възможност като се използва одобрено средство за унищожаване.

2. При задействане на плановете за действие при извънредни ситуации, предимство се дава на преместването или унищожаването на информация с ниво на класификация за сигурност SECRET UE/EU SECRET и след това на всяка информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL.

3. Самите оперативни данни за плановете за евакуация и унищожаване при извънредни ситуации са с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED. Във всеки сейф, използван за съхранение на информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET се пази копие, което да бъде достъпно в случай на извънредна ситуация.

Член 44

Архивиране

1. Решенията дали и кога да се архивира информацията и съответните практически мерки, които трябва да се предприемат, трябва да бъдат в съответствие с политиката на ЕСП за сигурност на информацията, за класифициране на информацията и за архивирането на документи.

2. Документи с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL и SECRET UE/EU SECRET не се изпращат в Историческите архиви на Европейския съюз във Флоренция.

ГЛАВА 7

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 45

Прозрачност

Настоящото решение се свежда до вниманието на служителите на ЕСП и всички други лица, за които се прилага, и се публикува в Официален вестник на Европейския съюз.

Член 46

Влизане в сила

След приемането му от Административния комитет, настоящото решение влиза в сила в деня след публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Люксембург на 19 март 2024 г.

За Административния комитет на Европейската сметна палата

Председател

Tony MURPHY

ПРИЛОЖЕНИЕ

Категории служители, които могат да имат достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET, когато това е необходимо за изпълнението на задълженията им

Категории служители на Европейската сметна палата	Достъп до информация с ниво на класификация за сигурност CONFIDENTIEL UE/EU CONFIDENTIAL или SECRET UE/EU SECRET	Условия
Членове на ЕСП	Да	Инструктаж + потвърждение
Длъжностни лица	Да	Проучване + инструктаж + потвърждение + разрешение + необходимост да се знае
Срочно наети служители	Да	Проучване + инструктаж + потвърждение + разрешение + необходимост да се знае
Договорно наети служители	Да	Проучване + инструктаж + потвърждение + разрешение + необходимост да се знае
Командировани национални експерти (КНЕ) от държавите — членки на ЕС	Да	Само ако имат разрешение за достъп от своите държави членки преди встъпването им в длъжност + инструктаж от ЕСП + потвърждение + разрешение от ЕСП + необходимост да се знае
Стажанти	Не	Без изключения
Всяка друга категория служители (лица, наети чрез агенция за временна заетост, външни служители intra-muros и др.)	Не	Без изключения